Projet ICare

Utilisation de la signature électronique (2) :

La dématérialisation documentaire dans les téléprocédures

Référence : ICARE/CAB/TPC/DOC_23/v2
Type : Note de travail
Diffusion : membres du consortium seulement

Date : 23/06/2003
Titre : **ICare – Utilisation de la signature électronique : la dématérialisation documentaire dans les téléprocédures**

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

Résumé :
Ce document expose à quelles conditions il est possible de dématérialiser un document administratif, par exemple une déclaration, afin de le transmettre et comment il est possible de valider juridiquement cette opération, en particulier grâce à la signature électronique.

TABLES DES MATIERES

1 INTRODUCTION - LA PROBLEMATIQUE DE LA DEMATERIALISATION DES TELEPROCEDURES ET LES SOLUTIONS 3

2 PARTIE I- LA PROBLEMATIQUE DE LA DEMATERIALISATION DOCUMENTAIRE 5

2.1 LA DÉMATÉRIALISATION, ATTEINTE AU FORMALISME JURIDIQUE 5
2.1.1. Rappel sur la notion de formalisme juridique 5
2.1.1.1 Le concept de formalisme juridique 5
2.1.1.2. Le formalisme juridique appliqué aux documents 6
2.1.2. Les déclarations administratives et le formalisme juridique 7
2.1.2.1. Notion de formulaire administratif 7
2.1.2.2. La diffusion du formulaire administratif, du papier à l'électronique 7
2.1.2.3. La pratique administrative des formulaires 8
2.2 LA PRÉSENCE DE MENTIONS OBLIGATOIRES 9
2.2.1. Présence des mentions obligatoires 9
2.2.2. Forme des mentions 9
2.3 L'EXIGENCE DE SIGNATURE 10
2.3.1. Le dispositif juridique de la signature électronique 10
2.3.2. Le dispositif technique de la signature électronique 11
2.3.4. Le sens de la signature des télédéclarations 12
2.3.4.1. Un consentement donné aux obligations ou au contenu 12
2.3.4.2. Les enseignements des déclarations existantes 13
2.3.5. La signature du déclarant 14
2.4. L'ABANDON DU SUPPORT PAPIER 15
2.4.1. Les bases juridiques de l'abandon de l'écrit-papier 15
2.4.2. L'acte électronique 16
2.5. LES FORMALITÉS COMPLÉMENTAIRES 19

3. **PARTIE II- LA PROBLÉMATIQUE DE L'ÉCHANGE ÉLECTRONIQUE 19**

3.5. LA PROBLÉMATIQUE JURIDIQUE DE L'ÉCHANGE D'ÉCRITS ENTRE ABSENTS 19
3.6. LE CADRE LÉGAL DE L'ÉCHANGE ÉLECTRONIQUE DE L'ARTICLE 4 DE LA LOI MADELIN 20
3.2.1. Le cadre légal 20
3.2.2. La pratique administrative 21
3.2.2.1. Le cadre conventionnel 21
3.2.2.2. La transmission multimodale 22
3.7. LES EXIGENCES LÉGALES À CONSIDÉRER 23
3.3.1. La question de la lisibilité 24
3.3.2. La question de la fiabilité 24
3.3.3. La question de la confidentialité 25
3.3.4. La question de l'horodatage 25
3.3.4.1. La question juridique 25
3.3.4.2. La solution technologique : la certification de l'horodatage 27
3.8. LES SOLUTIONS TECHNIQUES 29
3.4.1. La solution aux besoins d'authentification et d'intégrité 29
3.4.1.1. A la recherche d'une solution 29
3.4.1.2. L'emploi d'une signature électronique 30
3.4.1.3. Une signature numérique dans les téléprocédures 31
3.4.1.4. Les certificats référencés 32
3.4.2. L'assurance d'un bon acheminement 33
3.4.2.1. Vers le recommandé électronique 33
3.4.2.2. Vers l'accusé de réception administratif 34

3 SYNTHÈSE 35

AVERTISSEMENT :

La présente note est issue du dédoublement de la note DOC_11.
Le thème de la dématérialisation documentaire a été traité pour le Commerce Electronique dans le

DOC_11 version 2, tandis que le présent document DOC_23 envisage la dématérialisation dans les téléprocédures.

1 INTRODUCTION - LA PROBLEMATIQUE DE LA DEMATERIALISATION DES TELEPROCEDURES ET LES SOLUTIONS

Ce document traite d'une question juridique fondamentale[1] : l'écrit et son devenir dans un monde transformé par les télécommunications. Le grand public découvre aujourd'hui avec Internet et le Web un problème juridique fondamental : la dématérialisation de l'écrit. L'écrit disparaît avec les messages électroniques sur Internet et les autres services télématiques. Aussi tout utilisateur connaît-il de graves difficultés pour accepter la validité juridique de la dématérialisation. Et s'il l'accepte, il ne sait plus comment en apporter la preuve.

Cette problématique juridique a fait l'objet de nombreuses études, en particulier à la Commission de Bruxelles dans le cadre d'une autre technologie, l'EDI[2]. Depuis les années 1980, les études sur l'EDI ont en effet montré que la problématique juridique était double :

- Les données qui se substituent aux documents écrits.
- L'échange électronique.

Ce document expose les deux aspects de la problématique juridique de la dématérialisation des déclarations administratives qui donne naissance aux téléprocédures. Pour chacun des aspects, les éléments de solutions seront précisés.

La dématérialisation des téléprocédures et les solutions

Déjà annoncées par les télécommunications traditionnelles, les échanges électroniques sont en plein développement avec l'émergence d'Internet. L'expression "*échanges électroniques*" est ambiguë puis qu'elle désigne à la fois ce qui est échangé et la modalité électronique de l'échange. Ainsi l'écrit (autrefois sur papier) est transformé en une forme électronique elle-même véhiculée par un vecteur de télécommunications.

Il est aisément perçu la fragilité de cette forme électronique qui voyage sur un média électronique sans une "enveloppe" de protection. Tout incident technique, toute pollution électronique occasionnera une "déformation" du message échangé, ce qui se traduira à terme par une impossibilité d'administrer la preuve : le message reçu ne sera plus identique au message échangé. Si le message n'est pas altéré pendant l'échange, le média utilisé doit être suffisamment fiable pour que l'origine du message puisse être déterminée avec précision. Cette condition est encore indispensable pour le droit en terme de preuve. Tout élément de preuve est nécessairement issu de celui à qui on l'oppose. La question est particulièrement cruciale dans le monde Internet où les protocoles de transport employés ne donnent pas de garanties sur l'origine des messages.

La dématérialisation entraîne bien un problème de preuve, c'est le premier aspect de la problématique juridique. Encore faudrait-il que la forme électronique initiale soit permise c'est-à-dire qu'on ait pu s'exonérer de l'écrit-papier pour passer, selon les termes des études juridiques de la CNUDCI, à un *équivalent fonctionnel* licite, la

[1] Ceci est la 6ème évolution d'un papier de recherche que l'auteur a produit sur la problématique juridique relative à la dématérialisation documentaire dans les échanges électroniques et sur les éléments de solutions envisageables. Des diverses études juridiques qu'il a menées dans l'EDI, une première contribution avait été intégrée dans l'ouvrage collectif "*l'EDI pour les contrôleurs et les vérificateurs*" (Edition des Comptables Agréés canadiens, Montréal, 1992 et 1994). Une seconde version augmentée et intitulée "*La sécurité au secours du droit*" avait été préparée pour être soumis au Groupe des Rapporteurs Juridiques du comité EDI des Nations-Unies (U/TRADE/ECE/WP4). Le texte est repris dans l'article "*Un nouveau dispositif de preuve pour l'EDI basé sur la sécurité*", Expertises des systèmes d'information, mai 1994 p.187 et suiv. Cette vision a ensuite été soutenue à la Conférence d'août 1995 "Faire des affaires en toute sécurité sur les autoroutes de l'information" à Montréal (Canada) dans l'exposé "*Sécurité technique et sécurité juridique sur les autoroutes de l'information*". Une quatrième évolution prenant acte de l'émergence d'Internet et de la préparation de la Directive Signature Electronique a fait l'objet d'une conférence à la Faculté de Droit de Lisbonne en mai 1999. En 2001, le thème a été exposé en octobre au CIMRE (Conférence sur le Management des réseaux d'entreprise) de Mahdia (Tunisie), puis à Buenos-Aires (Argentine) à CLA'2001 (Computer Law Association d'Amérique latine).

2 Cf. sur les aspects juridiques de l'EDI en général, notre ouvrage "*L'EDI et le Droit*", Editions Hermès, septembre 1991, collection A. Bensoussan.

forme électronique. Le passage de la forme papier à la forme électronique constitue le second aspect de la problématique juridique.

La problématique juridique en matière de téléprocédures est identique à celle qui s'ouvre pour les actes sous-seing privés dans le domaine civil et commercial. Les nouvelles solutions nées avec la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique sont applicables aux téléprocédures. Chacun des deux aspects de la problématique juridique, la dématérialisation documentaire et l'échange électronique, se décline en une série de questions standards et auxquelles nous nous efforcerons d'apporter une réponse.

2 PARTIE I- LA PROBLEMATIQUE DE LA DEMATERIALISATION DOCUMENTAIRE

Dans l'EDI comme dans la messagerie électronique sur Internet ou sur le WEB, la disparition de l'écrit constitue une grande difficulté. De nombreuses années durant, les juristes expliquaient habituellement que sans un écrit sur papier, il n'était pas possible d'apporter la preuve en cas de litige en justice. Pourtant la question n'est pas aussi importante dans le droit commercial où la liberté des partenaires en affaires est grande en ce qui concerne l'administration de la preuve. Il y a cependant une autre difficulté à régler avant la question de la preuve : celle du formalisme juridique[3].

2.1 La dématérialisation, atteinte au formalisme juridique

Le formalisme juridique[4] s'intéresse à la forme et aux formalités obligatoires pour créer les actes juridiques et leur donner une force juridique. Le formalisme juridique est plus important dans les pays de droit civil que dans les pays de *common law*[5]. Pour prendre un exemple parmi les plus flagrants, une loi peut exiger qu'un document particulier soit écrit sur un papier. Dans ce cas, message électronique ou fichier électronique, rien ne peut remplacer le document écrit. Il est alors inutile de chercher comment apporter la preuve puisqu'il faute d'écrit sur papier il est soit nul soit inexistant !

2.1.1. Rappel sur la notion de formalisme juridique

2.1.1.1 Le concept de formalisme juridique

Le concept de formalisme juridique[6] englobe toutes les règles de forme et toutes les formalités nécessaires à la formation d'un acte. Traditionnellement les auteurs distinguent plusieurs catégories de formalisme, selon la finalité poursuivie :

- La validité des actes : la Loi prescrit certaines formalités comme la rédaction d'un écrit, la présence d'une signature, de mentions obligatoires, voire même la présence ou la rédaction par un officier ministériel (acte solennel). L'objectif est de protéger les parties, d'attirer leur attention sur la rédaction et la formalisation du texte pour éviter les ambiguïtés. Le non respect du formalisme entraîne la nullité de l'acte.
- La préconstitution de la preuve : la rédaction de l'acte sur un papier, par exemple, doit permettre de faciliter l'administration de la preuve. Ce type de formalisme se traduit par la nécessité d'un écrit-papier mais également de mentions obligatoires ou de la datation. La violation de ce formalisme entraîne l'impossibilité de produire l'acte aux fins de preuve.
- La publicité des actes : Cette formalité est nécessaire afin de pouvoir opposer l'acte aux tiers (exemple : les hypothèques ou les notifications à l'administration fiscale, à l'INPI pour les cessions de brevets, etc.). A défaut, l'acte est inopposable aux tiers.

---

3 Pour une analyse en profondeur du formalisme juridique, cf. notre article "*La véritable problématique juridique de l'EDI : le formalisme avant la preuve*", Cahier du LAMY droit de l'informatique de décembre 90 et janvier 91.

4 La notion de *formalisme* s'oppose à celle de *consensualisme* où au contraire, la volonté de l'auteur de l'acte ou des parties est suffisante valider l'instrument juridique porteur de l'acte.

5 Se dit du système juridique des pays anglo-saxons qui résulte non de textes législatifs mais de la pratique des juridictions (Lexique des termes juridiques, 13ème édition, Dalloz).

6 Pour une étude et des commentaires consacrés au concept même de formalisme, voir Association Henri Capitant, "*Journée Jacques Flour sur le formalisme*", *Rép. Defrénois*, 2000, pp. 865-943 ; P. BRASSEUR, "Le formalisme dans la formation des contrats. Approche de droit comparé", in *Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen*, Bruxelles, Bruylant et Paris, L.G.D.J., 2002, pp. 605-691 ; J. FLOUR. "Quelques remarques sur l'évolution du formalisme", in *Le droit privé français au milieu du XX e siècle. Etudes offertes à Georges Ripert*, Paris, L.G.D.J., 1950, t. I, pp. 93-114 ; F. GENY, *Science et technique en droit privé positif*, t. III, Paris, Sirey, 1921, pp. 94-122 ; M.-A. GUERRIERO, *L'acte juridique solennel*, Paris, L.G.D.J., 1975 ; X. LAGARDE, "Observations critiques sur la renaissance du formalisme", *J.C.P., G.*, I 170, pp. 1767-1775 ; B. NUYTEN et L. LESAGE, "Formation des contrats : regards sur les notions de consensualisme et de formalisme", *Rép. Defrénois*, 1998, pp. 497-509 ; M. PLANIOL, G. RIPERT et P. EISMEIN, *Traité pratique de droit civil français*, t. VI, *Obligations*, *op. cit.*, pp. 125-135.

- Les raisons fiscales : il s'agit, par exemple, de porter l'acte à l'enregistrement de l'administration avec ou sans obligation de régler une taxe (droit de timbre). Selon le type d'acte, le défaut d'enregistrement ou de timbre se traduit par une nullité ou entraîne une sanction fiscale ou pénale
- Le but informatif : la Loi détermine que certains actes doivent être portés à la connaissance de l'administration (déclaration, notification, immatriculation, inscription, agrément). Les conséquences de la violation de ce formalisme sont très diverses. Elles peuvent comporter des sanctions administratives ou pénales.

Les textes légaux et réglementaires qui établissent des règles de forme n'indiquent pas toujours pour quels motifs, les formalités sont imposés (saut à vérifier dans les motifs du projet de loi). Une même formalité peut d'ailleurs répondre à plusieurs de ces finalités.

2.1.1.2. Le formalisme juridique appliqué aux documents

Le formalisme juridique appliqué au document ou formalisme documentaire comporte principalement les trois éléments suivants : l'écrit, la signature, des mentions obligatoires. Dans le monde du papier, signature et mentions obligatoires arrivent généralement en complément de l'écrit : on n'est sûr de l'existence des mentions obligatoires dans un document que … s'il adopte un support papier !

