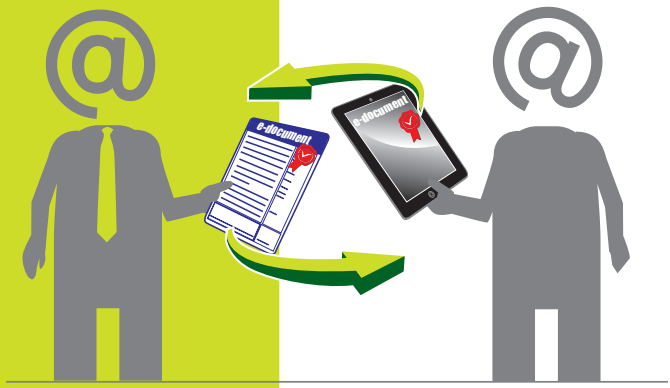
Fédération Nationale des
Tiers de Confiance

GUIDE DU DOCUMENT HYBRIDE ET DE LA CERTIFICATION 2D

Passer en toute confiance du numérique
au papier et inversement



COLLECTION
LES GUIDES DE LA CONFIANCE
DE LA FNTC

Par le groupe de travail « mode hybride »
de la Fédération Nationale des Tiers de Confiance

DANS LA COLLECTION LES GUIDES DE LA CONFIANCE DE LA FNTC,


Guide du Document Hybride et de la Certification 2D (déc. 2011)


Vade-mecum juridique de la dématérialisation des documents nouvelle édition (juin 2011)


Fascicule e-paie « le rôle du bulletin de paie dans la reconstitution de carrière » (mars 2011)


Guide du vote électronique, nouvelle édition (mars 2011)


Guide de l'archivage électronique et du coffre-fort électronique (nov. 2010)


Au-delà de la migration Etebac (sept. 2010)


Guide de la Facture électronique (janv. 2010)


Du mandat au mandat électronique (déc. 2009)


Guide de la signature électronique (sept. 2008)

SOMMAIRE

INTRODUCTION

La dématérialisation est irréversible et touche chacun de nous : particulier, citoyen, professionnel, mais aussi entreprises, institutions…

Notre capacité à agir dans « le monde numérique » augmente à chaque instant. La France compte aujourd'hui 38 millions d'internautes, dont 20 millions d'abonnés ADSL (février 2011, source Médiamétrie), l'Allemagne 40 millions d'internautes, le Royaume Uni 36,8 (source Comscore).

L'accès au haut débit est très répandu en France. Le taux d'équipement est également assez important : ordinateurs, smartphones, imprimantes multifonctions. Scanner, recevoir, lire, imprimer, écrire, échanger via e-mail… c'est aujourd'hui très simple.

Pourtant, le « tout numérique » n'existe pas, pas encore, ou peut-être pas du tout. Chaque document émis est aussi imprimé, retransmis sous forme papier à un tiers. Ce tiers, qu'il soit particulier ou professionnel, l'utilise ensuite, après parfois une coûteuse vérification, pour des processus importants (carte électeur ou pièce d'identité, dossier de crédit, etc.).

La FNTC a établi de nombreux référentiels de valeurs dans le monde numérique : sur l'archivage à vocation probatoire, la facture électronique, le coffre-fort électronique par exemple. Ces techniques sont maintenant mûres et permettent d'étendre un climat de confiance propice aux affaires et à la productivité dans le monde numérique.

Mais comment s'assurer, avec la même confiance, de l'intégrité d'une facture imprimée, d'un bulletin de paie numérique imprimé et photocopié, d'un e-contrat redevenu simple contrat papier ?

En effet, ces logiciels de traitement d'image, qui font avancer le numérique, peuvent aussi servir à tromper, en maquillant ou modifiant les informations d'un document. La fraude aux documents, sur les factures, bulletins de paie, peut se chiffrer en centaines de millions d'euros, rien que pour le secteur bancaire français (dossier de crédit, leasing,…).

Le changement de « statut » d'un document, son passage du mode numérique au mode papier, et inversement, pose la question de la valeur du document, mais aussi de son information :

• Un document numérique, justificatif de domicile, reste-t-il un original fiable quand il est imprimé pour remplir un dossier administratif ?

• Un bulletin de paie numérique imprimé pour un dossier de crédit, est-il réellement intègre sur la valeur du salaire ?

• Au-delà du support, papier ou numérique, n'y a-t-il pas des informations propres à chaque document qu'il faut protéger, sécuriser, afin qu'elles restent intègres au fil du temps et moins sensibles à la fraude ?

• Enfin, n'y a-t-il pas des gains de productivité possibles en associant écriture lisible et « écriture numérique » sécurisée ?

Le document « hybride » permet un changement de statut, à la fois numérique et papier, toujours intègre et fiable dans ses informations.

En parallèle des travaux menés par l'état français sur la lutte contre la fraude documentaire, la Fédération Nationale des Tiers de Confiance a donc souhaité organiser ce groupe de travail pour définir plus en détails la notion de « document hybride ». Ses caractéristiques, à chaque statut, ses prérequis technologiques, organisationnels, juridiques, et sa valeur ajoutée dans notre monde d'aujourd'hui et de demain.

Le présent guide est une première version, qui n'a pas vocation à être exhaustive, et présente le recueil des technologies du marché, le contexte juridique, des cas d'usages pertinents et quotidiens, et une vision plus prospective de ce que pourra être, bientôt, un monde encore plus confiant !

****

1. CONTEXTE JURIDIQUE

1.1 Equivalence juridique des signatures électroniques et manuscrites

Juridiquement et depuis la loi n°2000-230 du 13 mars 2000 (transposant la directive n°1999-93 du 13 décembre 1999) qui modifie le droit de la preuve, le droit évolue dans l'utilisation de l'écrit électronique en lui conférant la même force probante que l'écrit papier. Elle introduit l'article 1316-3 du Code civil et pose le principe que « l'écrit sur support électronique a la même force probante que l'écrit sur support papier » sous réserve de respecter certaines conditions : la personne dont il émane doit pouvoir « être dûment identifiée » et il doit être « établi et conservé dans des conditions de nature à en garantir l'intégrité » comme l'énonce l'article 1316-1 du Code civil.

Puis, la loi du 21 juin 2004 a complété le Code civil afin d'admettre, à l'article 1108-1 (et sous réserve des exceptions de l'article 1108-2), non plus l'équivalence en terme de preuve mais également l'équivalence en terme de validité de l'écrit et de la signature que l'on peut désigner comme « manuscrite », lorsque la signature est requise à ce titre par les textes.

Ainsi, lorsque le document à établir nécessite un formalisme particulier afin que l'acte acquière sa pleine validité (engagement de grande importance) ou que sa preuve nécessite d'être apportée suivant les critères posés par le cadre législatif (contrat d'un montant supérieur à 1.500 euros par exemple – décret n° 2004-836 du 20 août 2004), la signature électronique, en identifiant le signataire (via la fonction d'identification) et en liant le contenu à cette identification (via la fonction d'intégrité), permet de démontrer le consentement du signataire à l'acte juridique, rendant celui-ci parfait.

L'article 1316-4 du Code civil, issu de la loi n°2000-230 du 13 mars 2000, indique ainsi que :
« 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. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.
Lorsqu'elle est électronique, 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 ».

1.2 L'hybridation au plan juridique

Au plan juridique, les avancées vers une reconnaissance du passage facilité de l'écrit à l'électronique ou de l'électronique au papier (interchangeabilité des supports) sont encore timides alors même que l'équivalence entre les documents nativement sur support papier et les documents nativement électroniques a été reconnue, comme indiquée précédemment. En introduisant dans le Code civil la notion d'écrit « originairement » électronique, la loi n°2000-230 du 13 mars 2000 n'a toutefois pas été jusqu'à prévoir, contrairement à la loi québécoise, la possibilité d'hybridation du document (original électronique puis papier et réciproquement).

Il a fallu attendre l'Ordonnance n° 2005-674 du 16 juin 2005 en matière de lettre recommandée (cf. 4.1) afin de voir, pour la première fois, la reconnaissance de la notion d'hybridation dans le droit français, c'est-à-dire la reconnaissance du changement de support d'un document tout en assurant la conservation de la valeur juridique identique à celui-ci. Bien que dans une bien moindre mesure, l'instruction fiscale du 11 janvier 2007 a également reconnu une pratique d'hybridation de certaines factures (cf. 4.2.2 ci-après). Et encore cela ne fonctionne-t-il que dans un seul sens, de la forme papier vers la forme électronique. L'inverse est donc interdit.
Pour le reste, les exigences du droit fiscal imposent une prise en compte d'une chaîne de traitement papier (souvent historique) en parallèle d'une chaîne de gestion électronique (l'avenir) sans que le panachage soit facile à vivre ou générateur d'économie.

D'autant que, protection du consommateur oblige, celui-ci se voit par exemple reconnaître le droit de demander à continuer à recevoir du papier (Alinéa 3 de l'article L. 121-20-11 du Code de la consommation) en matière de commercialisation à distance de services financiers.

Hormis ces exigences où la forme de documents particuliers tels que les factures est imposée, reste le domaine :
• des **actes juridiques** (les contrats pour l'essentiel). Ceux-là ne peuvent changer de forme sans que l'on considère que leur résultante est une « copie », qui se doit d'être « fidèle et durable » (article 1348 alinéa 2 du Code civil) si l'on veut qu'elle remplace un original perdu ou détruit. Sinon, l'original prévaudra en tout état de cause. Et la jurisprudence est encore peu prolixe sur l'interprétation de cette notion, souhaitée par le législateur en 1980 pour accueillir la copie (et la destruction des originaux) des chèques sur microfiches. Les entreprises, lorsqu'elles effectuent cette transition, doivent donc analyser les contrats concernés, les exigences juridiques auxquels ces actes sont soumis et les risques encourus (la stipulation d'intérêt, à titre de validité, entraîne l'application du taux d'intérêt légal si l'écrit (contenant la stipulation d'intérêt) signé n'est pas reconnu comme valide par le juge) afin d'apprécier les risques et de mettre en œuvre les procédures de contournement et/ou d'accompagnement (politique de numérisation, politique de destruction, politique d'archivage, etc.) ;
• des **faits juridiques** (justificatifs divers et variés, notes récapitulatives de frais, bulletins de paie, etc.) pour qui, hors exigences particulières afférentes à la confiance que les parties peuvent y apporter (ex : bulletins de paie dont la remise doit être effectuée dans des « conditions de nature à en garantir l'intégrité » si elle est électronique – article L. 3243-2 du Code du travail), peuvent passer d'un état à l'autre sans que le droit y trouve à redire : leur valeur juridique en terme de preuve sera identique c'est-à-dire faible et dépendant entièrement de l'appréciation des magistrats.

L'un des problèmes majeurs de l'hybridation a trait à l'interchangeabilité des supports (notamment du papier vers l'électronique) et de la destruction de l'original papier.

Ainsi, l'article 1334 du Code civil dispose que *« les copies lorsque le titre original subsiste ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée. »*

Pour faire application des dispositions de l'article 1348 du Code civil (précité) il faut prouver que :
• le titre original n'a pas pu être conservé ;
• la copie de l'original en est une reproduction fidèle et durable.

Les juges disposent d'un pouvoir souverain d'appréciation du caractère fidèle et durable de la copie par rapport au document original. Se pose ainsi la question de la valeur légale

incertaine des documents archivés électroniquement.
Les conséquences juridiques de la destruction du document papier original pourraient donc être considérables dans le débat judiciaire ; certaines preuves pouvant ne pas être reçues par le juge.

Afin de faciliter l'interchangeabilité des supports et la destruction des originaux papiers, il conviendrait d'apporter des modifications substantielles au Code civil.

2. ETAT DE L'ART

Il existe bien évidemment sur le marché différents dispositifs consistant à utiliser des supports spéciaux ou des mécanismes de sécurité comme les hologrammes, les encres magnétiques, le marquage, etc. Le groupe de travail s'est volontairement concentré ici sur les technologies numériques accessibles et manipulables avec un équipement standard.

2.1 Signature électronique

La signature électronique est aujourd'hui une réalité, prenons un exemple de la vie quotidienne : le passeport électronique ou biométrique[1] . Ce passeport est l'exemple même de ce qui nous entoure et qui combine à la fois la matérialisation physique d'un objet et l'utilisation de la signature électronique.

D'apparence identique et mentionnant les données qui caractérisent chacun d'entre nous (nom, prénom, date de naissance…), il intègre également ces données dans une puce sans contact insérée dans la couverture. Elles sont complétées par la photo numérisée, deux empreintes digitales sur les huit prélevées et une signature électronique, apposée par l'Etat émetteur du passeport biométrique, qui garantit qu'il est impossible de modifier ces informations. De fait, lors d'un contrôle aux frontières, l'agent va pouvoir lire les données imprimées sur le passeport grâce à la bande MRZ (Machine Readable Zone ou bande de lecture optique) et les comparer à celles présentes dans la puce ; toute différence sera immédiatement détectable grâce à la vérification de la signature électronique. Il y a donc un contrôle d'intégrité (elles n'ont pas été modifiées) et d'authenticité (elles proviennent bien de l'Etat émetteur). Pour autant, l'utilisation de cette signature électronique est transparente pour le titulaire du passeport qui s'en sert comme auparavant. Nous avons ainsi un très bon exemple de l'utilisation d'une technologie sans perturbation pour les utilisateurs que nous sommes.

---

1 Le passeport électronique, qui intègre des données biométriques, est encadré par le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques et reprenant les obligations issues du règlement (CE) n° 2252/2004 du 13 décembre 2004 du Conseil. Modifié par le décret n°2008-426 du 30 avril 2008 (puis par le décret n° 2010-506 du 18 mai 2010), le passeport n'est plus mentionné comme étant « électronique », signe des temps et de l'assimilation souhaitée à l'ancien passeport « classique ».

L'application de la signature électronique à tout type de document est donc à portée de main, car :
• Les technologies sont matures ;
• Le contexte légal et réglementaire existe ;
• La volonté politique est présente ;
• Les besoins (latents ou exprimés) demandent cette mise en application.

Que garantit la signature électronique ? Au plan technique, la signature électronique assure deux fonctions principales :
• Tout d'abord, la signature électronique assure l'intégrité d'un document. Elle permet ainsi de vérifier qu'un document n'a pas été modifié depuis qu'il a été signé. Toute modification du document entraîne automatiquement une incohérence entre la signature électronique et le document qui est censé s'y rattacher ;
• Ensuite, et c'est l'aspect que nous connaissons tous par rapport aux signatures sur support « papier », la signature électronique assure le lien entre le document et le signataire.

On voit donc que la signature électronique dépend de ce qu'on peut appeler « une identité numérique » qui va représenter une personne physique ou morale (pour certains documents comme les factures électroniques). Cette identité numérique (matérialisée par un certificat électronique) est associée de manière unique à une clé qui va être utilisée par un logiciel de signature (que l'on peut assimiler au stylo). L'association des deux permet de réaliser la signature électronique sur les données à signer, que ces données composent un document (bureautique ou non), une image, une transaction…

Dans le cadre de ce guide, la signature électronique est plutôt envisagée pour garantir l'authenticité d'une ou plusieurs informations portées sur un document, tel que le domicile sur une quittance, les mentions fiscales obligatoires sur une facture, etc. D'ailleurs, quand l'importance du document pour l'Etat le nécessite, comme dans le cas des factures vis-à-vis des contrôles opérés par l'administration fiscale, la loi impose d'elle-même que l'intégrité de ces documents soit techniquement assurée, comme dans le cas des factures transmises par voie électronique (cf. 3.2 du présent guide).

D'autre part, les documents sont envisagés comme pouvant exister sous leur forme numérique ou imprimée, ce qui veut dire que, pour la version imprimée, la signature doit pouvoir être représentée sous une forme visualisable et interprétable par un mécanisme d'acquisition d'image (scan, LAD/RAD, etc.)

Deux aspects sont donc nécessaires à prendre en compte:

• Avoir la capacité de traiter en masse ces documents pour respecter les impératifs industriels (liés notamment aux lots pour les factures EDI ou signées par exemple) tout en assurant la sécurité des données grâce à leur signature électronique, que cette sécurité soit requise à des fins opérationnelles ou s'impose dans certains cas pour des raisons juridiques;
• Avoir la capacité de vérifier cette signature au travers d'outils simples et déployables pour les systèmes/personnes qui vérifieront les signatures

En conséquence, les outils de validation des signatures peuvent être centralisés pour la gestion des documents sécurisés ou déportés au niveau bureautique selon les capacités techniques et les formats de documents. Ainsi, la validation d'une signature de justificatif de domicile, acquise au travers d'une chaîne éditique entrante va nécessiter de disposer d'une solution serveur alors que la validation de signature électronique sur un document de type PDF peut se faire au travers d'outils de type Adobe Reader sans nécessiter de déploiement spécifique.

Pour plus d'informations sur la signature électronique, se reporter au *« Guide de la signature électronique » de la FNTC (2008)*.

2.2 Les codes 2D

La sécurisation d'un document hybride peut être assurée par l'utilisation d'un code 2D.
Cette sécurisation s'effectue en encapsulant les informations « critiques » d'un document dans le code 2D. Le principe en est simple.
Lors de la création du document à sécuriser, il convient de créer un code 2D qui reprendra les informations à protéger.
Au moment de la vérification des informations critiques, il faudra rapprocher les informations en clair, de celles figurant dans le code 2D. L'intégrité de ces informations critiques est assurée par un procédé d'empreintes et de signatures asymétrique.

Si les données figurant en clair sur le document sont identiques à celles contenues dans le code 2D, alors ces données sont exactes. Dans le cas contraire, elles sont fausses.

C'est une approche que semble considérer l'état français pour la sécurisation des « factures[2] » utilisées comme des justificatifs de domicile, en particulier lors de l'établissement des papiers d'identité.

Il existe de nombreux codes 2D dont la plupart ressortent de la même logique.

Il s'agit des codes dits « globaux » (ou encore « matriciels ») qui sont des images créées à partir d'un algorithme. Le plus connu et le plus utilisé en Europe est le Datamatrix. Son pendant asiatique est le QR Code. Il existe également de « faux » codes 2D, qui sont en fait des codes-barres 1D empilés tel que le PDF417.

Distincte des codes 2D globaux, une nouvelle sorte de code 2D vient d'apparaître, sous forme d'écriture numérique, dont l'Alphacode est un des représentants (voir chapitre 2.2.2).

2.2.1. Les codes 2D globaux

Les plus utilisés sont le Datamatrix et le QR code.
Différent des « codes à barres » qui sont composés de barres noires de différentes largeurs et d'espaces blancs (tel que l'EAN 13 qui figure sur les articles passant aux caisses des commerces et qui encode uniquement les treize chiffres du code article), un code 2D est une image constituée (le plus souvent) d'un ensemble de carrés noirs et blancs (dots en anglais).

Les codes 2D ont donc pour base des surfaces élémentaires binaires. L'information codée est alors représentée sous forme de bits.

---

2 Ces documents sont en réalité des récapitulatifs de frais envoyés au grand public, notamment par les fournisseurs d'eau, d'énergie ou encore de communications électroniques. Juridiquement, ce ne sont pas des factures au sens fiscal du terme – bien qu'ils soient qualifiés ainsi par le grand public - car il n'y a pas de problématique de déduction de TVA entre entreprises et particuliers expliquant les formes imposées par la législation fiscale, cf. 3.2.