Traditionnellement, on observe trois familles de documents en fonction du degré d'exigence d'un environnement papier traditionnel :

- 1ère catégorie : les documents sans formalisme sont ceux qui ne sont pas cités par les textes juridiques, mais qui peuvent être très fréquents à cause des usages du commerce. Il y a aussi les documents connus ou cités par les textes sans autre précision. Ces documents bénéficient de la liberté la plus complète dans leur formation, leur forme, leur présentation. Il est souvent possible de les dématérialiser immédiatement.
- 2ème catégorie : les documents à formalisme variable sont très divers et éparpillés dans de nombreux textes. Les éléments du formalisme sont alors variables et hétérogènes : support papier, mentions obligatoires, titre, signature... Une analyse juridique fine est nécessaire pour vérifier s'il est possible de les reclasser dans la catégorie supérieure ou inférieure.
- 3ème catégorie : les documents très formalistes. Les textes décrivent avec précision les obligations qui président à leur création. Par exemple, l'obligation d'un support papier. A défaut, le document n'existe pas juridiquement. Ces documents sont impossibles à dématérialiser si le droit n'évolue pas.

Cette analyse trouve son application la plus large en droit commercial. Par contre le droit administratif est caractérisé par une relation de force entre l'administration et l'administré qui penche en faveur de l'administration. D'autre part, il est également nécessaire de sauvegarder les droits de l'administration. Aussi ne s'étonnera-t-on pas de constater que le formalisme est tout particulièrement rigide dans ce domaine où le papier est un support constant pour de nombreux actes administratifs.

Le formalisme documentaire doit être satisfait dans le monde électronique, comme dans le monde de l'écrit. Le formalisme étant le domaine de la rigueur, avec quelle rigueur transposer le formalisme juridique du papier à l'électronique ? Comme l'affirme un auteur[7], *"Formalisme ne signifie pas forme compliquée, mais forme impérative, c'est-à-dire imposée, sans équivalent possible (…)"*. A cet égard, l'application du formalisme juridique nécessite de définir une stratégie de travail : puisqu'il ne peut être question de contourner le formalisme juridique, comment le respecter dans le contexte des téléprocédures ?

Comme souvent en Droit, le choix est binaire et une option contraire existe sous la forme de deux atténuations à la rigueur pour ne pas dire au rigorisme du formalisme juridique :

- La pratique jurisprudentielle française : faute de précision explicite, la jurisprudence avait tendance à considérer que la formalité n'était pas requise à peine de nullité (ad validitatem) mais à titre de preuve (ad probationem), mettant quelquefois à mal l'intention du législateur soucieux de protéger les parties. Cette pratique des années 1950[8] s'est en grande partie inversée actuellement où le juge est plus proche du législateur[9].

[7] J. FLOUR, "Quelques remarques sur l'évolution du formalisme", in *Le droit privé français au milieu du Xxème siècle. Etudes offertes à Georges Ripe*rt, Paris, L.G.D.J., 1950, t. I, p. 101, n° 9.

[8] Cf. J. FLOUR, article précité.

[9] Cf. X. LAGARDE, G. COUTURIER, articles précités et TERRE, P. SIMLER et Y. LEQUETTE, *Droit civil. Les obligation*s, Paris, Dalloz, 1996, 6 e éd., pp. 117-120, n°138. 104 J.P. Renaix, 26 sept. 2000, *D.C.C.R.*, 2001, p. 283, *D.A./O.R.*, 2001, p. 179 ; *Ann. jur. créd.*, 2000, p. 101.

- Les travaux de la CNUDCI : à l'occasion de l'adoption de la Loi Modèle pour le Commerce Electronique, la Commission des Nations Unies pour le droit commecriao international (CNUDCI) a développé la théorie de l'*équivalent fonctionnel*. Il s'agit moins de rester sur une position rigide mais d'identifier les fonctions qui sont assignées aux formalités et de leur trouver un substitut dans le monde électronique. Des formalités électroniques prendraient alors le relais des formalités traditionnelles autour de l'écrit-papier[10]. Cependant peu (pas ?) de textes fondateurs du droit positif français s'inspire de cette théorie.

Aussi sommes-nous restés dans une position de stricte orthodoxie. Comme l'a exprimé un auteur, "*la règle de forme, par définition, exclut le recours à des procédés équipollents : on ne peut échapper à son application en prétendant que le résultat attendu de la règle a été atteint par une autre moyen que la formalité prescrite*"[11].

2.1.2. Les déclarations administratives et le formalisme juridique

Le papier est le support privilégié des déclarations administratives que les particuliers et les entreprises produisent aux services administratifs. Le formalisme est même maximal lorsqu'il prend la forme d'un formulaire préalablement préparé par l'administration et quelquefois pré-renseigné.

2.1.2.1. Notion de formulaire administratif

Le formulaire administratif est un moyen de respecter un des grands principes du droit public français, l'égalité de tous devant les services publics, qui peut se décliner également sous la forme du principe de l'égalité de traitement. Les obligations déclaratives qui forment la base réglementaire des téléprocédures comme des déclarations papier sont remplies en première étape par le biais d'un document papier identique pour tous les assujettis. Le terme de "formulaire administratif" doit être entendu de façon large puisque selon la *Circulaire du 31 décembre 1999 relative à l'aide aux démarches administratives sur l'internet*[12], il recouvre "*l'ensemble que constituent une grille de demande d'informations, une notice explicative et la liste limitative des pièces justificatives à présenter*".

Le formulaire administratif préparé par l'administration considérée fait l'objet d'une validation globale par un organisme spécialisé, le CERFA, aujourd'hui la COSA[13], qui vérifie son homogénéité par rapport à d'autres formulaires administratifs de nature connexe. Le formulaire porte un numéro d'identification propre à l'administration d'origine et un numéro de matricule délivré par le Cerfa.

2.1.2.2. La diffusion du formulaire administratif, du papier à l'électronique

Le formulaire est disponible auprès de l'administration créatrice en ses bureaux ou par courrier. A signaler également comme très fréquents dans les téléprocédures, les formulaires pré-renseignés par l'administration qui mentionnent le nom et l'adresse de l'assujetti, le service administratif de rattachement et d'autres indications diverses comme la période considérée pour la déclaration et la date limite de paiement, par exemple.

Internet constitue un moyen récent de diffusion des formulaires. Il s'agit cette fois que l'assujetti ou le déclarant récupère le formulaire en ligne et en réalise une copie papier sur son imprimante avant de le remplir comme il se doit. Cette nouvelle pratique est encouragée par le gouvernement qui y voit comme une marque du développement de l'administration en ligne et le moyen d'une meilleure accessibilité pour le public. Le *Décret n°99-68 du 2 février 1999 relatif à la mise en ligne des formulaires administratifs*[14] prévoit que les formulaires dont l'usage est nécessaire pour accomplir une démarche auprès d'une administration ou d'un établissement

---

[10] Voir DEMOULIN M., "*Le traitement des obstacles formels aux contrats en ligne - Recommandations relatives à la mise en œuvre de l'article 17 du projet de loi sur certains aspects juridiques des services de la société de l'information*", avec la collaboration et sous la direction du professeur Etienne MONTERO, 15 octobre 2002.CRID-FUNDP.

[11] G. COUTURIER, "*Les finalités et les sanctions du formalisme*", Rép. Defrénois, 2000, pp. 885-888.

[12] J.O. Numéro 5 du 7 janvier 2000 page 279

[13] La Commission pour les simplifications administratives, présidée par le Premier ministre, a été créée par le décret n° 98-1083 du 2 Décembre 1998 (JO du 3 Décembre 1998), modifié par le décret 2001-452 du 25 mai 2001 (JO du 29 mai 2001). Elle succède à la Commission pour la simplification des formalités (COSIFORM) et au CERFA. C'est une instance d'étude, d'impulsion et de suivi en matière de simplifications administratives. Elle assure, notamment, la mission d'homologation et de révision des formulaires administratifs précédemment dévolue au CERFA, ainsi que leur mise en ligne au service des usagers.

[14] J.O. Numéro 29 du 4 février 1999 page 1775 - Voir l'article 1 du Décret.

public administratif de l'Etat soient tenus gratuitement à la disposition du public, sous forme numérique, par divers sites d'information administrative du public accessibles sur le réseau Internet[15].

La *Circulaire du Premier Ministre du 7 octobre 1999 relative aux sites internet des services et des établissements publics de l'Etat*[16] est venue apporter les précisions nécessaires. Les formulaires disponibles en ligne doivent être identiques, dans leur contenu, aux formulaires sur support papier enregistrés et répertoriés par la commission pour les simplifications administratives (COSA), conformément aux dispositions du *Décret no 98-1083 du 2 décembre 1998 relatif aux simplifications administratives*. Comme le Décret en avait fixé le principe, les sites administratifs de téléchargement[17] doivent mentionner l'avertissement spécifique suivant : "*Les administrations et établissements publics administratifs de l'Etat ne peuvent refuser d'examiner les demandes présentées au moyen de formulaires imprimés à partir des données disponibles sur ce site, dès lors qu'il s'agit d'un formulaire dûment renseigné et n'ayant fait l'objet d'aucune altération par rapport aux données figurant sur le site*".

Un organisme spécifique, la COSA, a pour mission d'enregistrer et de réviser les formulaires administratifs et de les référencer sur le site central de téléchargement de l'administration. Elle tient à la disposition des usagers la liste exhaustive des formulaires et des services interactifs d'aide aux démarches administratives diffusés sur les sites publics.

Chaque ministère est responsable de la création, de la mise à jour et de la diffusion des formulaires nécessaires à la réalisation des démarches qui relèvent de son domaine de compétence. Il lui appartient donc de diffuser ceux-ci sur son site national. Si un ministère ne les diffuse pas ou jusqu'à ce qu'il les diffuse, la COSA peut mettre en ligne les formulaires préalablement enregistrés par elle. De leur côté, les services déconcentrés peuvent mettre en ligne des formulaires dans le cas où il n'en existerait pas au niveau national, ou lorsque ceux-ci concernent des procédures soumises à des règles locales. Les formulaires diffusés localement devront, par application des dispositions précitées du décret du 2 février 1999, être acceptés par les services déconcentrés de l'ensemble du territoire national (habilitation particulière du Premier ministre).

2.1.2.3. La pratique administrative des formulaires

L'étude de la pratique de quelques déclarations susceptibles de donner naissance à une téléprocédure permet d'illustrer les difficultés de régler la question de la dématérialisation documentaire face au maquis des textes réglementaires qui régissent ces obligations déclaratives dans le monde du papier.

Exemple de la Déclaration Unifié d'Embauche - L'embauche d'un employé par une entreprise est l'occasion de déclarations administratives auprès d'organismes variés des sphères administratives et sociales. Mais une initiative simplificatrice existe avec la Déclaration Unifié d'embauche (DUE)[18] qui est mise en application depuis le milieu des années 1990. En matière de DUE, la déclaration est effectuée sur un formulaire spécifique qui a été standardisé par le CERFA. Ce formulaire est disponible auprès de divers organismes administratifs, notamment les URSSAF et peut être téléchargé sur le portail gouvernemental http://www.service-public.fr.

[15] Cf. Les sites Admifrance ou Service Public

[16] J.O. Numéro 237 du 12 octobre 1999 page 15167

[17] Ces sites sont référencés sur une liste publiée par un arrêté du Premier ministre (art.2 du Décret précité).

[18] L'embauche d'un employé par une entreprise doit faire l'objet d'une formalité déclarative prévue par l'article L.320 du Code de travail : "*L'embauche d'un salarié ne peut intervenir qu'après déclaration nominative effectuée par l'employeur auprès des organismes de protection sociale désignés à cet effet dans les conditions fixées par un décret en Conseil d'Etat*". A côté de ce document déclaratif découlant du Code du Travail, certaines circonstances de l'embauche réclament l'émission d'autres déclarations ou demandes. Aussi la loi n°94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle (Loi Madelin) a-t-elle posé un principe de simplification administrative dans son article 32-I. qui dispose : "*Les données relatives aux rémunérations ou gains et aux effectifs, que les employeurs sont tenus de transmettre aux organismes gérant des régimes de protection sociale relevant du Code de la Sécurité Sociale et du Code Rural ou visés aux articles L.223-16 et L.351-21 du Code du Travail, font l'objet d'une seule déclaration établie sur un support unique et adressée à un seul destinataire*". La DUE est née du croisement de ces deux textes. Conçue dans un rôle de simplification, la DUE permet à l'aide d'un seul document d'accomplir 9 formalités différentes auprès d'autant organismes administratifs ou parapublics. La DUE est émise vers une URSSAF qui la redirige vers les organismes concernés.

2.2 La présence de mentions obligatoires

Dans le formalisme juridique appliquée aux documents sur papier, la hiérarchie des éléments formalistes est du type support écrit, puis apposition d'une signature et enfin, mentions obligatoires. Les mêmes éléments sont à envisager dans une vision électronique du formalisme qui ne retranche rien à la rigueur traditionnelle. Pour la commodité, de l'analyse qui a tout d'une démonstration, les éléments seront étudiés dans l'ordre inverse.

2.2.1. Présence des mentions obligatoires

La présence de mentions obligatoires sur une déclaration électronique répondent au principe du parallélisme des formes : les mentions (obligatoires) figurant sur le support papier doivent être reprises par le support électronique

Pour déterminer quelles sont les mentions obligatoires à porter, il faut examiner document par document quelles sont les mentions obligatoires et aussi quelles sont les sanctions de leur absence. Cependant les exigences des textes légaux et réglementaires sont très variées, puisque l'administration pour des besoins de suivi de l'activité économique, de la vie sociale et des procédures fiscales a besoin de nombreuses informations.

L'existence d'un formulaire "cerfaté" préexistant est une garantie que les mentions légales et réglementaires sont présentes.

Exemple de la DUE - En ce qui concerne la DUE, toute déclaration d'embauche comporte comme le prévoit l'article R.320-2 les mentions suivantes :

- *Dénomination sociale ou nom et prénoms de l'employeur, code APE ou code NAF s'il a été attribué, adresse de l'employeur, numéro du système d'identification du répertoire des entreprises et de leurs établissements ou numéro sous lequel les cotisations de sécurité sociale sont versées,*
- *Nom patronymique, prénoms, nationalité, date et lieu de naissance du salarié ainsi que son numéro national d'identification s'il est déjà immatriculé à la sécurité sociale.*
- *Date et heure d'embauche.*
- *Pour les employeurs dont les salariés relèvent du régime agricole, nature et durée du contrat."*

Ces mentions sont reprises dans les formulaires papier et électroniques.

2.2.2. Forme des mentions

Lors du passage d'un formulaire papier à un formulaire électronique, les mentions doivent rester constantes ; elles seront logiquement de nature électronique. C'est une question de bon sens qui sera fondé en droit lors de l'adoption de la Loi sur l'Economie Numérique (LEN). Le formalisme des mentions obligatoires sera en effet impacté, quoique marginalement, par la transposition en droit interne de la Directive Commerce Electronique[19]. Cette directive devait être transposée en droit interne par la Loi sur la Société de l'Information (LSI). Les changements politiques que la France a connu ces dernières années ont entravé la procédure parlementaire et ajourné l'adoption de la LSI. Cependant les Pouvoirs publics ont annoncé leur volonté d'aboutir prochainement. Le gouvernement a annoncé à la mi-novembre 2002 son intention de mettre rapidement un terme à l'enlisement des chantiers législatifs relatifs à la société de l'information. La LSI est remplacée par une *Loi sur la confiance dans l'Economie Numérique* (LEN) qui transpose la Directive européenne commerce électronique ainsi qu'une partie de la Directive protection des données personnelles. Parmi les objectifs retenus par le projet de loi figure "*l'amélioration de la sécurité dans l'économie numérique*". A ce titre, selon les termes du Premier Ministre, "*l'un des moyens d'augmenter la sécurité, et donc la confiance, est l'utilisation de moyens de cryptographie qui permettent d'assurer des fonctions de signature électronique sécurisée, d'intégrité et de confidentialité des échanges. Ce projet de loi procède à la libéralisation complète de l'utilisation de la cryptologie, attendu de longue date, tout en s'accompagnant des mesures nécessaires pour lutter contre l'utilisation à des fins criminelles de cet outil*".