Chaque code 2D se différencie par des éléments de graphisme caractéristiques permettant aux logiciels de lecture à la fois sa localisation et son identification. Ce graphisme constitue un repère permettant une lecture multidirectionnelle.

Tous ces codes 2D sont créés à l'aide d'un logiciel appelé « générateur » qui code de manière globale une chaîne de caractères en fonction de divers paramètres (taux de redondance, taille des dots…).
Pour enlever ou ajouter un ou plusieurs caractères, le générateur recompose totalement une image 2D globale en utilisant de nouveau ses algorithmes de codage.

La forme principale de tous ces codes est carrée. Ils peuvent quelquefois se présenter sous forme rectangulaire.

Leur taille dépend du nombre de caractères à encoder. A noter que l'accroissement du nombre de caractères à encoder ne se répercute pas de manière strictement linéaire sur la taille du code. L'accroissement de la taille du code 2D se fait par saut. Autrement dit, la surface d'impression n'est pas directement proportionnelle à la quantité d'informations codées.

Néanmoins un code 2D s'accroît significativement en hauteur et en longueur avec la quantité d'informations codées. Si cette particularité peut être adaptée à des utilisations isolées, elle devient très encombrante voire inutilisable dans un document à mise en page rigoureuse et dont la surface disponible est rare : un courrier marketing, une facture, un contrat, une étiquette, un journal, etc.

Les codes 2D permettent de contenir un nombre d'informations limité qui varie selon les codes :

		Datamatrix	QR Code	PDF 417
Type		Matriciel	Matriciel	Code 1D empilé
Capacité	Numérique	3.116	7.089	2.710
Capacité	Alphanumérique	2.355	4.296	1.850
Capacité	Binaire	1.556	2.953	1.018

Ces codes intègrent des niveaux de sécurité variables grâce à l'introduction d'une redondance de l'information en plusieurs endroits du code afin d'en assurer l'intégrité en cas de destruction partielle. Le taux de redondance d'un code 2D est généralement paramétrable. Si la dégradation du code est supérieure à ce taux de robustesse, aucune donnée n'est lue.

Ces codes de type matriciel nécessitent une technologie de capture numérique de l'image et non plus un simple faisceau de lecture.

Ces codes 2D globaux ne proposent aucun outil simple de description des données à coder, i.e. de classification des données par type (sémantique) et d'organisation (syntaxe). Ils ne restituent qu'une information faiblement structurée restreignant son exploitation par le récepteur. Ils sont limités par leur structure à des applications très simples où la structure des données est connue au caractère près : incrémentation de nombres, association d'un nombre à une adresse web, codage de chaînes de caractères à faible valeur sémantique, etc.

2.2.2. *L'écriture numérique*

C'est pour pallier les limites des codes 2D détaillées ci-dessus qu'a été créé le système d'écriture numérique Alphacode.

Exemple d'une police : 

L'écriture numérique est un hybride extrêmement innovant entre :
• les polices de caractères ;
• les codes 2D ;
• et les langages informatiques.

Elle a été spécialement créée pour la lecture par des capteurs numériques (scanners, caméras, webcams, etc...)

Cette écriture numérique (symbologie) combine et hérite des avantages de ces trois composantes :

• la matérialisation sous forme de **polices de caractères** permet une insertion aisée dans tous les documents même très denses car cette écriture numérique se présente sous forme d'une ligne de texte, compatible avec les systèmes de production et d'impression de documents,

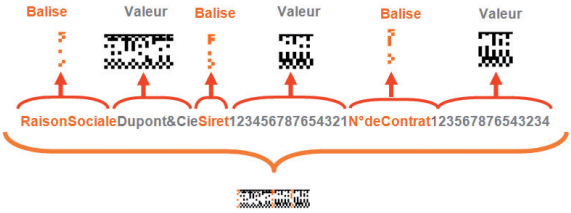
• la structure physique de ces polices de caractères, leur permet de bénéficier de la même robustesse de lecture que celle des **codes 2D**, et leur représentation informatique sous forme de chaîne de 0 et de 1, leur permet de porter des algorithmes de hash, de cryptage et de correction d'erreur,

• l'usage de polices de balises sémantiques de type XML autorise la création de véritables **métalangages**, permettant de réduire fortement le nombre de caractères utilisé pour coder les informations.

Exemple d'utilisation de balises :

Le recours à l'écriture numérique sur un document papier permet de transformer le document en un objet communiquant numérique, sécurisé et interactif à un coût négligeable.

L'écriture numérique garantit la lecture, l'intégrité, l'identification et l'authentification des données critiques des documents dans des conditions de sécurité extrêmement élevées.



****

3 EXEMPLES D'USAGES

3.1 Lettre recommandée électronique

Certaines formalités doivent nécessairement être réalisées par lettre recommandée (lorsqu'un texte prévoit de recourir à La Lettre recommandée électronique). D'autres fois, la lettre recommandée est requise à titre de précaution (afin de se préconstituer une preuve fiable d'un envoi et d'une réception) et ce sans qu'un texte prévoie ce recours. A l'heure de la dématérialisation des échanges, les textes ont prévu l'adaptation de la lettre recommandée électronique à travers deux types de services distincts : la lettre recommandée toute électronique et la lettre recommandée « hybride », chacun de ces procédés apportant de réels avantages.

Le terme de « lettre recommandée hybride » fait référence à une solution d'envoi par voie électronique du contenu de la lettre, qui sera édité sur papier et acheminé classiquement par voie postale.
Le terme « lettre recommandée électronique » fait quant à lui référence à une solution d'envoi d'un courrier électronique.

Dans les deux cas, ces solutions ont une valeur juridique équivalente à la lettre recommandée postale dès lors que les conditions prévues dans l'Ordonnance n° 2005-674 du 16 juin 2005 et le Décret n° 2011-144 du 2 février 2011 sont respectées et permettent de disposer d'une preuve fiable de la date d'un envoi et, lorsqu'un accusé de réception est demandé, de la date de sa réception de même que de l'identité de la personne en accusant réception.
Notons que l'Ordonnance n° 2005-674 du 16 juin 2005 est le premier texte apportant la notion d'hybridation dans le droit français, c'est-à-dire reconnaissant le changement de support d'un document tout en conservant une valeur juridique identique à celui-ci. Il faudra attendre l'Instruction fiscale du 11 janvier 2007 pour retrouver, mais de façon beaucoup plus limitée, un principe équivalent pour certaines factures (cf. 3.2.2 ci-après).

3.1.1 La valeur légale des lettres recommandées électroniques et hybrides

Les envois électroniques recommandés sont régis par l'article 1369-8 du Code civil inséré par l'ordonnance n° 2005-674 du 16 juin 2005 sur le procédé d'envoi d'un email recommandé ainsi que par le décret n° 2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat.

L'ordonnance n°2005-674 du 16 juin 2005 vient conférer une valeur juridique à l'email recommandé. Le procédé utilisé pour l'envoi d'un courrier électronique recommandé répond à quatre exigences énumérées à l'alinéa 1 de l'article 1369-8 du Code civil :

- le procédé doit identifier le tiers « désigné » qui achemine le courrier électronique recommandé
- le procédé doit désigner l'expéditeur du courrier électronique recommandé ;
- le procédé doit garantir l'identité du destinataire du courrier électronique recommandé ;
- le procédé doit établir si la lettre a été remise ou non au destinataire dudit courrier.

L'alinéa 3 de ce même article apporte quant à lui des précisions relatives à la date du courrier, laquelle est un élément fondamental en matière de recommandé. Ce texte reproduit dans l'électronique le fameux « cachet de La Poste faisant foi ». Il est inscrit que « Lorsque

l'apposition de la date d'expédition ou de réception résulte d'un procédé électronique, la fiabilité de celui-ci est présumée, jusqu'à preuve contraire, s'il satisfait aux exigences fixées par un décret en Conseil d'Etat. ». Les exigences de fiabilité de la datation électronique de la lettre électronique ont ainsi été fixées par le décret n°2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat. Un arrêté du 20 avril 2011 est relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique (PSHE) et à l'accréditation des organismes qui procèdent à leur évaluation. Ces deux textes sont venus préciser les conditions de fiabilité des contremarques de temps (lorsque le PSHE souhaite distribuer des contremarques de temps fiables) et les conditions de qualification du PSHE pour les délivrer.

L'alinéa 2 de l'article 1369-8 du Code civil reconnaît juridiquement l'existence de la lettre recommandée tout électronique avec ou sans avis de réception, mais aussi les lettres recommandées « hybrides », envoyées par voie électronique, éditées sur papier et acheminées par voie postale. Les deux modalités de réception de la lettre recommandée électronique sont prévues. Si une lettre recommandée par voie électronique est envoyée, l'expéditeur peut choisir une réception sur support papier ou une réception sous forme électronique. Si le choix a été fait pour une réception sur support papier, le contenu de la lettre recommandée électronique est imprimé par le tiers pour être distribué au destinataire sous forme papier. Cette possibilité est importante car elle vise certaines pratiques dites « hybrides » dont la reconnaissance juridique pouvait, jusqu'alors, être source d'interrogation. En revanche, en cas d'option pour une réception sous forme électronique, la lettre recommandée est alors adressée au destinataire par voie électronique, étant noté que « si le destinataire n'est pas un professionnel, il doit avoir demandé l'envoi par ce moyen recommandé ou en avoir accepté l'usage au cours d'échanges antérieurs ».

Pour préciser et compléter ces textes, le décret n°2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat a été publié. Ce décret décrit le processus d'envoi et d'acheminement d'une lettre recommandée électronique. Il précise ainsi les informations que le tiers chargé de l'acheminement doit communiquer avant tout envoi d'une lettre recommandée électronique, ainsi que celles que l'expéditeur doit fournir lors du dépôt de la lettre (et notamment le statut professionnel ou non du destinataire et, dans ce dernier cas, son accord préalable à la réception d'une lettre recommandée électronique), les éléments constitutifs de la preuve de dépôt et sa conservation par le tiers chargé de l'acheminement ainsi que les règles relatives à la transmission de la lettre recommandée au destinataire et à l'avis de réception. Enfin, le décret précise les modalités de distribution et de remises des lettres recommandées hybrides par des prestataires de services postaux.

Et si la lettre recommandée présente un contenu vide ?

La question est souvent posée au juriste de la complétude de la preuve apportée par la lettre recommandée, en particulier en prenant le cas d'une lettre recommandée qui arriverait vide à son destinataire
Or, la jurisprudence a déjà eu l'occasion de se pencher à plusieurs reprises sur cette hypothèse. Ainsi, selon une jurisprudence déjà ancienne et en application des articles 667 et 670 du Code de procédure civile, en cas de notification sous enveloppe, « il appartient au destinataire de prouver que celle-ci était vide et non pas à l'expéditeur d'établir que l'acte notifié était contenu dans cette enveloppe » (Cass. Com, 16 avril 1951 : Bull ; civ. IV, n°854, Cass. Com, 15 juillet 1993, n°92-04.092 et plus récemment CA Montpellier, 16 novembre 2010, n° 10/03005).

Il appartient donc au destinataire recevant une lettre recommandée sans contenu de s'en inquiéter et de prendre contact, idéalement avec une nouvelle lettre recommandée, avec l'expéditeur, prouvant ainsi sa bonne foi.

Et si le contenu de la lettre recommandée venait à être discuté ?

Que ce soit en droit civil ou en droit administratif, il existe une présomption, émanant des tribunaux, selon laquelle la lettre recommandée contient effectivement le document allégué par l'expéditeur. Cette présomption peut toutefois être renversée en cas de preuve contraire (ex : affranchissement de l'enveloppe incompatible avec le poids des documents allégués - CE, 30 décembre 2002, n°229957).

Ainsi, en matière de bail, le document envoyé par l'expéditeur est considéré comme celui qu'il a indiqué, faute de l'apport de la preuve contraire par le destinataire (Cass. Civ 3e, 2 mai 1978, n°76-15479), tout comme en matière fiscale («les requérants n'apportent pas la preuve, qui leur incombe, que le pli du 27 septembre aurait contenu, comme ils le soutiennent, un autre document (…) - CE, 30 décembre 2002, n°229957»).

3.1.2 Processus / usages

Dans la plupart des cas, et notamment entre professionnels, l'envoi d'une lettre recommandée se justifie pour des raisons qui ne sont pas imposées par le cadre légal. En effet, de nombreux échanges se font avec la volonté de diffuser des documents confidentiels et de garder la preuve d'envoi.
Les principaux cas d'usages :

- Un courrier relatif à la conclusion ou à l'exécution d'un contrat (résiliation, etc.) ;
- Les mises en demeure contractuelles ;
- Les notifications contractuelles ;
- Les convocations aux Assemblées Générales et aux instances dirigeantes (dès le moment où la voie électronique est reconnue dans les statuts d'une société ou dans un règlement de copropriété) ;
- Lettres de relance ;
- Lettres de rappel ;
- Lettres de contentieux ;
- Lettres de contestation ;
- Courriers sensibles ;
- Envoi de documents créatifs dont la paternité doit être prouvée.

En plus de sa valeur probante, la lettre recommandée électronique ou hybride offre de multiples avantages qui sont :
- de sécuriser les échanges de documents confidentiels ;
- de garantir une traçabilité des envois ;
- de bénéficier d'un délai d'acheminement immédiat ;
- de générer des économies sur les coûts d'impression et d'affranchissement ;
- de s'inscrire dans une politique de développement durable ;
- d'améliorer la gestion et le traitement des recommandés papier et de leurs accusés de réception.

Néanmoins les textes juridiques présentés dans la section ci-dessus encadrent l'usage de la lettre recommandée électronique ou hybride.

Conditions d'utilisation de la lettre recommandée toute électronique

Le décret sur la lettre recommandée électronique est paru le 2 février 2011 et précise les modalités d'application de l'article 1369-8 du code civil qui autorise l'envoi d'une lettre recommandée relative à la conclusion ou à l'exécution d'un contrat par courrier électronique.
Il est bon de noter que ce décret restreint l'utilisation de la lettre recommandée toute électronique aux documents relatifs à la conclusion ou à l'exécution d'un contrat ; on peut donc en déduire qu'un contrat ou une lettre de relance peut être envoyée dans ce format. Néanmoins les convocations d'assemblées générales de copropriété par exemple sont exclues de ce champ d'application. Les convocations des AG de copropriété relèvent de textes spécifiques. Elles peuvent être remises en main propre ou envoyées par voie postale (pas de format électronique possible).
Une réflexion est en cours pour introduire un dispositif de convocation électronique. A ce titre une question a été posée par le Sénateur Jean-Louis Masson le 16 juin 2011 pour modifier le décret du 17 mars 1967 et autoriser l'envoi par courrier électronique des convocations aux Assemblées Générales de copropriété. A ce jour, la question n'a pas encore obtenu de réponse. A terme, ce procédé devrait sans doute être autorisé.

Concrètement, comment fonctionne l'envoi d'une lettre recommandée électronique ?

Les services d'envoi de lettre recommandée électronique ou hybride se fondent au départ sur l'envoi d'un document électronique qui est, selon les cas, envoyé au format électronique ou imprimé, mis sous pli, affranchi et remis en poste.

Dans le cas où un émetteur veut envoyer une lettre recommandée toute électronique, il va transmettre sa lettre électronique à un opérateur en précisant :

- La qualité du destinataire particulier ou professionnel ;
- L'accord du destinataire s'il s'agit d'un particulier ;
- L'adresse email de destination.

L'opérateur va remettre à l'émetteur une preuve électronique de dépôt.

Le destinataire va recevoir un email l'informant qu'une lettre recommandée électronique lui a été envoyée. L'émetteur de la lettre recommandée reste anonyme. Le destinataire peut alors choisir de l'accepter ou de la refuser dans un délai de 15 jours.

Si le destinataire l'accepte, il va alors recevoir un email lui permettant d'accéder à sa lettre recommandée électronique. La consultation de la lettre recommandée électronique génère l'envoi d'un accusé de réception à l'émetteur.

Si le destinataire refuse ou ne consulte pas l'email au-delà du délai de 15 jours, l'émetteur aura la possibilité de renvoyer sa lettre recommandée par voie postale en utilisant la méthode d'envoi traditionnelle ou la méthode d'envoi hybride.
Contrairement à la lettre recommandée toute électronique, l'envoi de la lettre recommandée hybride n'est pas soumis à de telles conditions. Garantir le contenu du pli et sa preuve de dépôt, optimiser le contrôle de son format, de l'envoi, du suivi et de l'archivage sont autant d'atouts associés à la Lettre Recommandée hybride en conservant la valeur juridique d'une lettre recommandée papier traditionnelle.

Aujourd'hui, l'industrialisation du traitement des lettres recommandées permet aux entreprises et administrations de bénéficier de toutes les avancées technologiques pour bénéficier de gains de productivité et de réductions de coûts tout en respectant la valeur légale de l'envoi : date de dépôt, date de distribution et identité du destinataire. L'Avis de Réception (AR) peut être dématérialisé et archivé tout comme la preuve électronique de dépôt et le contenu du pli.

3.1.3 Les technologies au service de la lettre recommandée hybride ou toute électronique

Une signature électronique peut être appliquée sur les versions électroniques :

- du document envoyé par lettre recommandée électronique ou hybride ;
- de la preuve de dépôt ;
- de l'accusé de réception ;

Afin d'apporter plus de garanties sur le contenu de la lettre et éviter que le contenu soit discuté, la version électronique de la lettre recommandée, qu'elle soit tout électronique ou hybride, pourrait être publiée sur un portail. Ainsi le destinataire ou l'émetteur pourrait vérifier la version électronique du document.

L'archivage électronique permet également de conserver le document, les preuves d'envoi et de réception en ligne et pendant les 3 ans d'obligation de conservation.

Pour les recommandés hybrides, il est important de s'assurer de l'intégrité et de l'intégralité du pli. Les technologies de codes barre unidimensionnel (1D) permettent de donner les garanties du nombre de plis à remettre et du bon contenu des plis.

Les technologies de codes 2D telles que présentées au chapitre 3.2 permettent de sécuriser les données pertinentes (les données importantes relatives à l'usage), et permettent de garantir que ces données n'ont pas été altérées. L'ajout d'un code 2D pourrait garantir la conformité entre la version électronique et la version papier de la lettre recommandée.
Le calcul du code 2D et son intégration dans le document doit être de préférence réalisé par un tiers de confiance de façon à ce que, dans le cas où il y aurait une différence entre le contenu envoyé et le contenu reçu, la vérification puisse être effectuée de façon impartiale.
Il faut, dans ce cas, que l'émetteur de la lettre recommandée puisse indiquer les champs pertinents au tiers de confiance.

Une généralisation du procédé pourrait être imaginée en sécurisant l'intégralité du texte envoyé. Ainsi, toute modification pourrait être identifiée, sans qu'il soit nécessaire de spécifier les champs pertinents. Dans ce cas, il faudrait faire appel à une écriture numérique, permettant une densité d'information numérique plus grande.