[19] 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).

Le projet de *Loi relative à la confiance dans l'économie numérique* adopté par le Conseil des ministres le 15 janvier 2003 est en cours de vote devant le Parlement. L'Assemblée Nationale a, pour sa part, adopté après amendement le projet de loi qui inclurait un article 1108-1 ainsi rédigé dans un alinéa 2 sur les mentions[20] :

> "*Lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir que la mention ne peut émaner que de lui-même.*"

En ce qui concerne les téléprocédures, il est possible de dénier l'application immédiate de cette prochaine disposition du Code Civil. Mais sa valeur d'exemplarité est notable. Il sera sans doute facile à établir que les mentions obligatoires sont présentes si la forme électronique de substitution est de type formulaire avec un rubriquage préalablement vérifié. Surtout si sa présence peut être attestée par une signature électronique.

2.3 L'exigence de signature

De nombreux documents demandent l'apposition d'une signature par laquelle son auteur laisse une marque personnelle sur le document et par laquelle il manifeste son accord sur le contenu et se l'approprie.

La question du respect du formalisme documentaire appliqué à la signature se suffit du principe du parallélisme des formes : si une signature autographe accompagne un acte, l'acte électronique devrait comporter une signature électronique.

2.3.1. Le dispositif juridique de la signature électronique

La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique apporte d'importantes modifications au Code Civil en ce qui concerne la notion de signature et l'écrit pour preuve (Cf. INFRA). Pour la première fois, le Code Civil dans l'article 1316-4 énonce une définition de la signature dont on peut tirer deux caractéristiques présentées par toutes les signatures : la signature identifie le signataire et manifeste son consentement au contenu du document signé.

Article 1316-4. - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte (...)

Cette définition est valable pour tous types de signature. Par analogie avec l'écrit défini dans un autre article de la loi, la signature, jusqu'ici uniquement manuscrite, pourra adopter la modalité électronique. La signature électronique répondra naturellement à la même définition mais des précisions sont apportées sur la façon dont elle est réalisée. En effet, toute signature répond ainsi pour sa création à un véritable processus. Si la signature manuscrite est le résultat d'un procédé manuel, qui n'a généralement pas besoin d'être organisé, la signature électronique est produite par un procédé informatique d'identification fiable.

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. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.

Le procédé doit présenter un lien avec l'acte auquel la signature s'attache. Cette précision est inutile dans le cas de la signature manuscrite dont on dit qu'elle est apposée sur le support papier. Mais l'électronique ne possède pas de support, c'est seulement une forme. Aussi la signature électronique doit donner une assurance qu'elle correspond bien à un message électronique déterminé. D'où l'idée du lien puisque de plus, la signature électronique peut voyager indépendamment des données concernées. Mais surtout le procédé technique doit être fiable. Les éléments qui concourront à cette fiabilité sont déterminés par le décret d'application[21] en Conseil d'Etat. La loi liste certains des points à couvrir : création de la signature, assurance de l'identité du signataire et garantie de l'intégrité.

[20] Il reste à attendre la validation de l'article 1108-1 dans les mêmes termes par le Sénat qui devrait procéder à l'examen de la loi et à son adoption en juin 2003.

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

Autre point à signaler, le respect des exigences formulées par le décret en Conseil d'Etat ne permet que de conférer une "présomption" de fiabilité au procédé. En effet, dans tous les cas, il sera nécessaire d'être en mesure de démontrer que le procédé technique est fiable :

- Si les exigences du décret sont respectées (et constatées par une "qualification"), il y a aura présomption simple c.a.d. pas de charge de la preuve, mais seulement jusqu'à preuve contraire,
- Si les exigences du décret ne sont pas respectées, les utilisateurs devront supporter la charge de la preuve en cas de contestation et se préparer à démontrer par tout moyen la fiabilité du procédé.

2.3.2. Le dispositif technique de la signature électronique

Il existait (et il existe toujours) une réalité de la "signature électronique technologique" avant même que les juristes ne s'y intéressent. Une variété de signature technologique mettant en œuvre des mesures cryptographiques est généralement qualifiée de "*signature numérique*" (*Digital signature* en anglais). La loi française en application de la directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques lui a donné une reconnaissance juridique : la signature numérique des techniciens s'est vue imposer par le droit des exigences techniques et juridiques pour devenir une signature électronique sécurisée.

La signature électronique se présente sous une forme numérique qui est fonction, à la fois, de l'identité du signataire mais encore du contenu du document signé. Instrument de sécurité, elle présente les caractéristiques suivantes :

- elle met en œuvre des moyens cryptographiques (clé privée et clé publique)...
- attestés par un prestataire de services spécialisé (le prestataire de service de certification électronique)…
- au moyen d'un message électronique spécialisé appelé "certificat".

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 explicite les termes de l'article qui annonce les conditions dans lesquelles "la fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie". La signature qui respecte les impératifs techniques du Décret prend le nom de signature électronique sécurisée (SES). Seul ce type de signature permet de bénéficier de la présomption de fiabilité instaurée par le Code Civil, ce qui lui permet de jouer sur un message électronique le même rôle qu'une signature manuscrite sur papier.

Les composants de la signature électronique sont les suivants :

- La signature électronique est générée par un logiciel qui prend le nom de "Dispositif de création de signature" (DCS),
- La signature électronique dans le message arrivé à destination doit être vérifiée par un logiciel appelé "Dispositif de vérification de signature" (DVS).
- Le DVS doit disposer de certaines informations (la clé publique du signataire) contenue dans un certificat électronique.
- Le certificat électronique est préparé, vérifié et diffusé par un Prestataire de Services de Certification Electronique (PSC).
- Le décret impose à chacun de ces composants un supplément de rigueur et de précision par rapport à l'utilisation purement technique de la signature. La SES comprend un DCS sécurisé et met en œuvre un certificat électronique qualifié délivré par un PSC également qualifié :

S.E.S. = Dispositif SECURISE de création de signature + certificat électronique QUALIFIE	
⇓	⇓
le DCS est sécurisé si :	Le certificat est QUALIFIE si
1) Exigences techniques remplies	1) certificat conforme
2) Certification du DCS	2) un PSC QUALIFIE

La difficulté est grande pour les utilisateurs de juger par eux-mêmes de la conformité des spécifications techniques aux exigences réglementaires. Aussi le décret établit-il des systèmes de contrôles sanctionnés par divers agréments :

- Pour se présenter comme "sécurisé", un DCS doit respecter les exigences techniques de l'article 5.-I et se faire contrôler et certifier par les services spécialisés du Premier Ministre (la DCSSI) (art. 5.-II).

- Pour se présenter comme "qualifié", un certificat doit être conforme aux prescriptions de l'article 6.-I. Le certificat est émis par un PSC qui répond quant à son organisation et son fonctionnement aux stipulations de l'article 6.-II.
- En cas de doute ou d'incertitude sur la qualification du certificat, l'utilisateur pourra se tourner vers la DCSSI qui auditera certificats et prestataire et en rendra publics les résultats (art. 9).
- Les PSC pourront faire constater l'excellence de leurs prestations en sollicitant une qualification de leur activité auprès du Ministre chargé de l'Industrie (art. 7).
- Les Dispositifs de vérification de signature, qui doivent être compatibles avec les DCS pourront être évalués par la DCSSI, s'ils répondent aux exigences de l'article 5.

Selon certains juristes, ces dispositions ne seraient pas applicables à l'administration. A cela, il faut répondre en deux branches :
- Il incombe à l'administration de faire le choix de la signature électronique à finalité juridique qu'elle veut voir employer par ses agents. Mais il faudrait que la signature électronique des agents et des autorités administratives présente des attributs juridiques originaux et différents de ceux de la signature traditionnelle, en un mot, *exorbitants du droit commun* pour que répondant à son critère général, le droit administratif instaure une signature électronique différente[22].
- Les téléprocédures dont il s'agit sont émises par les particuliers et les entreprises en direction de l'administration. Ces émetteurs n'ont à leur disposition que les signatures du Code civil.

2.3.4. Le sens de la signature des télédéclarations

Selon le Code civil, la signature sert à rendre parfait un acte sous-seing privé. Le signataire consent aux obligations contenues dans l'acte. La situation de la signature d'une téléprocédure répond-elle a ce schéma ? Si non, quelle est le sens de cette signature ?

2.3.4.1. Un consentement donné aux obligations ou au contenu

Selon l'article 1316- du Code civil, *"la signature manifeste le consentement des parties aux obligations qui découlent de cet acte"*. Classiquement la doctrine[23] et la jurisprudence, à une époque où le Code ne définissait pas la notion de signature, affirmaient que la signature est une marque personnelle de l'auteur du texte. Ce qui 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 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[24]. L'article 1316-4 précise qu'il s'agit d'obligations. Une obligation se définit comme "*un lien de droit entre deux ou plusieurs personnes en vertu duquel l'un des parties, le créancier de l'obligation peut contraindre l'autre, le débiteur de l'obligation, à exécuter une prestation (obligation de donner, obligation de faire ou de ne pas faire)*"[25]. 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.

---

[22] La Directive européenne Signature électronique n'ignore pas la spécificité du monde administratif lorsqu'elle déclare dans sont article 3.7. : "*Les Etats membres peuvent soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée*..."

[23] 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.

[24] Il est ici rappelé qu'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.

[25] Lexique des termes juridiques, 13ème édition, Dalloz, ouvrage précité.

En retenant des obligations consenties comme ressort de la signature, le droit français est assez restrictif. La signature de la Commission des Nations Unies sur le Droit Commercial International (CNUDCI) est d'une application plus large. L'article 2 de la loi type de la CNUDCI sur les signatures électroniques[26]. 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".*

Le document de la CNUDCI relève que sa la Loi type sur le commerce électronique se fonde sur la reconnaissance des fonctions générales remplies par la signature dans un environnement papier, ainsi que ses fonctions particulières selon la nature du document sur lequel elle est apposée :

- identification d'une personne,
- certitude quant à la participation en personne de l'intéressé dans l'acte de signature,
- association de cette personne avec la teneur d'un document,
- intention d'une partie d'être liée par la teneur d'un contrat signé,
- intention d'une personne de revendiquer la paternité d'un texte (montrant ainsi qu'elle a conscience du fait que l'acte de signature peut avoir éventuellement des conséquences juridiques),
- intention d'une personne de s'associer à la teneur d'un document rédigé par quelqu'un d'autre;
- du fait que et du moment où une personne se trouvait en un lieu donné.

A cause du sens donné par les nations du monde à la signature, la définition CNUDCI ne parle que d'*information qui y est contenue.*

Quant à la Directive Signature Electronique, sa première version, la proposition COM(98)297 sur un cadre commun pour les signatures électroniques, exposait que la signature électronique était le concept central et qu'elle se définissait dans l'article 2.1 de la façon suivante :

"*Une signature sous forme numérique intégrée, jointe ou liée logiquement à des données, utilisée par un signataire pour signifier son acceptation du contenu des données*[27]*, et 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 détectée.*"

La version finale de la Directive est pourtant toute différente. De plus, elle comporte deux types de signature électronique. En compilant les 2 définitions, le résultat suivant est visible pour la "*signature électronique avancée."* C'est "*une signature électronique, (c.a.d. une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification) 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 ;"*

Ainsi la signature électronique avancée de la directive a perdu le sens primordial qu'on peut lui donner en droit français : elle ne ratifie pas plus les contenus que les obligations. D'ailleurs, elle abandonne toute velléité d'acceptation de quoi que ce soit ! Elle se cantonne aux aspects sécuritaires de la signature des techniciens.

2.3.4.2. Les enseignements des déclarations existantes

La pratique de la signature dans les déclarations existantes permet d'alimenter la réflexion quant au véritable sens de la signature des déclarations administratives.

---

[26] 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 .

[27] C'est nous qui avons souligné.

En matière de déclaration administrative, nous sommes en présence d'une signature "dégradée". En effet, la déclaration a pour objet de présenter à l'administration un ensemble d'informations ; elle est de nature informative. Sur un autre plan, les formalités déclaratives sont souvent effectuées pour le compte de l'entreprise et par un tiers déclarant qui n'appartient pas toujours à celles-ci (cas de l'expert-comptable). La signature sur une déclaration administrative n'est qu'une marque personnelle au déclarant qui permet d'identifier la source (c'est-à-dire l'entreprise) soit directement (employé de l'entreprise), soit indirectement par le biais du mandataire (expert-comptable). En considérant les caractéristiques de la signature pour une déclaration administrative, la télédéclaration ne nécessite pas une Signature Electronique Sécurisée (SES) du Code Civil, mais une signature numérique.

Exemple de la déclaration de TVA - Un formulaire Cerfa n°2514 K (avis d'acompte de TVA – régime simplifié) doit être signé comme le montre la structure du document. Si la déclaration papier est bien signée, on peut s'interroger sur la dimension juridique de cette signature. Il ne semble pas s'agir d'une signature juridique comme celle de l'article 1316-4 du Code Civil. La question n'est pas, en effet, de consentir à l'obligation de payer la TVA[28] qui découle directement du CGI à partir d'un fait générateur (vente d'une chose ou la réalisation d'une prestation de service) et qui pèse sur une personne physique ou morale assujettie. Tout au plus s'agit-il d'une signature attestant qu'on mène à bien son obligation déclarative (portant en réalité sur les montants de TVA à régler et non sur le principe du paiement de la taxe). Mais cette signature n'atteste de rien, puisque c'est l'administration qui décide que l'obligation de déclarer (et de payer !) a été accomplie.

En fait, chaque entreprise possède un compte TVA à la DGI et la déclaration - règlement permet de l'alimenter. L'important est surtout que celui qui alimente le compte soit identifié. Cette identification est toute relative pour au moins les deux raisons suivantes :

- D'une part, le déclarant n'est pas obligatoirement le représentant de l'entreprise (cas de l'expert-comptable). Il est alors nécessaire d'établir le lien entre le déclarant et l'entreprise[29]. Si on admet que sa signature est bien donnée par délégation de l'entreprise, elle n'a toutefois pas plus d'efficacité que ce qui est dit plus haut.
- D'autre part, on peut noter que généralement les avis d'acomptes sont édités par l'administration et pré-renseignés au nom et à l'adresse du déclarant pour le compte de l'entreprise identifié par son SIRET.

En définitive, la signature portée sur le formulaire papier ne possède pas la valeur d'une signature du Code Civil. Elle permet tout juste une identification de premier niveau du déclarant dont le "rattachement" à l'entreprise assujettie à l'obligation de déclaration est établir par d'autres moyens que la signature. Cette signature est purement formelle et d'habitude.

La signature est bien une marque d'identification ou d'authentification dans la sphère administrative. L'article 95[30] du Code des douanes en donne encore une bonne illustration à propos des déclarations en douane :

> "3. Elles doivent être signés par le déclarant. Celui-ci est la personne qui fait la déclaration en douane en son nom propre ou celle au nom de laquelle une déclaration en douane est faite."