3.2 La Facture

3.2.1 Définition

Une facture est un document comptable par lequel un fournisseur établit une créance, résultant de la fourniture d'un bien ou de la prestation d'un service, vis-à-vis de son client, bénéficiaire de ce bien ou de cette prestation.
En France, le Code de commerce impose la facturation pour les achats de produits ou prestations de service pour une activité professionnelle. Le vendeur doit la délivrer dès la réalisation de la vente ou la prestation, l'acheteur doit la réclamer. Elle est établie en un exemplaire pour chacun, à conserver dix ans en application des exigences comptables issues du Code de commerce (art. L. 123-22 du Code de commerce).

Elle est de forme libre, mais mentionne :
• le nom des parties,
• leur adresse,
• la date de la vente ou de la prestation de service,
• la quantité,
• la dénomination précise,
• le prix unitaire hors TVA des produits vendus et des services rendus,
• la date de règlement,
• les conditions d'escompte en cas de paiement anticipé,
• le taux des pénalités exigibles en cas de dépassement.

Le règlement est réalisé dès que les fonds sont mis à la disposition du bénéficiaire par le client.

De plus, le Code général des impôts ajoute la nécessité de mentionner :
• le numéro d'identification à la TVA du vendeur,
• un numéro de facture,
• si l'entreprise est assujettie à la TVA :
  - le taux de TVA applicable à chacun des biens livrés ou services rendus,
  - le montant de la taxe à payer et, par taux d'imposition, le total H.T. et la taxe correspondante.

Pour optimiser le coût de production des factures émises et celui de traitement des factures reçues, pour répondre aux réglementations en vigueur concernant les conditions de conservation de ces factures, certains professionnels ont opté pour l'archivage électronique ou la dématérialisation (***voir le guide de la facture électronique de la FNTC***)

Ainsi une facture peut aujourd'hui être sous forme papier et/ou électronique sous réserve de respecter certaines exigences posées par les textes.

Il convient de ne pas confondre ces factures destinées à un usage BtoB avec ce que le grand public reçoit de la part des fournisseurs d'eau, d'énergie, de communications électroniques ou encore des commerçants en ligne, en justification des coûts payés par le consommateur.

Appelés improprement « factures », ces documents, propres au BtoC et émis à titre d'information du consommateur, ne sont pas tenus au cadre réglementaire strict de la facture véritable.

3.2.2 Précisions juridiques

En effet, il est important de noter que la facture dont il est ici question est la facture au sens fiscal du terme, c'est-à-dire qui :
• contient des informations relatives au régime de TVA applicable ;
• sur laquelle s'exerce le contrôle de l'administration fiscale ;
• et permettant surtout de justifier, le cas échéant, du droit à déduction de la TVA.

Cette nature de pièce justificative de TVA et les contrôles stricts de l'Administration fiscale qui peuvent avoir lieu, expliquent que ce document fasse l'objet d'une réglementation fiscale très particulière concernant aussi bien son contenu (ses mentions) que sa forme.

Il est toujours possible de se reposer sur une facturation sous forme papier doublée ou accompagnée d'une information transmise sous forme électronique, parfois sur la facture papier en elle-même sous la forme d'un code 2D par exemple. Reste que fiscalement, ce sont les informations figurant sous forme papier qui devront faire foi en cas de contrôle par l'administration fiscale.

Et il convient de rappeler que tout manquement à la réglementation est sévèrement sanctionné par des peines d'amendes importantes [3].

Pour l'heure, en France, la loi permet l'utilisation de factures :

• dites « dématérialisées » c'est-à-dire utilisant l'EDI pour leur transmission. Ainsi, selon l'article 289 bis du Code général des impôts, *« Pour l'application des articles 286 et 289, seules les factures transmises par voie électronique qui se présentent sous la forme d'un message structuré selon une norme convenue entre les parties, permettant une lecture par ordinateur et pouvant être traité automatiquement et de manière univoque, constituent, sous réserve des dispositions ci-après, des documents tenant lieu de factures d'origine »*.

• ou *« transmises par voie électronique » « dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique. Les factures ainsi transmises tiennent lieu de facture d'origine pour l'application de l'article 286 et du présent article. Les conditions d'émission de ces factures, de leur signature électronique et leurs modalités de stockage sont fixées par décret »* (article 289 V. du Code général des impôts. Voir également le décret n°2003-659 du 18 juillet 2003[4] pris pour l'application de l'article 17 de la loi de finances rectificative pour 2002 du 30 décembre 2002, l'arrêté du 18 juillet 2003[5] qui a fixé les conditions d'émission et de conservation des factures dématérialisées en application de l'article 289 bis du CGI et modifiant l'annexe IV de ce code, ou encore l'Instruction fiscale du 7 août 2003 [6]).

Un tempérament a toutefois été apporté par l'administration fiscale à cette réglementation

3 Voir notamment l'article L. 441-4 du Code de commerce : « Toute infraction aux dispositions de l'article L. 441-3 est punie d'une amende de 75000 euros. L'amende peut être portée à 50 % de la somme facturée ou de celle qui aurait dû être facturée » mais également les articles 1737, 1741 et 1751 du Code général des impôts.
4 J.O. du 20 juillet 2003, p. 12272.
5 J.O. du 20 juillet 2003, p. 12273.
6 B.O.I. n° 136 du 7 août 2003.

pour encadrer les hypothèses où les entreprises produisent des factures électroniques, mais les transmettent sur support papier : le document valant facture au sens fiscal du terme est alors papier, mais il aurait été peu efficace d'obliger, dans ce cas, les entreprises émettrices à imprimer et à conserver leur exemplaire sous forme papier.

L'objectif ici recherché est de faciliter la vie à deux types d'entreprises :

- Celles qui émettent des factures électroniques, mais dont les clients ne peuvent ou ne souhaitent pas recevoir leurs factures par la voie électronique ;
- Celles qui produisent leurs factures de façon électronique et l'envoient sous forme papier, oubliant de plus en plus au passage d'en conserver pour elles-mêmes un original papier.

C'est la raison pour laquelle, dans le cas des seules factures de vente et en application de l'Instruction fiscale du 11 janvier 2007[7], ces entreprises pourront procéder à un archivage électronique (dans les formes requises) de leur propre exemplaire original, envoyant ensuite un original papier à leur client. **L'administration fiscale interprète de façon extensive la notion de « double original », en abandonnant le critère de stricte identité des deux documents.**

Pour la conservation du double original de leurs factures de vente créées sous forme informatique et transmises sur support papier, les entreprises ont deux possibilités :

- soit elles conservent un double papier de la facture transmise, ce qui suppose l'impression de deux documents : l'original de la facture destiné au client et son double papier qui doit être archivé par le fournisseur ;
- soit elles conservent un « *double électronique* » de cette facture.

Pour ce faire, l'instruction précise que *« la valeur probante du « double électronique » conservé par le fournisseur dépend essentiellement de l'utilisation d'un dispositif technique assurant au système d'information utilisé une fiabilité équivalente à celle que procure l'impression des factures sur papier et permettant de considérer que le « double électronique » constitue, au sens du n° 3, la reproduction fidèle et durable de l'original de la facture adressée au client sur support papier ».*

Nous renvoyons pour un aperçu de l'ensemble du (riche) cadre juridique applicable aux factures « transmises par voie électronique », ainsi que de sa récente évolution au niveau de l'Union européenne, au guide de la facture électronique de la FNTC : ***« Guide de la signature électronique » de la FNTC (2008).***

A l'opposé de ces factures électroniques au cadre juridique strict, existent d'autres types de documents appelés également « factures » par le grand public, mais qui n'en ont ni l'objet (déduction de la TVA), ni le cadre réglementaire : il s'agit des documents émis par les fournisseurs d'eau, d'énergie, de communications électroniques ou encore les commerçants en ligne et qui ne sont juridiquement que des notes récapitulatives du montant payé pour les achats opérés par un particulier.

7 *B.O.I. n°4 du 11 janvier 2007.*

Si la délivrance de ces notes récapitulatives[8] est obligatoire pour toute prestation de service **lorsque son prix est supérieur ou égal à 15,24 €, TVA comprise, aucune forme particulière n'est exigée et a fortiori aucun formalisme du document remis au client n'est requis quant à la protection en intégrité ou non de cette note.**

En effet, la facture au sens fiscal du terme concerne directement un tiers (l'Etat) à la relation commerciale, qui doit pouvoir contrôler la régularité de l'opération donc l'émetteur et le récepteur.

Dans le cas de la note récapitulative, celle-ci n'est pas destinée à être opposée à un tiers, mais uniquement, en cas de contentieux, au commerçant par le consommateur. Or celui-ci, face au commerçant, peut prouver ses prétentions – et notamment la réalité des prestations fournies ou du contrat conclu – par tout moyen. Compte tenu de cet avantage, il est inutile de prévoir que le document soit protégé en intégrité, sauf à ce que le commerçant le fasse de sa propre initiative… pour se prévaloir plus facilement de son contenu.

Reste que dans la vie courante, et malgré le droit prônant l'effet relatif des contrats (un tiers à la relation contractuelle ne peut en principe opposer les stipulations d'un contrat à l'un des contractants), ces « factures » (qui n'ont pas d'exigence de format particulier) ont été utilisées pour des raisons pratiques par des tiers comme moyen de preuve du domicile du client, par exemple.

La question se pose alors de la fraude liée à ces documents. Juridiquement, celle-ci est réprimée (faux et usage de faux[9], escroquerie, etc.), mais techniquement et du fait des progrès du numérique, elle pourrait sans doute être évitée ou en tout cas grandement limitée par l'utilisation de moyens techniques que le droit, pour l'heure, ne rend pas obligatoire dans le rapport contractuel considéré.

Ainsi, pour répondre à ce problème « d'antifraude » mais également pour optimiser le coût de traitement de factures reçues sous forme papier, nous vous présentons ci-dessous des solutions pragmatiques qui consistent à reprendre les informations clés d'une facture, lors de sa conception, et de les intégrer dans un code optique préalablement chiffré.