2.3.5. La signature du déclarant

Quoique le thème central de cette note soit la création d'une téléprocédure sous l'angle documentaire, le présent développement sur la signature amène à consacrer quelques paragraphes à la personne du signataire. En plus des spécificités déjà soulignées, la signature d'une téléprocédure comme d'une déclaration papier n'est pas toujours celle de l'*auteur intellectuel*. L'expression auteur intellectuel permet d'identifier celui qui est en puissance de droit et qui en conséquence, est seul apte à signer le document lui conférant ainsi le statut d'acte sous-seing privé. Dans le domaine qui nous intéresse, la déclaration-instrument est le document qui formalise la déclaration-formalité. Pour chaque obligation déclarative, la loi et le règlement précisent à qui la formalité incombe. Mais cette personne n'opère pas toujours par elle-même. En définitive, la déclaration est remplie et/ou signée par un *déclarant*. Aussi est-il utile de vérifier à quel titre un déclarant prétend-il remplir la formalité.

[28] Le fisc refuse-t-il d'encaisser un chèque de paiement si le formulaire papier qu'il accompagne est dépourvu de signature ?

[29] La solution efficace en électronique consisterait plutôt à établir en quelle qualité le déclarant déclare pour le compte de l'entreprise. Le système des *certificats d'attributs* devrait convenir, mais n'est pas encore disponible sur le marché.

[30] Loi nº97-1239 du 29 décembre 1997 finances rectificative art. 26 V Journal Officiel du 30 décembre 1997.

Il est primordial d'effectuer une distinction entre :
- La délégation (qui doit probablement plutôt être une délégation de pouvoirs que de signatures selon les définitions fournies par ce groupe) qui est interne à l'entreprise,
- Le mandat reçu par une personne extérieure à l'entreprise.

La délégation est totalement interne à l'entreprise et s'effectue selon un lien de subordination liant le délégataire (celui qui donne délégation) et le délégué (celui qui reçoit la délégation). Dans les entreprises d'une certaine taille, cette délégation peut être réalisée à plusieurs niveaux ou générations. C'est ce qui avait été qualifié de subdélégation, c'est-à-dire le fait que la personne déléguée délègue à son tour une partie de ses pouvoirs à un sous-délégué. Dans ce type de solution, la seule vérification qui semble possible est l'identité du dirigeant (qu'il soit PDG, DG, Président du Directoire ou Gérant). Il est vrai qu'il faut pouvoir vérifier la limitation des pouvoirs du dirigeant qui pourrait être opposable à un tiers. Or les recherches juridiques montrent que ces limitations de pouvoirs ne sont opposables aux tiers que si elles sont statutaires. Dans la pratique, ces limitations concernent toujours des opérations sortant de l'objet social ou de la gestion courante de la société. En matière de télédéclarations, nous nous trouvons systématiquement dans la gestion courante de la société. Il paraît quasiment impossible qu'une limitation de pouvoirs puisse frapper le dirigeant en matière de télédéclarations.

A partir de là, c'est en toute liberté que le dirigeant pourra décider de tout type de délégation de pouvoirs au sein de son entreprise. Cette délégation restant, bien sûr, sous son entière responsabilité. Des contraintes imposées aux dirigeants, notamment sur la preuve de leurs pouvoirs ou de la délégation octroyée, serait gênante pour l'usager et risquerait de limiter fortement l'adhésion des entreprises aux téléprocédures. D'autant qu'il n'est pas dans les usages de l'entreprise de formaliser systématiquement des relations qui découlent du lien de subordination né lors de la conclusion du contrat de travail. En matière de risque pour l'administration ou les organismes sociaux, cela ne semble pas entraîner de difficulté, puisque pour eux, l'entreprise sera toujours responsable du non-dépôt dans les délais impartis de ses télédéclarations et aura à en assumer toutes les conséquences.

En ce qui concerne le mandat et les mandataires, il faut noter qu'un certain nombre de professions libérales (avocats, commissaires aux comptes, experts-comptables, huissiers, notaires, géomètres, architectes, …) sont chargés de faire un certain nombre de formalités pour des entreprises clientes. Pour ce faire, la loi leur reconnaît tantôt un mandat légal, tantôt un mandat tacite ou express. Dans ce dernier cas, le professionnel devra donc s'assurer de la réception d'un document papier (mandat) émanant de son client.

En matière de risque de contestation de mandat, il est inconcevable qu'un professionnel libéral fasse une déclaration pour un client sans avoir été mandaté par celui-ci. S'il le faisait, il engagerait intégralement sa responsabilité civile et peut-être également pénale. En matière de responsabilité, encore une fois l'administration ou l'organisme social ne connaît que l'entreprise contre laquelle elle se retournera en cas de non-déclaration ou anomalie dans sa déclaration. Cette entreprise sera toujours tenue responsable de ces faits. Par contre, elle aura ensuite toute possibilité de se retourner contre le mandataire auquel elle aurait confié cette mission.

Au total, l'administration et l'organisme social peuvent, en toute légalité, s'appuyer sur *la théorie du mandat apparent***.**

2.4. L'abandon du support papier

La faisabilité d'une téléprocédure se révèle délicate à réaliser lorsque le formalisme juridique impose explicitement, à travers les termes des textes réglementaires, la référence au papier pour la formalité déclarative traditionnelle.

2.4.1. Les bases juridiques de l'abandon de l'écrit-papier

Pour passer de la déclaration papier à la télédéclaration, il faudrait créer un formulaire électronique. A condition, naturellement que la rédaction des textes législatifs et réglementaires ne s'oppose pas à la dématérialisation documentaire, ce qui est plus souvent le cas en droit administratif qu'en droit commun[31].

[31] Cf. notre article "*L'échange de données entre administrations – Quelques réflexions sur l'utilisation de l'écrit*", la Gazette du Palais, doctrine, 15-17 janvier 1995.

L'attachement au support papier n'empêche pas les Pouvoirs Publics de préparer la voie au "e-gouvernement". Le passage du formulaire papier transmis par la poste au formulaire électronique transmis via Internet connaîtra deux étapes intermédiaires :

- l'impression du formulaire papier par l'administré à partir d'un fichier téléchargé sur Internet,
- la transmission par Internet d'un formulaire à remplir directement à l'écran où Echange de Formulaires Informatisés (EFI).

L'aboutissement de la diffusion électronique des formulaires surviendra lorsque le formulaire visible à l'écran pourra être rempli sur le poste informatique. Le Premier ministre a décidé de franchir ce pas et l'a confirmé par la *Circulaire du 31 décembre 1999 relative à l'aide aux démarches administratives sur l'internet*[32]précitée où il indique clairement :"

> "*On ne saurait toutefois s'en tenir aujourd'hui à la seule diffusion de formulaires numérisés. En effet, l'évolution des technologies et le large développement des sites internet des administrations permettent d'offrir au public des services interactifs d'aide à la démarche administrative, voire de véritables téléprocédures*".

La circulaire se termine par une "*Charte de mise en ligne sur des sites internet des services de l'Etat et des établissements publics administratifs de l'Etat de formulaires administratifs et de téléprocédures*" où les administrations sont invitées à mettre en place divers types de services interactifs comme :

- des e-services d'aide à l'accomplissement des formalités administratives, des services personnalisés liés à la démarche (accusé de réception, attribution d'un numéro de dossier, prise de rendez-vous,...)
- des téléprocédures.

Des développements locaux pour ce genre de services à valeur ajoutée sont possibles même dans le cas où existent des formulaires nationaux. Leurs initiateurs devront cependant veiller à ce qu'aucune demande d'information, pièce justificative ou condition de toute nature, réserve faite des éléments nécessaires à l'interactivité de la démarche proposée (numéro de téléphone, adresse électronique,...), ne soit ajoutée à celles qu'exige le formulaire arrêté au niveau national. La circulaire ajoute qu'aucun témoin de connexion autre que ceux nécessaires à l'interactivité de la démarche ne seront employés.

Sur la question de la forme électronique qu'on va substituer à la forme écrite, grâce à la dématérialisation prévue par la loi, on reprendra les documents choisis comme exemples.

2.4.2. L'acte électronique

Au centre de la téléprocédure c'est-à-dire de la formalité déclarative effectuée par des moyens électroniques, la télédéclaration. Quelle statut doit-on donner à cette déclaration électronique ? Ce statut sera-t-il voisin de celui de l'écrit sous forme électronique du Code civil ?

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 (JO du 14 mars 2000 p. 3968) montre une innovation fondamentale : l'ouverture du Code Civil aux formes électroniques de l'informatique. Pour la première fois, le Code Civil définit la notion générique d'écrit :

Article 1316 - 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.

1) La loi du 13 mars 2000 et la définition de l'écrit électronique

La fin du 1er alinéa de l'article 1316 apporte une précision importante. En visant le support et les modalités de transmission, le texte ouvre la voie à deux variétés d'écrit : l'écrit traditionnel sur support papier et l'écrit sous forme électronique. La nouvelle modalité, l'écrit sous forme électronique, peut comme l'écrit papier traditionnel, et à égalité avec celui-ci, être porteur de force probante. Le principe est stipulé par l'article 1316-1 :

Art. 1316-1. - 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

[32] J.O. Numéro 5 du 7 janvier 2000 page 279.

conditions de nature à en garantir l'intégrité.

L'écrit de forme électronique doit être accompagné de certaines caractéristiques qui vont de soi dans l'écrit-papier traditionnel, mais qui devront être intégrés, maintenus et vérifiés dans le contexte électronique. Selon l'article 1316-1, il faut 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. Pour l'écrit traditionnel, il peut être simple de déterminer son origine : papier à entête, indication de l'auteur en toutes lettres, éléments postaux etc. La chose est plus délicate en électronique surtout s'il y a télétransmission. Il y a aussi la question de la pérennité du support : malgré une apparente fragilité, le papier peut se conserver plusieurs siècles. Quant à l'écrit électronique, il ne possède pas de support et n'est constitué que d'informations élémentaires qui peuvent cheminer par des voies différentes et donc se perdre pendant les télétransmissions. D'où une exigence d'intégrité à respecter. Cet article est une étape notable dans l'histoire de la dématérialisation de l'écrit qui à vrai dire, se profilait depuis ces dernières années[33].

A noter également que les garanties d'identification et d'intégrité sont réclamées, non seulement, au moment de la formation de l'écrit sous forme électronique, mais encore pendant la conservation de l'écrit, ce qui va produire de sérieuses incidences sur l'archivage.

2) L'apport de la signature électronique à l'écrit électronique

Toutes les mesures de sécurité permettant de garantir authentification et intégrité permettront aux messages et fichiers d'obtenir la qualification d'écrit sous forme électronique. Ainsi l'écrit électronique exige-t-il des garanties qui sont celles de la signature électronique intégrée dans le Code civil par la même loi. Dès lors la conclusion suivante s'impose : une signature électronique valide c.a.d. conforme à l'article 1316-4 permettra efficacement à tout ensemble de données d'acquérir la qualité d'écrit (sous forme) électronique et la force probante qui s'y attache (c'est-à-dire la même que s'il s'agissait d'un écrit sur papier).

La définition de la signature électronique a été précisée par 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 (JO du 31 mars 2001 p. 5070). La plus grande efficacité juridique est obtenue grâce à une signature électronique sécurisée (SES) ;

« Signature électronique » : 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 ;
« Signature électronique sécurisée » : une signature électronique qui 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 en revenir à l'écrit sous forme électronique, toutes les combinaisons de moyens techniques garantissant l'identification et l'intégrité sont valables. Parmi celles-ci, la signature électronique sécurisée. Cependant et il faut insister sur ce point : la signature électronique sécurisée est un moyen primordial d'administrer la preuve, mais pas le moyen unique[34] !

3) Les limites de la loi du 13 mars 2000 – La loi sur l'Economie Numérique

Si un texte de loi requiert un support papier 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 validée ultérieurement par l'emploi d'une signature électronique ? A ce jour, la réponse est non. 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[35], tout contournement de la règle,

[33] Cf. 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.

[34] A l'appui de cette opinion, l'exemple de la facture électronique qui peut revêtir deux formes : un mail avec signature électronique ou bien un message structuré de type EDI sans signature électronique obligatoire mais respectant l'identification et l'intégrité ! (Cf. Notre article ???)

[35] Compte tenu du nouveau contexte, chaque terme employé par les textes va avoir son importance. Le terme "*écrit*" ne pose plus désormais de difficulté. Pour des mots tels que "*copie*", "*exemplaire*", voire "*liasse*", on pourra plaider que la forme électronique se conçoit aisément, ce qui ne sera pas le cas avec "*lettre*", "*papier*", "*registre*" etc…

n'aboutit généralement à la nullité de l'acte ou à son inexistence. La réforme du printemps 2000 n'a pas changé cet état de chose.

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*. Ces écrits sur papier sont en effet indispensables pour la validité-même du document que l'on dresse. Mais la distinction *ad validitatem / ad probationem* pourrait être remise en cause lors de la transposition de la Directive précitée sur le commerce électronique qui prévoit que les contrats pourront être négociés par voie électronique. L'Assemblée Nationale a déjà voté le projet en première lecture qui intégrerait au Code civil l'article 1108-1 dont le premier alinéa serait 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 (...)"
Au terme de ce projet d'article 1108-1, l'obligation préalable de dresser un écrit-papier pour former un acte est bien présente. La dématérialisation pourra néanmoins être opérée si le message électronique présente, lors de sa formation, de sa transmission et de sa conservation, toutes les garanties assurant identification de l'auteur et intégrité du message. Ces garanties pourront être efficacement assurées si une Signature Electronique Sécurisé (SES) est employée, sans que cela soit une obligation. Cependant l'utilisation d'une SES sera encore un atout considérable au moment d'administrer la preuve de l'écrit électronique.

La LEN et la validation de la dématérialisation

Le nouvel article 1108-1 s'il est définitivement adopté renvoie à deux articles du Code, le 1316-1 et le 1316-4. Aussi se pose-t-il la question duquel choisir et dans quelles circonstances.

Face à la problématique isolée du support papier exigé, c'est vers l'article 1316-1 qu'on peut se tourner. Il peut être utile d'en rappeler les termes : "*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.*" En application de cet article, il serait possible d'*établir* la forme électronique d'une déclaration habituellement sur papier à condition de garantir l'intégrité et la source de la déclaration. Notons que l'article traite de "*la personne dont il émane*", c'est-à-dire la source du document. Il est vrai que la source ou l'origine du document renvoie à une personne qui dans un contexte juridique devra être identifié. Si la personne dont l'écrit émane ne consent pas spécifiquement à un contenu obligataire de l'acte, la personne source du document ne se comporte pas en auteur intellectuel de l'acte, en signataire. Cette précision apportée à la personne source de l'acte électronique, émettrice ou signataire, est la différence fondamentale, en excluant l'intégrité qui est commune, entre l'article 1316-1 et 1316-4 (la signature). Cette différence de gradation dans le rôle de la personne à la base de l'acte électronique semble d'ailleurs particulièrement commode dans les téléprocédures, où la personne dont elle émane est le déclarant qui n'est pas nécessairement un signataire au sens du Code civil.

Les garanties d'origine et d'intégrité demandées peuvent être apportées par tout moyen technique, mais aussi par une signature électronique générique dite encore *signature numérique*[36] 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).* Dans cette circonstance, la validation de la téléprocédure, forme électronique d'une déclaration, serait acquise par une simple signature numérique.