Ainsi toute modification frauduleuse sur une de ces informations clés de la facture engendrera une incohérence avec le contenu du code optique. Ceci aura pour effet de garantir l'intégrité du document physique.

---

8 La note récapitulative doit comprendre la date de rédaction de la note, le nom et l'adresse de l'entreprise, le nom du client, la date et le lieu de la prestation, le décompte détaillé en quantité et prix, de chaque prestation et produit fourni ou vendu, la somme totale à payer hors taxe, (article 3 de l'arrêté n°83/50 du 3 octobre 1983).

9 Article 441-1 du Code pénal : « Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende ».

3.2.3 Processus / usages

Les cas d'usages ci-dessous sont prospectifs dans le cadre de l'utilisation de factures hybrides. L'environnement légal et législatif n'oblige pas, à ce jour de mettre en place de tels processus.
Il s'agit d'exprimer comment la facture hybride, si elle était mise en place pour les factures « BtoB » et aussi pour les particuliers, permettrait de gagner en productivité, mais aussi en confiance vis-à-vis de l'intégrité des documents.

Cas d'usage d'une facture fournisseur en BtoB :

Les professionnels connaissent bien la difficulté à traiter les factures reçues de ses fournisseurs :
• Extraction des données nécessaires aux contrôles et à la comptabilisation ;
• Rapprochement avec le ou les bons de commandes et de livraisons ;
• Circuit de validation ;
• Etc.

Eu égard aux considérations juridiques indiquées concernant l'exigence de factures papiers ou de factures électroniques, la présence de la technologie d'hybridation permettra, outre de vérifier la cohérence et l'intégrité des factures, d'optimiser considérablement les traitements d'extraction de leurs données.

La lecture du tag, par un simple procédé de lecture automatique de document (LAD), permettra de récupérer de manière fiable une partie significative des informations contenues dans la facture telles que :
• le nom du fournisseur ;
• le N° et la date de la facture ;
• les montants HT et TTC ;
• le N° de commande et de BL.

Les cas d'usages ci-dessous illustrent l'intérêt des technologies d'hybridation dans des actes courants de la vie des particuliers et citoyens que nous sommes tous, ainsi que l'intérêt pour des entreprises utilisant dans leur processus des données d'entrées documentaires et maintenant souvent numériques au départ.

Cas d'usage sur le justificatif de domicile :

Lors de l'ouverture d'un compte bancaire, il est demandé de produire un justificatif de domicile. Ce justificatif est souvent une « facture » de type fournisseurs d'eau, d'énergie (gaz, électricité) ou de communications électroniques (téléphone/Internet). Dans le cas d'un justificatif de domicile avec un tag apportant une preuve de contenu, le processus suivi en agence pourrait être du type suivant :

- Fourniture à l'agence bancaire d'un justificatif imprimé papier et contenant un tag de sécurité
- Traitement par l'organisme bancaire ou financier du document :
  - Vérification des données imprimées sur le papier (ou le scan dans le cas où le justificatif est scanné pour le traitement) ;
  - Vérification de la cohérence des données avec celles du tag ;
  - Vérification de la signature du tag pour s'assurer de la véracité des données (intégrité des données signées avec une clé reconnue et valable).

Dans ce cas de figure, le justificatif, qu'il soit sous une forme imprimée ou numérique (scan), peut garantir l'intégrité des données imprimées par rapport à celles présentes dans le tag. Il devient donc plus difficile de frauder en fournissant une mauvaise adresse.

Cette illustration concerne aussi l'ouverture d'un abonnement à un opérateur mobile par exemple où l'utilisation du justificatif peut être imaginée selon un processus similaire. La lecture du tag sécurisé peut aussi être réalisée directement sur site via une douchette qui scanne le tag pour le lire en direct et procéder aux validations nécessaires avant de pouvoir afficher le résultat.

Exemple d'une facture avec écriture numérique (ligne codée en bas).

Cas d'usage pour le service après-vente d'un grand magasin

Les ventes sur internet, commandes d'appareils électroniques ou autres progressent constamment. Cependant, chaque télé achetée sur internet n'est pas plus, pas moins fiable qu'un appareil acheté dans un grand magasin. Certaines enseignes proposent même un mode mixte (acheter sur le site ou dans le magasin).

Par ailleurs, pour le particulier et pour l'enseigne, comment garantir une saine relation après vente ensuite ?

Lors d'une défaillance, l'appel à garantie pour le particulier peut se traduire par la visite du service après-vente de l'enseigne avec l'objet défaillant, et en présentant un bon de garantie, mais souvent une « facture » servant également de garantie, récupérée par exemple sur le site internet du cybercommerçant.

Malgré la bonne foi du client, comment est-ce que l'établissement peut s'assurer de la véracité de la facture ? Que ce n'est pas un faux, une copie détournée pour fausser la date de fin de garantie ou pour réparer un objet illicitement acquis ?

Si la « facture » avait été émise avec un « tag » ou bien une écriture numérique sécurisée, le technicien au guichet pourrait rapidement lire le document et y vérifier dans le « Tag » la cohérence d'informations comme :

- La date d'émission réelle de la facture ;
- Le code article de l'objet ;
- Le montant ;
- Le nom et prénom de l'acheteur (bien souvent imprimé sur une facture via Internet).

La lecture de ces informations pourrait se faire via une douchette ou un scanner à son poste de réception.

Le chiffrement de ces informations peut se faire via une clé et un certificat interne, directement géré par l'enseigne (dans ce cas, seule l'enseigne aurait la possibilité de lire et exploiter le document et son « intelligence ») ou via l'appel à une autorité de certification pour s'assurer de la validité du certificat.

Dans notre exemple, que la « facture » soit numérique ou bien imprimée, copiée via une imprimante couleur multifonction, les informations importantes, nécessaires pour assurer un service : « faire jouer la garantie », sont donc bien intègres et quasi infalsifiables par le plus grand nombre. Ce qui n'est pas le cas aujourd'hui avec des moyens simples (copie, retouche graphique, etc.)

Dans notre exemple, tout cela se fait en toute transparence pour le particulier. L'enseigne a besoin de s'équiper de deux éléments :

- Une brique logicielle pour pouvoir apposer une écriture numérique lors de la génération de la « facture », que ce soit un PDF numérique ou une facture papier.
- Une brique logicielle pour lire rapidement au guichet les informations du tag et assurer la cohérence des informations, et donc la validité du document.

Cela passe aussi par une rapide formation sur site pour les techniciens et commerciaux. Ces coûts sont tout à fait raisonnables et intégrables par exemple dans le budget « portail e-commerce » de ces enseignes.

Cet exemple démontre comment une enseigne privée peut facilement lutter contre la fraude à son niveau, en choisissant une technologie d'écriture numérique suffisamment dense pour y mettre les informations nécessaires

Cas d'usages de ventes entre particuliers.

Le succès des sites d'échanges, de ventes ou d'enchères communautaires n'est plus à démontrer ces dernières années, multipliant ainsi les transactions entre particuliers sur des objets parfois de valeur (montres, hifi, …).

Prenons l'exemple d'une montre de valeur qu'un particulier souhaite acheter à un autre sur un site d'enchère :

- Quelle assurance a-t-il que le produit n'est pas une contrefaçon mais un modèle original ?
- Quelle assurance que le produit n'est pas volé mais a bien été acheté par le vendeur avec qui il communique ?

L'application d'une écriture numérique sur les factures de produits de luxe ou d'un certain prix peut permettre d'imaginer le scénario suivant :

L'acheteur ou les acheteurs se font envoyer par le vendeur (par e-mail ou via une fonctionnalité future des sites d'enchères) une copie de la « facture » d'achat. Ce document comporte les données suivantes :

- Montant de l'achat.
- Date d'achat.
- Magasin vendeur.
- Marque et modèle du produit.
- Si la facture est éditée en magasin ou en ligne, il faudrait aussi intégrer le nom et le nom de l'acheteur et/ou le No de série de l'article.

Lorsque la « facture » est reçue, chaque acheteur intéressé peut, via un service payant ou à la demande, faire vérifier les points de cohérence du document avec les données sécurisées dans l'écriture numérique.

Ce scénario pourrait déjà se dérouler à partir de produits achetés en France, au-dessus d'une certaine valeur d'achat, puis se répandrait petit à petit sous forme de bonnes pratiques, avant d'envisager éventuellement une directive européenne à terme.

3.2.4 Recommandations

L'enrichissement d'une facture numérique (souvent sous le format PDF) avec une écriture numérique permet donc d'améliorer deux aspects distincts :

1- L'amélioration des traitements ou « Business Process » afin de récupérer plus facilement quelques meta-données importantes du document pour injection dans un système d'information (ERP, système commercial, etc…). Cet aspect est complémentaire, dans le cas par exemple de copie de mauvaise qualité, avec les technologies LAD/RAD existantes (Reconnaissance Automatique de Documents / Lecture Automatique de Documents.)

2- La sécurisation des informations des documents pouvant servir à des démarches officiels vis-à-vis de l'état, des banques, dans un contexte de lutte contre la fraude, via le chiffrement de données avec une écriture numérique (ou DataMatrix) apposée sur le document lors de son impression ou émission numérique.

Afin de promouvoir ces technologies, il est prudent de procéder par étape, avec une juste mesure entre l'aspect sécuritaire, le déploiement, et la confiance que les utilisateurs pourront percevoir.

Dans de nombreux cas BtoB, il existe de nombreux moyens de lutte contre la fraude des fausses factures sur l'ensemble de l'activité d'une société et sa relation avec ses clients ou fournisseurs : contrôle fiscal, contrôle de Tva, commissariat aux comptes… Dans ce contexte, l'intérêt de l'hybridation d'un document est surtout de l'ordre de la productivité pour des gains rapides, puis, petit à petit, de pouvoir également sécuriser l'écriture.

La question du chiffrement des données dès le départ au sein de l'écriture numérique se pose, pour des questions de coûts (coût du certificat, coût de l'exploitation) et de finalité.

Dans le monde du particulier ou pour des documents servant aux démarches officielles (justificatif de domicile), **la véritable valeur de confiance du document hybride passe par le chiffrement des données** pour éviter des manipulations frauduleuses sur le document (modification des données visibles et des données de cohérences injectées dans l'écriture numérique).

Par contre, il est important de donner accès facilement au déchiffrage, et à la vérification du document. Cela semble devoir passer par le développement de « portails » de vérification, organisés par des acteurs privés, en plus de celui ou ceux de l'état, mais scrupuleusement référencés et reconnus par l'Etat et respectant une norme ou un label nécessaire.

Par ailleurs, les acteurs de coffres-forts numériques peuvent aussi jouer un rôle en proposant directement la vérification d'intégrité des documents archivés qui possèdent une écriture numérique.

Ainsi, un document papier issu d'un original numérique pourrait être identifié directement en lançant une requête chez l'opérateur de coffre-fort numérique qui le gère.

Les opérateurs de coffres peuvent aussi proposer un service de marquage avec écriture numérique des documents imprimés issus de leur archivage, afin d'en garantir, non pas la provenance totale (l'émetteur réel du document) mais une garantie d'intégrité depuis son archivage.

Exemple : une facture d'achat d'un meuble est archivée dans un système d'archivage électronique (SAE) depuis 8 mois. Elle pourrait être imprimée avec deux services proposés par le SAE :

• L'écriture numérique apposée lors de l'impression garantit bien que ce document est identique à celui d'il y a 8 mois, archivé dans le SAE.
• Un service de vérification permet au lecteur du document imprimé de vérifier son intégrité depuis la mise au coffre.

> **Ce panel de services permet aussi de profiter de l'écriture numérique pour toutes les factures historiques anciennement émises.**

3.3 Le bulletin de paie

Honoraires, dividendes, émoluments, commissions, gratifications, primes, traitements, avantages, rémunération, salaire, paie, solde, règlement, rétribution, versement, indemnités, cachet, appointements, pige... font partie intégrante de l'histoire de l'humanité. On peut affirmer que les premiers bulletins servant de preuves de paiement d'un salaire quel qu'il soit remonte à la plus haute antiquité sur des tablettes d'argile retrouvées « grâce » à l'incendie d'un centre administratif sumérien ayant cuit, scellé et archivé ces documents jusqu'à nos jours.

En France, il a fallu attendre la loi du 4 mars 1931 pour rendre obligatoire la délivrance d'un document. Ce document avait pour objet d'éviter les contestations en matière de paiement de salaire. Ce document doit comporter tous les éléments constitutifs du salaire ainsi que les différentes cotisations sociales.

Ce document jalonne la carrière du travailleur salarié de ses débuts jusqu'à sa retraite, générant un lien affectif très fort : la première paie, la première cotisation retraite, etc. On en vient même à lui conférer des pouvoirs qu'il n'a pas… comme une sorte de «carte d'identité patrimoniale» opposable à tous.

Le bulletin de paie peut aujourd'hui être sous forme papier et/ou électronique.

3.3.1 Processus / usages

Le bulletin de paie atteste du versement d'une rémunération au salarié. Ce dernier l'utilise très largement comme un justificatif dans de nombreuses situations car de nombreuses personnes morales ou physiques le requièrent comme preuve, ou tout du moins comme une pièce pour évaluer le risque pris.

Au quotidien, il est notamment utilisé pour une obtention de crédit à la consommation ou un emprunt immobilier, pour la souscription d'un bail locatif, pour procéder à différentes formalités administratives (cf. guide FNTC « le bulletin de paie électronique »).

Dans un cadre plus proche de la relation employeur-employé, le bulletin de paie sert à la reconstitution de carrière (ex. : auprès de quel organisme le salarié doit aller chercher les écarts), il peut aussi servir de justificatif pour le salarié qui est amené à se retourner contre son employeur (dans le cas de cotisations non versées par exemple) ou encore il peut servir de justificatif pour aider à démontrer son activité (dans le cas de maladies professionnelles par exemple).
(cf. guide FNTC « le rôle du bulletin de paie dans la reconstitution de carrière »)

Toutes ces utilisations n'engagent que ceux qui les demandent et les acceptent. Cela fait du bulletin de paie une cible privilégiée pour les faussaires et les fraudeurs pour obtenir des droits auxquels ils ne pourraient avoir accès, même si ce type d'acte est pénalement sanctionné (faux et usage de faux, etc.)

Cas d'usage entre particuliers :

La location d'appartement est soumise au dépôt d'un dossier souvent assez volumineux comprenant :
• Déclaration d'impôt ;
• Feuille de paie ;
• RIB / IBAN ;
• Justificatif de domicile...

Nous nous attarderons volontairement sur le cas d'un propriétaire particulier qui loue son appartement en direct. Le cas d'une agence immobilière serait similaire.

Lorsqu'un propriétaire souhaite louer son appartement, comment peut-il s'assurer que les documents remis par un candidat ne sont pas falsifiés, en particulier le bulletin de paie ?

La technologie d'hybridation des documents permettrait au loueur de facilement vérifier la cohérence et l'intégrité des documents.

Les bulletins de paie et/ ou la déclaration d'impôt par exemple pourraient contenir une écriture numérique comprenant les informations suivantes :

• Nom employeur ;
• Date du bulletin de paie ;
• Nom et prénom salarié ;
• Montant net imposable...

Le particulier propriétaire, via un système de demande à l'acte, pourrait souscrire à un service sur le web pour 3 ou 5 documents. Il les numérise, les télécharge sur la plate-forme internet de services et l'écriture numérique sécurisée lui est alors déchiffrée. Il peut alors vérifier avec les données lisibles du bulletin la cohérence et l'intégrité et s'assurer de la solidité de son dossier.

3.3.2 Les différents supports du bulletin de paie et les problématiques associées

3.3.2.1 Le bulletin de paie sur support papier et la problématique de la fraude

Les moyens bureautiques modernes donnent accès à moindre coût au plus grand nombre à des moyens de falsification voire de création de toute pièce.
Ainsi, « l'amélioration manuelle » du bulletin de paie devient un jeu d'enfant pour les candidats à un logement, un prêt, un droit d'allocation etc. face à des organismes ou sociétés ne sachant pas lire et interpréter le contenu d'un bulletin de paie.

Il est possible de vérifier l'authenticité et la véracité du contenu du bulletin de paie, en opérant un certain nombre de contrôles, mais ce processus complexe et onéreux ne permet pas de garantir pour autant l'intégrité du document.

> Principales anomalies/fraudes sur les bulletins de paie :

• Fausse entreprise / incohérence code APE/convention collective ;
• Anomalie au niveau des taux : pas à jour, mauvais taux…
• Anomalie au niveau des données du salarié : incohérence ; fonction / niveau / coefficient / salaire ;
• Anomalie cumuls annuels par rapport à l'ancienneté ;
• Mentions interdites figurant sur le document (téléphone employeur, appartenance à un syndicat).

3.3.2.2. *Le bulletin de paie sur support électronique et la problématique de sa rematérialisation*

Le législateur a souhaité, par la loi du 12 mai 2009 (Loi n°2009-526), modifiant les articles L. 3243-2 et L. 3243-4 du Code du travail, rappeler expressément que le bulletin de paie peut être remis, avec l'accord du salarié, sous forme électronique. En opérant cette modification, et en prévoyant que cette « remise sous forme électronique » soit opérée dans des conditions de nature à en garantir l'intégrité, le législateur fait écho à des dispositions plus anciennes quoique différentes encadrant la facture « transmise par voie électronique » (cf. guide FNTC « le bulletin de paie électronique »).

Depuis cette loi permettant de remettre le bulletin de salaire sous forme électronique, la possibilité de modifier le document est devenue quasi nulle du fait de la sécurisation maximale obtenue dans un environnement de coffre-fort électronique ou équivalent … et uniquement dans cet environnement.

Le papier reste néanmoins le vecteur commun de transmission si bien que, même dématérialisé, le bulletin de paie arrive sous forme papier sur le comptoir de la banque ou de l'agence immobilière, qui peut ainsi être amené à douter de la réalité des informations figurant sur ce document.

Il est en effet toujours aisément falsifiable après sa rematérialisation. Il s'agit d'une vraie faille de confiance qu'il faut impérativement éliminer rapidement.

3.3.3. Recommandations

Une fois n'est pas coutume, le cahier des charges est des plus simples :

La mission :
- Donner un vrai statut de confiance au bulletin de paie en intégrant une garantie d'intégrité, quels que soient les changements de support que peut subir le document, assurant ainsi l'intégrité des informations fournies ;
- Assurer cette garantie via un tiers de confiance ;
- Donner la capacité d'extraire les données pertinentes de façon à les intégrer facilement dans le système informatique de la banque, l'agence immobilière ou l'organisme public ;
- Donner la possibilité d'une vérification/validation la plus simple et la moins onéreuse possible.

Comment ?

Première étape :
Rassurer les acteurs économiques qui requièrent les bulletins de paie de leurs clients en rajoutant des éléments de sécurité aux bulletins de paie dématérialisés.

Utilisation d'un code 2D ou d'une écriture numérique sécurisée (cf. 2.2)

Au-delà du nom, prénom et code postal il pourrait également être intéressant de protéger en intégrité également des données telles que :

- Nom de l'employé
- Statut : Cadre ou non Qualification Classification
- Nom de l'employeur/ Numéro de Siret
- Montant Brut/Net
- Code APE
- Période de paie
- Cumul annuel

Pour ce faire, on doit utiliser un volume plus important de données qui peuvent être limitées par la technologie de code employée. Dans ce cas, la structure morphologique et sémantique de l'écriture numérique révèle tous ses intérêts.