D'autres cas doivent être considérés. Dans l'immense variété des documents et pièces qui existent, quelques-uns réclament une signature autographe sans précision sur l'obligation expresse d'un support papier. Jusqu'à l'arrivée des formes électroniques, il était difficile d'imaginer une signature "apposée" en l'absence d'un support papier. Aujourd'hui le cas est à prendre en considération dans le contexte électronique. Mais peu importe si la nécessité du support est tacite ou expresse, l'exigence formaliste de la signature sera comblée par l'emploi d'une signature électronique de l'article 1316-4 qui rendra l'acte électronique parfait.

Enfin, il faut considérer la double problématique formaliste, comme cela est fréquent : le document établi sur un support papier doit également être signé par l'auteur. Selon nous, dans un semblable cas "support papier +

[36] Une signature numérique ("digital" en anglais) est une modalité de signature technologie basée sur une Infrastructure à clé publique (cryptographie asymétrique et biclé privé-public, certificats et certificateurs). La signature électronique du Code civil est une signature numérique auquel le législateur a donné une dimension juridique.

signature", la problématique du support papier est absorbée par celle de la signature. Par application du Code civil, la signature en question ne peut être remplacée que par une signature de l'article 1316-4, sécurisée ou non. Dès lors, il ne peut être question d'employer une seconde ou une autre signature pour remplir les garanties d'identification et d'intégrité de l'article 1316-1, ni même de s'interroger sur la nature de cette seconde signature. Une seule suffit.

Le tableau ci-dessus résume cette typologie :

Problématique formaliste		**Base juridique (art. 1108-1)**	**Solution**
Cas 1	Support papier seul exigé	Art.1316-1	Tous moyens d'identification & d'intégrité ou Signature numérique
Cas 2	Signature seule exigée	Art. 1316-4	Signature électronique (sécurisée ou non)
Cas 2	Support papier + signature exigés	Art. 1316-4	Signature électronique (sécurisée ou non)

2.5. Les formalités complémentaires

Dans de nombreux cas, la nécessité de joindre des pièces justificatives et des documents d'accompagnement a été un frein à la dématérialisation. Les documents d'accompagnement et pièces justificatives sont de nature différente selon les déclarations considérées.

Fréquemment une déclaration est accompagnée d'un paiement. Le cas du paiement électronique sécurisé ne sera pas étudié dans le cadre de ce rapport. Il constitue en soi une matière suffisante pour un autre chantier juridique. Tout au plus, remarquera-t-on ici que la formalité complémentaire de paiement peut constituer un obstacle formel à moins que la difficulté ne provienne des documents d'accompagnement ?

Souvent les déclarations administratives s'accompagnent d'un paiement que nous considérerons ici comme une formalité complémentaire à la formalité principale déclarative.

3. PARTIE II- La problématique de l'échange électronique

3.5. La problématique juridique de l'échange d'écrits entre absents

La situation juridique peut s'analyser aussi simplement que possible lorsque les personnes qui échangent un document sont face à face. Les relations juridiques peuvent se dérouler dans un environnement sûr et la transmission d'un document de l'un à l'autre ne vient pas ajouter des éléments d'incertitudes juridiques. Ce n'est pas le cas avec les échanges électroniques. Les personnes y sont absentes. Le contrôle du bon déroulement et de la régularité des opérations repose généralement sur le contrôle visuel. La présence physique des utilisateurs permet à chacun de contrôler l'identité de l'autre, la date et de l'heure de l'échange. On peut contrôler que l'échange est fait volontairement, que l'un est d'accord pour transmettre et l'autre d'accord pour recevoir. Cette présence physique et les possibilités de contrôles visuels garantissent de nombreux concepts juridiques, comme :

- la capacité et la compétence de chacun des acteurs contrôlés par l'autre,
- l'échange des consentements, parce que simultanément l'un offre et l'autre accepte,
- la datation des actes et documents,
- la préconstitution de la preuve,
- la localisation et la datation des actes et documents,
- la formalisation de l'ensemble des éléments précédents par la signature.

Au contraire, l'échange de messages électroniques s'analyse comme une situation juridique entre personnes absentes. L'absence physique rend les garanties citées incertaines :

- Il est impossible de vérifier visuellement la capacité et la compétence des personnes.

- L'échange des consentements est douteux car il n'est plus simultané ; il y a un délai entre l'offre de l'un et l'acceptation de l'autre.
- La datation de l'acte est problématique : un contrat existe d'abord pleinement pour l'un (l'offreur) alors que l'autre n'est pas encore lié (acceptant).
- La préconstitution de la preuve doit être contrôlée puisque l'acte ou le document n'est plus échangé de la main à la main ;
- La localisation de l'acte n'est plus unique mais double entre le lieu de l'émetteur et le lieu du destinataire ;
- L'apposition des signatures n'est plus simultanée.

Lorsqu'on considère les échanges électroniques au niveau technique, on s'aperçoit que les utilisateurs ont des préoccupations techniques proches des préoccupations juridiques. Les utilisateurs des systèmes informatiques sont à la recherche de sécurité pour ce qu'ils confient aux télécommunications : échanges électroniques privés, Commerce Electronique ou relations électroniques entre les entreprises et les administrations. Quelle que soit la méthode, viser la sécurité des échanges consiste à s'assurer de la réalisation d'un certain nombre de garanties techniques. Ces garanties visent à apporter autant de certitudes dans les conditions des échanges électroniques ainsi que dans les acteurs qui sont aux deux bouts de la ligne, à l'émission comme à la réception.

Parmi une riche typologie, les garanties de sécurité les plus recherchées sont les suivantes :
- L'authentification permet d'indiquer avec précision l'origine d'un message électronique expédié par télécommunications.
- L'intégrité garantit que le message électronique reçu par le destinataire lui est parvenu dans l'état où il a été émis.
- La confidentialité est obtenue lorsque le message n'est compréhensible que par son destinataire ou par les personnes autorisées.
- L'horodatage garantit avec exactitude le moment, en date et en heure, où un quelconque événement a pu survenir.

Ces garanties de sécurité sont concrètement obtenues par des moyens divers : équipements et terminaux, logiciels spécialisés, réseaux et/ou services ou par un mélange des uns et des autres.

3.6. Le cadre légal de l'échange électronique de l'article 4 de la loi Madelin

Il existe peu de textes législatifs dans le droit interne qui donnent des indices sur le cadre juridique de la transmission électronique. L'article 1316 du Code civil précise dorénavant que l'écrit, surtout dans sa forme électronique, est destiné à être transmis. Cependant la loi n°94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle (dite Loi Madelin) fixe un cadre général pour les *déclarations faites par voie électronique*.

3.2.1. Le cadre légal

L'article 4 de la Loi Madelin fournit le cadre légal général pour la transmission des téléprocédures. Le tableau ci-dessous présente le contenu des alinéas de l'article 4 :

Art.4-I	*Toute déclaration d'une entreprise destinée à une administration, personne ou organisme visés à l'article 1er peut être faite par voie électronique, dans les conditions fixées par voie contractuelle.*
Art.4-II Alinéa 1 Alinéa 2	*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.* *La réception d'un message transmis conformément aux dispositions du présent article tient lieu de la production d'une déclaration écrite ayant le même objet.*
Art.4-III	*Lorsque la transmission d'une déclaration écrite entre une entreprise et une administration, personne ou organisme visés à l'article 1er est soumise à une date limite d'envoi, le cachet de la poste fait foi de la date de cet envoi.*

Comme pour une grande majorité des actes juridiques, en tout cas jusqu'à une époque récente, les déclarations émises par les entreprises à destination des administrations étaient effectuées sur le support papier. L'article 4-I

de la Loi Madelin pose le principe qu'il est possible de transférer ces déclarations aux administrations par voie électronique. Cette autorisation de la loi constitue une base légale[37] pour la dématérialisation documentaire, dématérialisation qui constitue le premier axe de notre problématique juridique.

A noter cependant que l'art.4-I ne semble viser qu'un des aspects de la dématérialisation, l'abandon du support papier. Ce qui n'est pas le cas en réalité. Nous nous étions en effet posé la question au moment de l'adoption de la loi[38] :

> "Comment l'article 4 peut-il se concilier avec les textes juridiques qui fixent le régime des déclarations ? En effet, l'article autorise une transmission par voie électronique. Mais pour que cette transmission ait lieu, il faut encore que la déclaration soit elle-même sous forme électronique, ce que le texte ne mentionne pas. En d'autres termes, si le texte organisant la déclaration traditionnelle exige une forme écrite, on ne peut la dématérialiser sans violer ce texte. La loi Madelin ne pourrait jouer et perdrait alors toute portée.
>
> *Cependant selon le cabinet du Ministre Madelin, ceci n'est pas la bonne interprétation du texte. Pour preuve, l'article 4 écrit que "la déclaration peut être faite par voie électronique" et non qu'elle est "transmise". Ce n'est donc pas le document écrit qui est visé mais la formalité déclaratoire."*

On en terminera avec l'art. 4.I en ajoutant que l'opération n'est possible que si certaines *conditions*, à définir contractuellement, président à la transmission électronique. L'alinéa 2 de l'article II indique la finalité de la manœuvre : la validité de la forme électronique et l'équivalence avec la déclaration papier[39]. On comprend dès lors que si l'art.4.I a rendu parfaite la déclaration dématérialisée, comme l'est par essence la déclaration papier, la perfection de l'acte ne doit pas être dégradée pendant le transport électronique, altérant la validité à l'arrivée. L'art. 4.II alinéa 1 énumère les conditions de l'échange. L'échange doit s'entourer de moyens sécuritaires satisfaisant les exigences légales : identification de l'auteur, intégrité, lisibilité et à la fiabilité de la transmission, date et heure, assurance de la réception, conservation.

Les conditions énumérées par l'article 4.II alinéa 2 correspondent au deuxième axe de notre problématique juridique, l'échange électronique.

Enfin l'art. 4.III rappelle l'actualité du principe du "cachet de la poste qui fait foi". Le rappel est placé dans un article spécifique, car il s'impose aux envois postaux des déclarations écrites comme aux échanges électroniques des déclarations dématérialisées. Pour ces dernières, il apporte des précisions à l'exigence temporelle posée par l'art. 4.II al.1.

3.2.2. La pratique administrative

3.2.2.1. Le cadre conventionnel

Des exemples de conventions spécifiques existent en matière de téléprocédures, proposées aux particuliers et aux entreprises par l'administration.

Par exemple pour bénéficier du régime télédéclaratif en matière de TVA, le redevable devra préalablement déposer un dossier de souscription téléchargé sur le site www.finances.gouv.fr, ou bien retiré auprès d'une recette des impôts ou d'un centre des impôts. Ce formulaire de souscription à la télédéclaration et au télérèglement est déposé à la recette des impôts dont dépend le redevable pour le paiement de la TVA y compris pour ceux concernés par l'obligation de télédéclaration et télérèglement[40].

---

[37] En ce qui concerne les actes et documents commerciaux, les entreprises s'autorisent elles-mêmes la dématérialisation par voie contractuelle au moyen de l'accord d'interchange.

[38] Cf. notre article "*Relations entreprises-administrations, déclarez par EDI !*", La Gazette de l'entreprise communicante (Simprofrance), n°18, décembre 1994.

[39] L'alinéa 2 de l'article 4.II parle de "déclaration écrite". Mais comme la loi du 13 mars 2000 (signature électronique) est passée par-là, nous lisons "déclaration papier".

[40] Les adhérents à TéléTVA désireux d'utiliser la procédure EFI devront se procurer, auprès d'une autorité de certification du marché, un certificat numérique référencé par le MINEFI : «ticket unique» d'accès aux téléprocédures. La liste de ces certificats est disponible sur le site Internet du MINEFI. Ce certificat, totalement banalisé, pourra être utilisé par l'entreprise pour des échanges électroniques avec d'autres partenaires que l'administration.

La Déclaration d'Echanges de Biens (DEB)[41], qui est un document à la fois statistique et douanier, doit être rempli par tout importateur à l'entrée du territoire de l'espace économique européen. L'utilisation d'une forme électronique de DEB passe par la ratification d'un cahier des charges prévu par l'arrêté du 4 janvier 2002[42].

3.2.2.2. La transmission multimodale

D'après une notice de l'URSSAF intitulée "*Comment remplir votre déclaration unique d'embauche (DUE)*" (CERFA n°50282#02), le formulaire une fois rempli doit être transmis soit par courrier, par fax, par Minitel ou via Internet. Pour la transmission par Internet, diverses possibilités sont ouvertes, notamment l'utilisation d'un portail des URSSAF www.due.fr. Si l'employeur n'est pas en mesure de fournir toutes les informations demandées dans la DUE, il transmet une forme dégradée de DUE dite *Déclaration Préalable A l'Embauche* (DPAE). La DPAE est matériellement constituée par le même formulaire 10563*03 que la DUE, seules certaines informations figurant sur un fond bleu devant être renseignées.

La DEB montre l'exemple d'une téléprocédure multimodale. En effet, selon l'article 1 de l'arrêté du 4 janvier 2002, les divers moyens de transmission suivants peuvent être employés :

- Transmission directe de données mises en forme par le système informatique propre au déclarant. Il s'agit : 1° De supports magnétiques, c'est-à-dire disquettes, bandes magnétiques, cartouches ; 2° De services de messagerie électronique ; 3° De transferts de fichiers point à point.
- Utilisation d'un serveur de l'administration permettant de saisir en mode interactif et de transmettre des déclarations d'échanges de biens en ligne. Il s'agit d'un service Minitel, intitulé « 36-15 DOUANETEL », permettant de saisir et de transmettre la déclaration d'échanges de biens ou encore d'un service en ligne Internet intitulé « DEB sur le WEB » permettant de saisir et de transmettre des déclarations d'échanges de biens simplifiées ou détaillées à travers le site Internet du ministère de l'économie, des finances et de l'industrie.

Le choix de ces moyens nécessitent l'emploi de format différents pour la présentation des données attendues[43].

Comme ces moyens présentent un niveau disparate de sécurité, les garanties demandées s'apprécient différemment selon les vecteurs choisis :

Identification des déclarants (art .7)	Les émetteurs des déclarations d'échanges de biens transmises par voie informatique doivent être identifiés à chaque transmission. L'identification est la fonction permettant de s'assurer que l'information reçue a effectivement été transmise par un déclarant reconnu par le centre de collecte comme titulaire de l'autorisation prévue par l'article 1er du présent arrêté. L'identification est différente suivant les méthodes utilisées : a) Transmission directe de données mises en forme par le système informatique propre au déclarant : Le numéro de TVA et le numéro de l'autorisation prévue à l'article 10 du présent arrêté sont contenus dans le premier enregistrement des fichiers SAISUNIC ou INTRACOM pour les fichiers structurés en enregistrements de longueur fixe, et dans le segment UNB de l'interchange pour les messages aux normes UN/EDIFACT ; De plus : - pour les supports magnétiques, le nom, l'adresse et le numéro d'autorisation prévue par l'article 10 du présent arrêté doivent figurer de façon externe sur le support ; - pour la messagerie électronique, le titulaire de l'autorisation est identifié par son adresse électronique ; - pour le transfert de fichiers point à point, le site émetteur est identifié par la vérification

41 La loi n° 92-677 du 17 juillet 1992 (modifiée) qui fonde la déclaration d'échanges de biens a transcrit en droit interne la sixième directive TVA et le règlement CEE n° 218/92 du 27 janvier 1992 concernant la coopération administrative dans le domaine des impôts indirects (TVA).