- L'augmentation du nombre de données sécurisées, contribue à la lutte contre la fraude tout en améliorant la productivité des traitements et des processus (ex : vérifications sécurisées et facilitation des captures automatiques des données contenues dans le document).
- Il est envisagé que ce mode hybride sécurisé s'adressera par exemple aux entreprises et à leurs employés qui auront choisi de dématérialiser leurs documents de RH.

Deuxième étape (prospective) :
Extension massive du processus pour tous les bulletins de paie et renforcement du niveau de sécurité.

- Il s'agit de sécuriser une part toujours croissante des bulletins de paie qu'ils soient sous forme papier ou électronique

- Une généralisation totale nécessiterait une intervention législative.

Le fait de garantir le document papier sans avoir à entrer dans un processus de dématérialisation peut représenter un premier pas vers la dématérialisation.

Ainsi, toute modification frauduleuse sur une de ces informations-clés engendrera une incohérence avec le contenu du code optique. Ceci aura pour effet de garantir l'intégrité du document physique.

Dans ce cas, la gageure pour le tiers de confiance qui va garantir le document sera de s'assurer de la véracité de l'émetteur de façon à ne pas certifier un vrai-faux bulletin de paie.

****

4 LES PERSPECTIVES

L'objectif de ce dernier chapitre est de se projeter dans 3 à 5 ans où, compte tenu des changements actuels dans l'univers de la dématérialisation et de l'usage numérique en général, nous nous permettons de donner des pistes, bien qu'elles ne soient pas toujours encore encadrées juridiquement. Ce ne sont que des projections légitimes pour développer l'usage du document hybride et augmenter une confiante et fréquente cohabitation entre le format numérique et papier.

• L'usage de la lettre recommandée électronique est aujourd'hui réservé aux seules situations contractuelles (cf 4.1). Il est évident qu'une démocratisation de l'usage du courrier recommandé à tout type de document apporterait un véritable bénéfice. Cela permettrait de faciliter de nombreuses démarches entre professionnels mais aussi entre particuliers.

Il est étonnant qu'un tel usage soit réservé aux relations contractuelles. Pourquoi un particulier ne peut-il pas s'en servir dans sa relation avec ses administrations, ou tout simplement lorsque deux particuliers souhaitent utiliser le courrier recommandé électronique dans un souci de formalisme ?
Par conséquent, et compte tenu de ce que nous avons essayé de démontrer tout au long de cette étude, il est évident que si un document, sous sa forme hybride (dans son format papier ou numérique), pouvait certifier de sa valeur probante, il n'y aurait aucun frein à l'utilisation du courrier recommandé électronique.

• A l'heure actuelle, le régime de la valeur du document papier et du document numérique sont soumis à des régimes juridiques la plupart du temps différents, empêchant souvent le passage facilité du papier à l'électronique et vice versa. Dans cette optique, et compte tenu de l'évolution de la société vers le tout numérique, on ne peut qu'espérer qu'à un horizon de 5 à 10 ans, ce soit le numérique qui acquiert une valeur supérieure au papier, tout comme la preuve orale avait été supplantée par la preuve écrite en son temps.

En attendant, grâce à l'apparition du document hybride, dont l'intégrité et la valeur pourraient être certifiées par des moyens techniques, on permet de combler un tant soit peu le vide qui persiste entre ces deux régimes. Il pourrait donc être envisagé de permettre soit un archivage numérique, soit un archivage papier du document hybride, puisque les solutions techniques présentées au 2.2 (code 2D, écriture numérique) permettent de conserver l'intégrité technique du contenu du document indépendamment de sa modification de support.

• Possibles évolutions de l'EDI : échange de données informatisées.
Les échanges entre donneurs d'ordres et sous-traitants de premier rang s'appuient sur une intégration forte avec une plate-forme d'échange EDI, pour accélérer l'acquisition d'information et lancer par exemple les ordres de fabrication, les expéditions, avec des cadences en phase avec les besoins du client (automobile, grande distribution). L'EDI a été créé il y a presque 30 ans pour accélérer les échanges et relations commerciales entre entreprises, d'une manière beaucoup plus rapide que ne le permettaient à l'époque le traitement papier ou LAD/RAD.

L'intégration des technologies d'hybridation au niveau des logiciels de gestion (ERP, gestion commerciale, logistique) permettrait de publier un document PDF contenant des méta-données exploitables quasiment aussi vite qu'un flux de données EDI. L'acteur à l'autre bout du flux (le client qui reçoit un avis d'expédition, le fournisseur qui reçoit une commande) pourrait alors très rapidement exploiter les méta-données nécessaires contenues dans le document, avec encore plus de fiabilité que la reconnaissance optique de documents.

Un seul véhicule (le document hybride) permettrait alors de gérer les échanges proactifs nécessaires aux flux économiques et les contraintes légales.

A l'heure actuelle, d'autres secteurs d'activités offrent la possibilité de passer du document papier au document digital ou à « l'expérience digitale » : « QR Code », Réalité augmentée, livre papier pour les enfants avec code numérique pour visualiser une séquence multimédia lors de la lecture…

Au-delà des échanges de confiance, l'hybridation commence donc à être bien présente dans nos quotidiens. Le concept d'hybridation n'est pas réservé au simple domaine de l'industrie et de l'éditique. Nous sommes persuadés que notre secteur saura aussi rapidement conjuguer les nouvelles technologies pour plus de confiance et de productivité, dans les échanges comme dans le respect de notre signature de citoyen….

****

5 REMERCIEMENTS

Nous remercions vivement tous les membres qui ont participé à l'élaboration de ce guide :

Vincent Barbey – Adminium
Paul Jeannest – Adminium
Gilles Barré – Alphacode
François Coupez – Caprioli & Associés
Denis Goussé – Cecurity.com
Ghislain Chaumont – Datasyscom
Emmanuel Cudry – eFolia
Alice Meyrignac – Esker
Jean Pierre Doussot – Esopica
Bernard Delecroix – FNTC
Corinne Laurie – FNTC
Rémi Pifaut – Keynectis
François Devoret – Lex Persona
Marc Vinckevleugel – Resocom
Sonia Neble – Resocom
Stephane Manach – Sagemcom
Eric Normand – TrustMission

A PROPOS DE LA LA FÉDÉRATION NATIONALE DES TIERS DE CONFIANCE

La FNTC est aujourd'hui reconnue comme un acteur essentiel de la sécurisation des échanges électroniques et de la conservation des informations, maillons essentiels à la maîtrise de l'ensemble de la vie du document électronique.

Elle regroupe aujourd'hui les principaux professionnels de la dématérialisation répartis en 4 collèges en fonction de leur activité professionnelle, tous concernés directement ou indirectement par la sécurisation des échanges électroniques et la conservation des informations. Elle réunit les opérateurs et prestataires de services de confiance (acteurs de l'archivage électronique, de la certification, de l'horodatage et des échanges dématérialisés ; les éditeurs et intégrateurs de solutions de confiance ; les experts et les représentants des utilisateurs ainsi que les institutionnels et les professions réglementées). Elle a pour but d'établir la confiance, de promouvoir la sécurité et la qualité des services dans le monde de l'économie numérique, d'offrir une garantie aux utilisateurs et de défendre les droits et intérêts liés à la profession des Tiers de Confiance.

LES ADHÉRENTS FNTC:*

Accelya ; ACOSS ; ADEN ; Adminium ; AFCDP ; Alexandre Diehl ; Almerys ; Alphacode ; APECA ; Aproged ; Argus DMS ; Aspheria ; Atos Worldline ; Bernard Starck ; Bruno Couderc Conseil ; Bull ; Cabinet Caprioli & Associés ; Cecurity.com ; Celtipharm ; CertEurope ; ChamberSign ; Chambre Nationale des Huissiers de Justice ; CodaSystem ; Compagnie Nationale des Commissaires aux Comptes ; Conseil National des Greffiers de tribunaux de commerce ; Conseil Supérieur de l'Ordre des Experts-Comptables ; Corus ; Cryptolog ; DARVA ; Darwin Consulting & Finance ; Data One ; Data Syscom ; Demaeter ; Digimedia Interactivité ; Docapost DPS; Document Channel ; Documeris ; DPII Telecom ; Ecosix ; Edificas ; Edokial ; EESTEL ; eFolia ; ESI ; Esker ; Esopica ; Everial ; Explain ; Extelia ; Forum Atena ; G.L.I. Services ; Gdoc Lasercom ; Hervé Schauer Consultants ; Imprimerie Nationale ; Info Service Europe ; Interb@t ; Isilis ; jedeclare.com ; Khan & Associés ; Keynectis ; Lettranet ; Lex Persona ; Locarchives ; Maileva ; MiaXys ; Micrographie Services ; Microlist ; MIPIH ; Neuflize OBC ; Odyssey Services ; Office des Postes et Télécommunications Polynésie Française ; OFSAD ; Omnikles ; OPUS Conseils ; Pauline Le More ; PF Numérique ; Pitney Bowes Asterion ; PPI ; Primobox ; ResoCom ; Scala ; Sogelink/DICT.fr ; SR Développement ; Stocomest ; Syrtals ; Tessi Docubase ; TrustMission ; Union Internationale des Huissiers de Justice ;Valerian ; Voxaly Electionneur ; Wacom.

** Liste arrêtée au 15 novembre 2011*

Fédération Nationale des Tiers de Confiance
19, rue Cognacq-Jay
75007 – Paris
info@fntc.org
www.fntc.org

Conception graphique et illustration : www.idsg.fr