42 *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 n° 30 du 5 février 2002 page 2336

43 Selon l'article 2 de l'arrêté : "Pour la transmission directe de données mises en forme par le système informatique propre au déclarant, ce dernier peut utiliser les formats de données suivants :
a) Fichiers structurés en enregistrements de longueur fixe. Il s'agit des structures suivantes :
INTRACOM : structure d'enregistrement spécifique aux échanges de biens avec les autres Etats membres ; SAISUNIC : structure d'enregistrement utilisée à la fois pour les échanges avec les autres Etats membres et pour les échanges avec les pays tiers.
b) Messages aux normes UN/EDIFACT. Il s'agit du message INSTAT, sous-ensemble du message CUSDEC."

	des paramètres transmis, nécessaires à l'établissement de la connexion ; b) Serveurs de l'administration : Minitel 36-15 DOUANETEL et service en ligne internet « DEB sur le WEB », le titulaire de l'autorisation est identifié par son numéro de TVA et son code opérateur.
Authentification des déclarations (art.8)	Les déclarations d'échanges de biens transmises par voie informatique doivent être authentifiées à chaque transmission. L'authentification est la fonction permettant de s'assurer que la personne physique responsable de l'établissement de la déclaration d'échanges de biens a pris la responsabilité de la déclaration transmise par voie informatique. Toute déclaration authentifiée est réputée émise par le titulaire de l'autorisation prévue à l'article 1er du présent arrêté. Par cette authentification, il engage sa responsabilité ou celle de son mandant sur les informations transmises. Dans le cas de la transmission directe de données mises en forme par le système informatique propre au déclarant, l'authentification des déclarations est assurée par la transmission, pour chaque envoi, d'un mot de passe personnel et confidentiel, remis sous pli recommandé au titulaire de l'autorisation prévue par l'article 1er du présent arrêté. Dans le cas du Minitel et du serveur en ligne Internet, l'authentification est assurée par l'utilisation d'un code confidentiel, remis personnellement au déclarant.
Contrôle d'intégrité des déclarations (art.8)	Le contrôle de l'intégrité des déclarations permet au déclarant de s'assurer que les données enregistrées par le centre de collecte sont identiques aux données qu'il a transmises : a) Transmission directe de données mises en forme par le système informatique propre au déclarant. Après réception effective de déclarations d'échanges de biens transmises par un des moyens prévu à l'article 1er (a) du présent arrêté, le centre de collecte de rattachement vérifie l'origine de la transmission, les formats utilisés et le respect des règles d'authentification prévues à l'article 8. Le centre de collecte renvoie, par télécopie ou par voie électronique, selon le moyen de transmission des déclarations utilisé par le déclarant et indiqué au protocole technique annexé à la convention prévue par l'article 1er du présent arrêté, dans un délai maximum de trois jours ouvrés, un accusé de réception. Cet accusé de réception contient, pour chacun des flux, l'indication de la prise en compte ou du rejet des déclarations contenues dans l'envoi et, en cas d'acceptation, le nombre de lignes de déclarations reçues et le total des valeurs fiscales. Si le déclarant ne reconnaît pas avoir transmis de déclaration d'échanges de biens correspondant aux indications renvoyées par l'administration, il dispose de trois jours ouvrés à compter de la date d'envoi de l'accusé de réception pour faire connaître son opposition par lettre recommandée avec accusé de réception adressée au centre de collecte de rattachement ; b) Utilisation d'un serveur de l'administration : le service (Minitel ou internet) affiche sur le terminal du déclarant, après chaque validation d'une déclaration, le nombre de lignes de la déclaration et le total des valeurs fiscales.

3.7. **Les exigences légales à considérer**

L'article 4-II alinéa 1de la Loi Madelin liste une série de garanties de sécurité à prendre en compte dans le contrat à passer entre le déclarant et l'administration. Parmi ces garanties figurent l'identification et l'intégrité qui sont particulièrement à l'honneur avec 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. Mais les autres peuvent être envisagées quelques instants dans la mesure où elles auraient un rôle à jouer en matière de conservation des déclarations[44].

[44] Cf. notre article "*Conservation et archivage de l'écrit sous forme électronique*", Jurisclasseur Communication et Commerce Electronique – mai 2002, chr. 12 et juin 2002, chr.14.

3.3.1. La question de la lisibilité

La lisibilité est le fait de pouvoir être lu par l'œil humain. Cette garantie ou cette qualité de lisibilité doit être présente pendant la transmission de l'écrit ainsi qu'à l'arrivée. C'est surtout par les effets juridiques attachés que la lisibilité est importante : elle garantit que le message électronique pourra recevoir le traitement juridique approprié. Dans les services à valeur ajoutée du marché positionnés en intermédiaire entre émetteur et destinataire des messages, la lisibilité est attestée par le service par l'envoi à l'émetteur d'une sorte d'accusé de réception plus ou moins spécifique[45]. La demande de lisibilité va plus loin dans le monde des téléprocédures. Les déclarations lorsqu'elles sont sur support papier doivent être produites par les administrés sur des formulaires ad hoc, au design et au contenu prédéfinis par le CERFA. La structuration et le rubriquage des déclarations sous forme électronique garantissent bien la lisibilité.

Comment la lisibilité doit-elle être satisfaite pour qu'en fin de transmission, le texte soit intelligible ? Les messages ont été créés et transmis, ultérieurement archivés, sous un certain format. La prudence est d'archiver le message dans un format indépendant du logiciel de traitement. La norme technique ISO 15489[46] indique que la lisibilité et l'intelligibilité doivent également permettre d'établir la pertinence de la syntaxe et la sémantique afin d'assurer l'exploitabilité des messages électroniques.

Toutefois un texte prévoit une garantie de lisibilité à intégrer prochainement dans le droit interne. Il s'agit de la *Directive 2001/115/CE du Conseil du 20 décembre 2001 modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée.* Ce texte incite les Etats Membres à accepter les factures électroniques "*à condition que l'authenticité de leur origine et l'intégrité de leur contenu soient garanties*" soit par des messages EDI soit en validant les factures électroniques par une signature électronique avancée. L'article 2.2.3.d) de la Directive indique que les mesures de sécurité doivent rester les mêmes pendant les opérations techniques : "*l'authenticité de l'origine et l'intégrité du contenu de ces factures, ainsi que leur lisibilité, doivent être assurées durant toute la période de stockage*". L'article poursuit en posant que les Etats peuvent imposer l'archivage de la pièce sous sa forme originale (écrit ou électronique) et que dans le cas d'un archivage électronique, "*les données garantissant l'authenticité de l'origine et l'intégrité du contenu de chaque facture soient également stockées*". Le texte montre in fine la prééminence d'autres garanties de sécurité déjà connues du droit français : identification et intégrité.

Aussi négligera-t-on l'exigence de lisibilité, en considérant que si Identification et intégrité sont satisfaites, elles emportent la lisibilité... si le message a été établi, naturellement, sous un format lisible.

3.3.2. La question de la fiabilité

En septembre 1998, le Conseil d'Etat a publié un important rapport, *Internet et les réseaux numériques*, disponible sur le Web et à la Documentation Française. Dans le chapitre 2 consacré à "*la reconnaissance de la valeur juridique du document et de la signature électronique*", le Conseil parlait de la fiabilité des techniques et apportait les précisions suivantes sur les effets juridiques : *"La fiabilité est conditionnée par le respect des exigences suivantes :*

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

Depuis l'intégration de la signature électronique dans le Code civil, l'article 1316-4 indique que cette dernière est un "*procédé fiable d'identification*". Le procédé doit être fiable c'est-à-dire susceptible d'aboutir à la fin pour lequel il a été mis en œuvre. La sanction est la suivante : si la fiabilité du procédé est établie, le procédé bénéficiera d'une présomption légale.

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

[45] C'est le cas avec les accusés de réception fonctionnel des services EDI.

[46] Norme ISO/DIS 15489 (ISO TC 46/SC11), en date du 29 mai 2000 dites " Records Management". Traduction française par l'AFNOR du document officiel en langue anglaise.

technique tel que la norme ISO 15489 qui déclare dans le même ordre d'idée : "*Un document fiable est un document dont le contenu peut être considéré comme la représentation complète et exacte des opérations, des activités ou des faits qu'elles attestent, et sur lequel on peut s'appuyer lors d'opérations, d'activités ou de faits ultérieurs*" (point "8.22 Fiabilité" de la norme).

Comment assurer pratiquement la fiabilité ? Ce résultat sera atteint en mettant en œuvre des moyens techniques présentant certaines garanties de sécurité recherchées par les lois. Ainsi l'article 1316-1 du Code Civil indique quelles sont les garanties de sécurité technique dont l'écrit sous forme électronique a besoin pendant son cycle de vie : "*L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité."* Les garanties techniques demandées sont l'*identification* de l'auteur de l'acte et *intégrité* de l'écrit.

3.3.3. La question de la confidentialité

Dans les échanges électroniques, les fichiers et les messages sont transmis sans enveloppe, ce qui les rend plus accessibles aux indiscrets, aux curieux et autres pirates. Aussi pour tous les réseaux de télécommunications, à plus forte raison pour Internet, les entreprises comme les particuliers présentent-ils une forte demande de confidentialité pour protéger les échanges commerciaux, stratégiques et concurrentiels ou même les données nominatives et de la vie privée.

Pourtant rien dans le droit civil ou dans le droit commercial ne traite du besoin de confidentialité. Il en est ainsi parce que la confidentialité est garantie par le secret qui est de mise dans les télécommunications. Appliqué dès l'origine aux lettres et paquets confiés à la poste, le secret des correspondances s'est étendu aux télécommunications. L'article L.41 du code des P et T qui traite de cette question en matière de services de télécommunications renvoyait au Code Pénal qui vise la correspondance postale. L'assimilation a été renforcée par la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications. Le principe est donné par l'article 2 de la loi :

Le secret des correspondances émises par la voie des télécommunications est garanti par la Loi

La loi ne fait plus référence à la correspondance privée. L'article 186.1 du Code Pénal qui vise la correspondance postale indique que le secret doit être conservé par "*tout agent de l'exploitant public, tout agent d'un exploitant de réseau autorisé ou d'un fournisseur de services de télécommunications*". Selon l'article 1 de la loi du 10 juillet 1991, le secret est absolu. Les seules exceptions au secret sont des *écoutes* de deux types : les interceptions ordonnées par l'autorité judiciaire et les interceptions de sécurité faite par l'administration sur autorisation du Premier ministre.

Si on persiste à vouloir utiliser des moyens cryptographiques pour protéger les messages électroniques, se pose la question du type de méthode cryptographique employée. Quoique de nombreux produits (quelquefois gratuits) de cryptographique symétrique existent sur le marché, des prestations de cryptographie asymétrique mettent en œuvre un bi-clé et un certificat électronique du même type que celui de la signature digitale.

En ce qui concerne les téléprocédures, les autorités administratives se préparent à recevoir des messages électroniques éventuellement chiffrés. La Politique de Certification-type du Minefi prévoit le cas. Toutefois ce ne sera vraisemblablement jamais une obligation.

3.3.4. La question de l'horodatage

3.3.4.1. La question juridique

Dans les téléprocédures, il sera souvent impossible de s'en remettre au temps système dans la mesure où la télédéclaration devra être effectuée avant une date limite. L'article 4 de la loi Madelin rappelle le principe selon lequel "*la date du cachet de la poste fait foi*". La question posée dans les "déclarations faites par voie télématique" et prochainement par les téléprocédures est celle de la transposition de ce principe du monde postal au monde électronique. Un premier essai de transposition a eu lieu dans le document préparé en son temps avec le cabinet du Ministre Madelin :

CLAUSES MODELES POUR LA TRANSMISSION PAR VOIE ELECTRONIQUE DE LA DECLARATION DE

... en application de l'article 4 de la Loi n 94-126 du 11février 1994 .../...
E- DATE ET HEURE DE LA DECLARATION
E1. Conformément à l'article 4-II de la loi n 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle, les parties conviennent expressément que la date et l'heure de la déclaration correspondent au moment où la transmission par voie électronique de la déclaration sous le format prévu devient irréversible.

Le point de l'horodatage est crucial en matière de téléprocédures et mérite à soi une étude complète. Pour les actes sous-seing privés la *date certaine* n'est pas toujours critique ; elle l'est souvent dans les téléprocédures qui doivent être accomplies, souvent accompagnées d'un règlement, avant une date administrative.

Pour cette question, on se reportera avec profit aux *Recommandations pour la sécurisation de l'horodatage électronique*[47] du groupe de travail commun IALTA / Edificas :

... S'il est couramment admis que le cachet de la poste permet d'établir la date d'envoi, certains services publics [48] retenaient, jusqu'à la loi du 12 avril 2000 [49] la date de réception alors que d'autres [50] prenaient en compte la date d'expédition. De plus, les textes qui imposent une date limite pour effectuer une déclaration ou produire un document ne précisent pas toujours s'ils intègrent ou non les délais d'acheminement des correspondances (dépôt des dossiers d'inscription à l'université, par exemple).
La loi du 12 avril 2000 a unifié les règles de preuve en matière de certification de date ou de délai. Dans son article 16, la loi précise que : "Toute personne tenue de respecter une date limite ou un délai pour présenter une demande, déposer une déclaration, exécuter un paiement ou produire un document auprès d'une autorité administrative peut satisfaire à cette obligation au plus tard à la date prescrite au moyen d'un envoi postal, le cachet de la poste faisant foi, ou d'un procédé télématique ou informatique homologué permettant de certifier la date d'envoi."

La loi généralise la règle selon laquelle la date limite d'exigibilité correspond à la date d'envoi certifiée par le cachet de la poste. Cette règle est étendue à toutes les formalités pour lesquelles les administrés sont tenus de respecter un certain délai [51]. L'administré dispose donc jusqu'au dernier jour du délai imparti pour envoyer une demande ou satisfaire à une obligation, le cachet de la poste faisant foi. Cette même loi précise que l'envoi des documents par un procédé télématique ou informatique homologué permettant de certifier la date d'envoi produit les mêmes effets que l'envoi par la poste. Un décret en Conseil d'Etat doit en fixer les modalités d'application.(...)

Pour l'application des téléprocédures, il ressort de ces deux lois que :
- il y a une corrélation forte entre la date d'envoi, le cachet de la poste faisant foi, et le procédé télématique ou informatique homologué certifiant la date d'envoi ;
- la date d'envoi se fixe au moment où l'entité n'a plus la maîtrise de son envoi : boîte aux lettres de la poste dans le 1er cas, envoi au Fournisseur d'Accès à Internet (FAI) ou à un Partenaire EDI DGI (PED [52]) dans le 2ème cas ;
- le décret d'application permettant de fixer les règles d'homologation du procédé télématique ou informatique n'a toujours pas été adopté, et qu'en son absence, les destinataires publics et parapublics font chacun leur meilleure interprétation.

Comme illustration, on se reportera à la question parlementaire ci-dessous :

M. Emmanuel Hamel attire l'attention de M. le ministre de la fonction publique et de la réforme de l'Etat sur le rapport d'un conseiller d'Etat intitulé "L'Etat et les technologies de l'information. Vers une administration à accès pluriel", rendu public le 6 mars 2000, dans lequel les auteurs préconisent de "mettre en place un système fiable des envois à l'administration de documents électroniques, équivalent au "cachet de la poste faisant foi", ainsi

47 Les Recommandations (version 2K du 30 avril 2003) sont téléchargeables sur les sites des partenaires.

48 Le code de la sécurité sociale pour les Unions de recouvrement de sécurité sociale et d'allocations familiales.

49 Article 16 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

50 La circulaire n° 1388 du 13 juin 1954 du ministère de l'économie, des finances et du budget et la lettre de l'UNEDIC n° 92-117 du 31 décembre 1992.

51 Toutefois ces dispositions ne sont applicables ni aux procédures régies par le Code des marchés publics ni à celles pour lesquelles la présence personnelle du demandeur est exigée en application d'une disposition particulière, ni à celles relevant des articles 1411 et s. du Code général des collectivités territoriales (article 16 de la loi n° 2000-321 modifié).

52 PED : Partenaire EDI DGI. Entité (SSII, profession libérale, entreprise, etc.) ayant fait l'objet d'un agrément de la part de la DGI pour être autorisée à émettre vers elle.

qu'un système automatisé d'accusé de réception". Il le remercie de bien vouloir lui indiquer si le Gouvernement entend mettre en place un tel système. Dans l'affirmative, quand le sera-t-il ? Et dans la négative, il souhaiterait connaître les raisons pour lesquelles le Gouvernement ne souhaite pas donner suite à cette suggestion.

Ministère de réponse : Fonction publique – Publiée dans le JO Sénat du 09/11/2000 page 3852.

Réponse. - La dématérialisation des procédures administratives et le développement des téléprocédures, inscrits dans le programme d'action gouvernemental pour la société de l'information au titre du chantier afférent à la modernisation des services publics, supposent la mise en place d'un dispositif homogène et fiable d'authentification et de certification des échanges de données entre les administrations et leurs partenaires extérieures. Cet environnement légal, qui va conférer au document électronique un statut équivalant à celui du document papier, est indispensable pour créer la confiance chez les usagers et les inciter à utiliser le plus possible les moyens électroniques dans leurs relations avec les services de l'Etat. En outre, l'article 16 de la loi 2000-321 du 12 avril 2000, relative aux droits des citoyens dans leurs relations avec les administrations, dispose que toute personne tenue de respecter un délai ou une date limite pour présenter une demande, déposer une déclaration, exécuter un paiement ou produire un document auprès d'une autorité administrative peut satisfaire à cette obligation au plus tard à la date prescrite au moyen d'un envoi postal, le cachet de la poste faisant foi ou d'un procédé télématique ou informatique homologué permettant de certifier la date d'envoi. Des expérimentations sont en cours dans de nombreux secteurs, qui vont permettre de vérifier la faisabilité des transactions électroniques entre les usagers et l'administration, notamment en termes de validation des envois à destination de l'administration et de dispositif d'accusé de réception des documents électroniques**.** Ces divers projets vont également contribuer à définir la doctrine générale de l'administration en matière d'utilisation de la signature électronique**,** qui s'avère indispensable pour garantir la sécurité juridique des échanges automatisés de données qui s'opèrent avec ses usagers.

Les difficultés de gérer les téléprocédures conduisent les administrations à aménager dans certains cas la date administrative dans les téléprocédures[53]. Ainsi dans l'EDI-TDFC[54], un délai supplémentaire de 15 jours, accordé à titre de tolérance aux adhérents de la téléprocédure de déclaration des résultats EDI-TDFC au-delà de la date limite fixée pour le dépôt des formulaires papier [55] de déclarations de résultat, est reconduit. Pour les documents déposés dans les délais requis et rejetés par la Direction Générale des Impôts (DGI) pour un motif d'ordre technique, les contribuables disposent d'un délai supplémentaire de 15 jours pour effectuer le dépôt du fichier corrigé. A titre de tolérance, aucune amende ou pénalité ne sera appliquée si la régularisation intervient avant l'expiration de ce délai.

Au contraire, les mêmes difficultés ont conduit dans le passé les organismes sociaux à avancer leur date de réception ! En cas d'échec, le déclarant disposait de quelques jours de grâce pour se rabattre sur la procédure papier et accomplir la formalité déclarative (et le règlement) avant la date butoir.

Les pratiques et les tolérances en ce domaine devront être unifiées. La même date butoir pour tous est en voie de constituer une nouvelle déclinaison de ce principe général du Droit, l'égalité de tous devant le service public ou encore l'égalité de tous devant les charges publiques.

3.3.4.2. La solution technologique : la certification de l'horodatage

Il est cependant délicat de définir ce moment surtout dans une configuration où les échanges électroniques entre entreprises et administrations font intervenir plusieurs intermédiaires. L'horodatage certifié[56] associe un temps mesuré à un message électronique déterminé. En conséquence, toute personne pouvant intervenir sur un message est susceptible de demander et d'obtenir cette certification. Au premier plan, l'émetteur du message c.a.d. le déclarant.

[53] Cf. *Les Recommandations* précitées.

[54] Voir BOI 13 K-8-00 N° 132 du 18 juillet 2000.

[55] Il s'agit soit de la date légale de dépôt telle qu'elle est précisée dans le Code général des impôts, soit de la date fixée annuellement par décision ministérielle, en l'espèce le 3 mai pour l'année 2000.

[56] Il s'agit d'un horodatage faisant intervenir un tiers certificateur spécialisé, dit *tiers horodateur*, qui garantit une heure précise au moyen du *jeton temporel* (sorte de certificat électronique spécialisé) qu'il délivre. Voir les travaux du groupe de travail commun IALTA France / Conseil Supérieur de l'Ordre des Experts-Comptables sur l'horodatage sécurisé.

On relève néanmoins une limite importante au système. La télédéclaration peut avoir été créée dans le système d'information du déclarant, avoir fait l'objet d'une horodatage certifiée et ne pas avoir été expédiée par négligence ou par oubli. Dans ce cas, on doit considérer que la dimension juridique repose dans l'accomplissement de la formalité déclarative et non dans l'envoi du document déclaratif. En conséquence, la formalité n'aura pas été accomplie. Cette hypothèse est identique à ce qui se passe, si l'entreprise après avoir rempli le formulaire écrit de déclaration l'oublie sur le bureau jusqu'à l'expiration du délai…

Dans cette circonstance, la date serait bien certaine mais la garantie perdrait son intérêt si la formalité n'est pas accomplie dans les temps. La transposition du principe de "la date de la poste fait foi" renvoie la fixation de la date au stade du transport électronique. Il semble que le mode opératoire de l'horodatage certifiée permet à plusieurs acteurs de produire une requête, l'émetteur naturellement, mais sans doute un certain nombre d'intermédiaires techniques ou non, ou même le destinataire final. Ce serait dans notre cas au transporteur électronique de faire établir un jeton temporel.

On pourrait alors imaginer le mode opératoire suivant :
- Le déclarant crée la déclaration dans son système.
- Il confie le message électronique à l'opérateur de télétransmission au plus tard quelques instants avant l'expiration du délai déclaratif.
- A réception du message et avant toute redistribution, par exemple dans la boite-à-lettres de l'administration, l'opérateur se fait établir un jeton par un Tiers Horodateur
- L'opérateur archive le jeton avec ou sans copie au déclarant.

3.8. Les solutions techniques

En retenant les garanties qui deviendront les plus usuelles tant en droit commun qu'un droit administratif, les mesures et moyens techniques à employer pour assurer identification et intégrité restent à déterminer.

3.4.1. La solution aux besoins d'authentification et d'intégrité

3.4.1.1. A la recherche d'une solution

Sur ce point, la DGI déclare sur son site Web que la sécurité des échanges sur Internet avec les contribuables est une priorité majeure pour les administrations fiscales. Afin de ne pas imposer aux usagers des contraintes disproportionnées aux enjeux, la stratégie Internet des administrations fiscales repose ainsi sur une gradation des mesures de sécurité en fonction de la nature des services proposés et du niveau de confidentialité ou de valeur juridique probante qu'ils exigent. Dans la recherche du meilleur équilibre possible, les téléservices[57] de l'administration offrent plusieurs niveaux de sécurité, sur le plan de l'authentification :

- anonymat,
- simple adresse électronique de correspondance,
- authentification par mot de passe
- authentification par l'usage de "certificat électronique".

Dans l'environnement "papier", l'authentification se fait couramment sur la présentation de pièces attestant de l'identité d'un individu ou des pouvoirs qu'il prétend avoir (carte d'identité, "pouvoir" donné par une autre personne d'accomplir un acte en son nom, comme, par exemple, pour le retrait d'une lettre recommandée à la poste) et la matérialisation de l'engagement juridique par l'apposition d'une signature manuscrite, d'un cachet, etc. qui servira de preuve en cas de différend. Transposant les besoins en matière électronique, une bonne partie des téléservices est accessible sans authentification[58], alors que les téléprocédures à proprement parler se classent en e-services accessibles après authentification.

Au premier niveau, administrations fiscales acceptent des certificats répondant aux critères de sécurité les plus stricts. Voici quelques exemples au Minefi à titre d'illustration :

- Télédéclarer et télépayer la TVA : les professionnels peuvent d'ores et déjà déclarer et payer la TVA et consulter leurs comptes TVA. Le certificat nécessaire pour sécuriser les échanges répond aux règles du ministère : doit provenir d'une autorité de certification reconnue par le ministère.
- Télédéclarer l'impôt sur le revenu et consulter son compte fiscal : les particuliers peuvent depuis 2002 déclarer leurs revenus et consulter leur compte fiscal (e-service de télédéclaration des revenus soumis à l'impôt sur le revenu et de consultation du compte fiscal) avec un certificat émis directement par le Minefi[59];
- Télépayer en ligne (hors TVA) : Pour payer un impôt quelconque, il n'est nul besoin de s'identifier, la réalité du paiement suffit. Toutefois, dans certains cas, notamment pour les grandes entreprises, la transaction sera sécurisée par le certificat utilisée pour la déclaration.

Naturellement si l'authentification doit être accompagnée d'intégrité, une solution réside dans l'utilisation d'une signature électronique. Mais on peut se demander laquelle ?

---

[57] Le terme de *téléprocédures* laisse la place de plus en plus souvent à celui de *téléservices*.

[58] Les services d'informations générales (simulations, actualité fiscale, téléchargement) sont délivrés aux usagers sous le régime de l'anonymat intégral. Pour certains services qui rendent des résultats personnalisés, une adresse email sera demandée ou utilisée pour délivrer la prestation demandée (exemple : réponse aux questions en ligne). Cette adresse sera évidemment celle communiquée par l'internaute sans aucune exigence particulière sous le libellé. Le site du Minefi ajoute : *"jean.dupont@provider.net " est à cet égard tout aussi utilisable que n'importe quel pseudo utilisé par l'internaute comme " christine.1214@xxx.fr " ou " xyz@provider.com* "

[59] Afin d'inciter les particuliers à utiliser ce service *et compte tenu de la minceur de l'offre du marché* (SIC), il a été décidé de fournir gratuitement et en ligne, un certificat. La contrepartie de la gratuité est que ce certificat n'est utilisable que pour cet e-service. Plus tard, dans quelques années, le certificat pour cet e-service devra entrer totalement dans le cadre réglementaire du ministère, et être acquis auprès d'une autorité de certification agréée. Il sera alors banalisé et utilisable pour d'autres transactions Internet.

3.4.1.2. L'emploi d'une signature électronique

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. Son rapport portait sur la question de la dématérialisation de la signature : "*la signature numérique" constitue-t-elle une véritable signature juridique ?*" était la grande question posée. Entre autres questions, le groupe de travail de l'O.J.T.I. s'était attaché à déterminer les rôles de la signature. Au regard de la personne qui rédige et signe un acte, elle a dégagé trois rôles qui interviennent simultanément :

- Identification de l'auteur de l'acte en même temps signataire : identifier la personne, c'est disposer d'informations permettant de l'individualiser (nom, prénom, dénomination sociale, adresse...) ;
- Authentification du signataire : l'authentification de l'auteur de l'acte s'opère par des informations qui assurent que la personne ayant apposé sa signature est bien celle indiquée comme signataire de l'acte ;
- Authentification de la volonté du signataire d'adhérer au contenu de l'acte : adhérer au contenu de l'acte signé, c'est établir un lien intellectuel entre la signature et le contenu du document : le signataire accepte d'être lié par les dispositions de cet acte. La signature exprime la volonté personnelle du signataire d'adhérer à ce qui a été signé et de se l'approprier[60].

Ce 3ème point est à relever et à rapprocher des caractéristiques de la signature électronique telles qu'on peut les relever dans l'article 1316-4 :

- manifestation du consentement du signataire aux obligations qui découlent de l'acte signé,
- assurance de l'identité du signataire et garantie d'intégrité de l'acte.

Pour ce qui est de la transmission de la télédéclaration, la manifestation du consentement du signataire n'est pas à l'ordre du jour, alors que l'identification et l'intégrité sont requises. Comme les besoins ne sont à pas à proprement juridiques, parce que par exemple, ils ne visent pas à l'appropriation du message par le signataire et ne formalisent pas son accord sur le contenu juridique de l'acte, une signature numérique sera suffisante. La signature électronique ou numérique des techniciens 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)".*

Si cette signature électronique ne présente pas la caractéristique fondamentale du droit civil (la manifestation du consentement), il n'est pas possible d'objecter sa nature technique pour l'écarter en cas de litige. Elle entre en effet dans la définition de l'article 2 de la Directive du 13 décembre 1999. L'article 2 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".* 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. Cependant elle ne reste pas privée de tout effet juridique, on peut le voir avec 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".*

Ainsi la signature numérique sera admissible en cas de litige, mais sa portée sera nécessairement limitée à la sécurité technique de la transmission, mais non à la sécurité juridique de la dématérialisation de la téléprocédure[61].

A défaut de signature un simple certificat pourrait suffire comme pour les déclarations de TVA. Les professionnels peuvent déclarer et payer la TVA et consulter leurs comptes TVA par le "*e-service TéléTVA*". Le certificat nécessaire pour sécuriser les échanges répond aux règles forgées par la DGI : le certificat provient

[60] Planiol et Rippert, Traité pratique de droit civil français, Tome VII 2ème édition 1954, n°1458. Ghestin J. et Goubeaux J., Traité de droit civil, Tome 1 les obligations, Paris 1980, n°621-22.

[61] Pour renforcer cette analyse, voir notre article sur la facture électronique "*La facture électronique entre dématérialisation documentaire et signature électronique*", Jurisclasseur Communication et Commerce Electronique – mai 2003, chr. 12.

d'une autorité de certification reconnue par le ministère, et totalement standard. Ce certificat dit "*certificat référencé"* est acquis auprès d'une autorité de certification recensée par le ministère. La FAQ du site donne les explications suivantes sur le certificat numérique[62] employé :

> ***A quoi sert le certificat numérique ?***
> *Le certificat numérique joue le rôle de pièce d'identité (passeport électronique). Il permet de garantir que Monsieur X est bien Monsieur X.*
> *Dans TéléTVA, le certificat contient l'ensemble des informations permettant cette identification (nom, prénom éventuellement, entreprise, SIRET, adresse, …). Il sert donc à l'authentification et permet également de signer les échanges électroniques garantissant ainsi la non-répudiation de l'échange et son intégrité. Il permet d'établir un environnement de confiance entre deux entités distantes qui ont besoin de communiquer entre elles.*

Constatons que le certificat permet de "*signer les échanges électroniques*"[63], ce qui laisse présager de la présence d'une signature électronique à proprement parler. Les *Questions – réponses* du site le disent à un autre endroit :

> *Q : Comment l'administration a-t-elle la preuve que c'est bien moi qui ai adressé ma déclaration et non une autre personne ?*
> *R : Grâce à votre signature électronique qui permet d'authentifier avec certitude l'émetteur d'un message reçu.*

La plaquette TéléTVA n'est pas plus claire. Elle est confuse sur la liaison certificat – signature et introduit la confidentialité :

> *Les échanges par l'Internet requièrent des solutions de sécurité adaptées aux réseaux ouverts. A cet égard, TéléTVA met en œuvre le dispositif utilisable pour **toutes les téléprocédures** du ministère destinées aux entreprises.*
> ***Les échanges seront signés et chiffrés**. La signature électronique assortie d'un certificat garantit l'authentification des internautes, l'intégrité des messages envoyés, leur non-répudiation par l'émetteur.*
> *Le chiffrement (ou cryptage) garantit la confidentialité des échanges.*
> *Les échanges EDI (TDFC et EDI-TVA) sont sécurisés par l'emploi de réseaux protégés, de messageries spécialisées (TEDECO) et du dispositif de scellement des envois hérité du monde bancaire (protocole EDI).*

Le bilan est ainsi assez contrasté. L'interrogation sur la dimension juridique de la signature paraphant le formulaire papier laisse entendre que l'*identification du déclarant* est l'élément important. Ce qui nous renverrait, au plan des échanges électroniques, à l'utilisation d'un simple certificat. Dans le concret, le site TéléTVA ne demande qu'un certificat référencé, bien que la documentation en ligne parle de signature électronique. Est-ce une erreur ou bien la prochaine évolution du service exigera-t-elle une signature électronique, signature dont l'utilité juridique reste contestable ?

3.4.1.3. Une signature numérique dans les téléprocédures

Si une signature électronique est finalement choisie, l'administration devra dire si elle est *sécurisée* ou non. La signature électronique sécurisée est accompagnée d'un *certificat qualifié*. Dans ce cas, le certificat serait assurément référencé et qualifié à la fois. En clair, il devrait passer un double audit, donc un audit de trop. Ou bien l'administration garderait une signature électronique juridique mais non sécurisée et accompagnée d'un certificat référencé. Peut-on imaginer qu'il existe une signature électronique de droit privé et une autre de droit public ?

La solution semble plus simple en considérant qu'il y a deux types de signature. Le contrat "General Legal Agreement" présenté dans un document de la Commission Economique pour l'Europe des Nations-Unies de février 2003[64], malgré son application au monde des échanges B to B, livre certains enseignements. Il prévoit deux types de signatures, une signature électronique et une signature numérique ("digitale" en anglais). En

[62] On notera le qualificatif de *numérique* appliqué au certificat et non celui d'*électronique*, comme l'établit le décret d'application de l'article 1316-4 du Code Civil. Est-ce une erreur, un oubli ou cela montre-t-il que la DGI ne se place pas dans un contexte juridique ?

[63] Ce qui est d'ailleurs un abus de langage. Le certificat (même numérique) ne permet pas de signer les échanges électroniques, mais de vérifier la signature des échanges signés.

[64] TRADE/CEFACT/2003/19 du 27 février 2003 "Trading Partner Agreement"

négligeant les technologies employées, la "signature électronique"[65]est appliquée à un document par une personne avec l'intention de le signer. Le fait que la définition vise l'acteur humain et un document comme support montre à l'évidence que cette signature possède une dimension juridique. Dans l'article 9 du contrat, les parties conviennent expressément par l'accord que le message / document paraphé par la signature électronique est considéré comme un "écrit" -nous dirions un écrit-papier"- et constitue un "original".

Le second instrument, la signature numérique[66], sert plus prosaïquement à assurer de l'identité de l'expéditeur du message / ou du signataire du document et de l'intégrité du message à destination. L'article 10 de l'accord prévoit que chaque partie doit signer avant la transmission à l'autre partie. Cette dernière devra à son tour vérifier l'identification et l'intégrité assurées par la signature numérique. Cette signature est entièrement tournée vers les garanties de sécurité de sorte qu'on peut en déduire que sa fonction principale sert à la sécurisation de l'échange électronique. Cette solution est conforme à celle qui peut être imaginé pour les messages électroniques de droit commun vis la messagerie électronique[67]

3.4.1.4. Les certificats référencés

Si la signature nécessitée pour la sécurisation de la transmission des téléprocédures est une signature numérique, le référencement des certificats n'entre naturellement pas en conflit avec la qualification des certificats.

Les dernières informations données par l'administration permettent de confirmer le résultat des réflexions précédentes.

Dans ces conditions, une téléprocédure pourrait faire appel à deux signatures conjointement pour des finalités résumées dans le tableau ci-dessous :

Niveau	***Acteur***	***Moyens***
Approbation de la téléprocédure lors de sa formation	Déclarant	Signature électronique du Code Civil
Sécurisation de la transmission électronique	Expéditeur	Signature numérique des techniciens

[65] *Electronic Signature : An Electronic Signature means an electronic sound, code, symbol, or process, attached to or logically associated with a contract or other document and executed or adopted by a person with the intent to sign the document.*

[66] *Digital Signature : A Digital Signature is an Electronic Signature that can be used to authenticate the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged.*

[67] Cf. notre article "*Transmission et preuve de l'écrit électronique, deux niveaux de signatures*", Lamy Droit de l'Informatique et des Réseaux – fasc. 158, mai 2003.

L'idée d'apposer deux signatures pour une même téléprocédure est logiquement dérangeante. Mais comment s'en dispenser faute d'un véritable recommandé électronique ?

3.4.2. L'assurance d'un bon acheminement

Un expéditeur de courrier par voie postale peut avoir besoin de se garantir de la délivrance certaine de son envoi auprès du destinataire. Il obtient cette garantie grâce à une procédure de recommandé postal avis de réception. Il pourrait obtenir la même assurance si le destinataire accuse réception spontanément.

3.4.2.1. Vers le recommandé électronique

Le destinataire de l'acte sous forme électronique attend des certitudes quant à l'identification et l'intégrité du message. Il y manque encore 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). 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.

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*[68]. On peut observer cependant les enseignements d'autres législations, comme celle du Luxembourg[69]. 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[70] qui intègre *l'heure, la date, l'envoi et le cas échéant la réception* sous la certification de

68 Ni recommandé électronique, ni avis de réception. Un *décret n°2001-492 du 6 juin 2001 (...) relatif à l'accusé de réception* (sic) *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.

69 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

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

l'archiveur de confiance. La leçon à en tirer est que l'horodatage 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.

A défaut de recommandé électronique mis en œuvre par le déclarant, il est possible d'envisager qu'à l'inverse, l'administration destinataire accuse réception. Dans le cas de TéléTVA, la déclaration et l'ordre de paiement sont envoyés dans le même message. En retour, TéléTVA informe de la bonne réception de la déclaration et de la prise en compte du paiement. La délivrance d'un avis de dépôt de la déclaration informe les redevables de la réception de leur envoi par la DGI. Un Certificat de Prise en compte de l'Ordre de Paiement (CPOP) sera délivré lors de la mise en paiement.

3.4.2.2. Vers l'accusé de réception administratif

Une mesure pratique pour l'amélioration des relations entre les usagers et les administrations consiste en l'assurance donnée par l'administration que les demandes et requêtes des usagers ont bien été reçues. Ce pas a été franchi par La *loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations* (dite loi DCRA). Avec ce texte l'obligation de confirmer la réception des demandes d'usagers est étendue à l'ensemble des services administratifs. Le Décret no 2001-492 du 6 juin 2001[71] est venu préciser l'application de l'accusé de réception.

Selon l'article 1 du Décret, l'accusé de réception prévu par l'article 19 comporte les mentions suivantes :
- La date de réception de la demande et la date à laquelle, à défaut d'une décision expresse, celle-ci sera réputée acceptée ou rejetée. L'accusé de réception indique si la demande est susceptible de donner lieu à une décision implicite de rejet ou à une décision implicite d'acceptation. Dans le premier cas, l'accusé de réception mentionne les délais et les voies de recours à l'encontre de la décision. Dans le second cas, il mentionne la possibilité offerte au demandeur de se voir délivrer une attestation prévue à l'article 22 de la loi du 12 avril 2000 susvisée.
- La désignation, l'adresse postale et, le cas échéant, électronique, ainsi que le numéro de téléphone du service chargé du dossier.

L'article 3 du Décret explique qu'au contraire, l'accusé de réception ne sera pas délivré, ce qui pourrait jouer pour une déclaration administrative, notamment lorsqu'une décision implicite ou expresse est acquise en vertu des lois et règlements au profit du demandeur, au terme d'un délai inférieur ou égal à quinze jours à compter de la date de réception de la demande.

Dans son contexte réglementaire, on envisage naturellement un accusé de réception sous forme écrite. L'accusé de réception peut-il être électronique ? De façon générale, la Loi DCRA indique que la communication par l'administration de documents administratifs par courrier électronique est désormais possible. Mais seulement si l'administration dispose de ce document sur support identique à celui demandé. Il semble que cette disposition puisse servir de fondement indirect dans la demande d'un administré d'obtenir un accusé de réception, suite à la transmission d'une téléprocédure.

Naturellement si le principe d'un accusé de réception électronique était accepté en retour d'une téléprocédure, cela ne résoudrait pas la question de savoir de quelle forme pourrait être cet accusé et s'il mettrait en œuvre directement ou non une signature électronique avec horodatage.

[71] Décret no 2001-492 du 6 juin 2001 pris pour l'application du chapitre II du titre II de la loi no 2000-321 du 12 avril 2000 et relatif à l'accusé de réception des demandes présentées aux autorités administratives, J.O. Numéro 133 du 10 juin 2001 page 9246

3 Synthèse

L'émergence d'Internet laisse augurer une simplification des relations juridiques dans la société française en permettant de renoncer dans une large mesure à l'écrit-papier. L'électronique peut être employée pour créer des documents de nature juridique, pour les transmettre puis les conserver, aussi bien dans les rapports entre particuliers que dans ceux des entreprises avec les administrations, notamment dans les téléprocédures. Mais pas à n'importe quelles conditions : l'efficacité, la simplicité et la rapidité ne peuvent pas et ne doivent pas prendre le pas sur la sûreté juridique.

L'abandon du papier est une question relative à la forme des documents juridiques

Abandonner le support papier (écrit), c'est se priver d'un des piliers du système juridique. Les juristes mettent en avant l'incertitude qui en découle dans l'administration de la preuve. Mais le précédent de l'EDI montre qu'un autre concept juridique est atteint prioritairement, le formalisme juridique. L'écrit sous forme électronique est entré dans le Code Civil en même temps que la signature électronique. Dans cette perspective, les déclarations administratives peuvent-elles évoluer vers des téléprocédures ? L'analyse juridique est seule en mesure de démontrer qu'une déclaration déterminée sur support papier peut migrer vers la forme électronique d'une téléprocédure si et seulement si le formalisme juridique est respecté.

Le formalisme juridique appliqué au document manifeste toute sa rigueur dans les pays de droit civil comme la France. Il repose sur l'obligation de respecter les trois éléments suivants :
- un support papier,
- l'apposition d'une signature autographe ou manuscrite,
- la présence de mentions obligatoires.

Pour chaque document ou déclaration que l'on souhaite dématérialiser, il est nécessaire de procéder à une analyse juridique spécifique qui consiste à :
- identifier dans les textes légaux et réglementaires les dispositions qui imposent des contraintes de formalisme documentaire,
- procéder à un audit de dématérialisation,
- préconiser, enfin, les moyens techniques nécessaires, moyens reconnus par le Droit, pour valider la dématérialisation du document papier et pour sécuriser la transmission de la forme électronique correspondante.

Premier but à atteindre : valider la dématérialisation du document papier et sa transformation en écrit électronique

Jusqu'ici les deux premiers éléments du formalisme (papier et signature) étaient suffisants pour s'opposer définitivement à la dématérialisation d'un acte ou d'une déclaration. Désormais le blocage pourra être supprimé dans la quasi-totalité des cas :
- d'une part, parce que la signature électronique de l'article 1316-4 du Code civil peut se substituer à la signature manuelle ou autographe sur un papier,
- d'autre part, parce que la Loi sur la confiance dans l'Economie Numérique (LEN), qui devrait être très prochainement adoptée, autorisera le passage du support papier à la forme électronique, à condition de mettre en place les garanties exigées par le faible niveau sécuritaire d'Internet, à savoir l'identification de la source et l'intégrité.

A noter que sur ce dernier point, identification de la source et intégrité peuvent être assurées par une signature numérique c'est-à-dire le même moyen technique que la signature électronique, sans les caractéristiques et les effets juridiques prévus par la loi.

Second but à atteindre : sécuriser la transmission de la forme électronique obtenue

Le but de l'opération est ici de prendre en compte par des moyens sécuritaires adaptés les caractéristiques juridiques atteintes lors de la dématérialisation documentaire et de les maintenir tout au long de la transmission électronique.

Les garanties de sécurité à prévoir sont celles qui sont issues de la Loi Madelin qui doit désormais être envisagé à la lumière des modifications récentes (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) et à venir (la LEN). Les garanties sont les suivantes :

- identification et intégrité, parmi les garanties classiques de sécurité,
- horodatage, si important dans un domaine où la déclaration (et le paiement) doit être accompli avant une certaine date ou pendant un certain délai.

Ici encore, l'identification et l'intégrité qui visent à sécuriser la transmission peuvent être pris en charge par la signature numérique. Il en est de même pour l'horodatage à défaut d'un procédé recommandé électronique prévu par le Droit.

Il importe en définitive de distinguer l'intervention des deux types de signature : signature numérique et signature électronique. Le tableau ci-dessous peu en donner une idée.

Niveau	*Acteur*	*Moyens*
Approbation de la téléprocédure lors de sa formation	Déclarant	Signature électronique du Code Civil
Sécurisation de la transmission électronique	Expéditeur	Signature numérique des techniciens

Pour résumer...

Ainsi la signature numérique et/ou la signature électronique pourraient intervenir à plusieurs niveaux pour la mise en place d'une téléprocédure. Il revient à l'analyse juridique de déterminer lesquelles sont indispensables pour une téléprocédure spécifique. Il lui incombe de réaliser les arbitrages et de préconiser l'emploi de moyens ou de mesures techniques adaptées à la téléprocédure et aux circonstances.

En résumé, un diagramme de la problématique juridique ressemblerait à ce qui suit :

<table>
<tr><th colspan="2">LA DECLARATION</th><th colspan="2">LA TRANSMISSION</th></tr>
<tr><td colspan="2">Dimension juridique :

3.1.1.1.1

3.1.1.1.2 Dématérialisation des déclarations

Notion juridique concernée :

3.1.1.1.3 Le Formalisme juridique</td><td colspan="2">Dimension juridique :

Sécurisation de la transmission

Notion juridique concernée :

Déclaration par voie télématique</td></tr>
<tr><td>Problème :

- Support papier

- Signature obligatoire ?

- Mentions obligatoires ?</td><td>Solutions :

⇨ Loi Economie Numérique

⇨ Signatures Electroniques du Code civil

⇨ Messages structurés</td><td>Problème :

- QUI ?
- QUOI ?

COMMENT ?

- QUAND ?</td><td>Solutions :

⇨ Authentification
⇨ Intégrité
= Signature numérique

⇨ Chiffrement facultatif

⇨ Horodatage fiable</td></tr>
</table>