Fédération Nationale des
Tiers de Confiance

VADE-MECUM JURIDIQUE DE LA DÉMATÉRIALISATION DES DOCUMENTS

5ème édition

COLLECTION
LES GUIDES DE LA CONFIANCE
DE LA FNTC

Par le cabinet d'Avocats Caprioli & Associés *(Paris, Nice)*
www.caprioli-avocats.com
Sous la direction de Eric A. Caprioli, Avocat à la Cour,
Docteur en droit, Vice-Président de la FNTC

AVANT-PROPOS

La dématérialisation au cœur de l'économie numérique

Depuis sa création début 2001, quelques mois après la loi du 13 mars 2000 sur la signature électronique, la Fédération Nationale des Tiers de Confiance a multiplié les initiatives pour rassembler les nouveaux acteurs de la confiance numérique.

En 2007, la FNTC mettait à disposition une première édition du vade-mecum permettant de prendre connaissance du cadre juridique applicable au secteur de la dématérialisation.

Depuis, ce guide juridique n'a cessé de s'enrichir au fil des évolutions des différents domaines d'application de la dématérialisation des documents (facture électronique, services de banque électroniques, envois électroniques recommandés, bulletin de paie, vote électronique, contrat d'assurance, billetterie dématérialisée, etc.).

La FNTC est heureuse de vous offrir cette 5ème édition qui prend en compte l'actualité 2011-2012, l'évolution de certains secteurs (assemblées générales d'actionnaires, marchés publics, téléprocédures, etc.) ainsi que les décrets les plus récents ; d'autre part, il aborde de nouveaux sujets tels que :

- la dématérialisation des procédures judiciaires ;
- la protection des données à caractère personnel ;
- les procédures de vérification de l'état civil ;
- la consultation préalable pour les actes réglementaires ;
- etc.

Ce guide a ainsi la vocation de contribuer à une meilleure compréhension des enjeux juridiques de la dématérialisation et générer la confiance numérique indispensable au développement de l'économie numérique.

La FNTC

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

Vade-mecum juridique de la dématérialisation des documents
5ème édition (juin 2012)

Guide l'interopérabilité des coffres-forts électroniques
(mars 2012)

Le bulletin de paie électronique
(mars 2012)

Du livret ouvrier au bulletin de paie électronique
(mars 2012)

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

PROCHAINE PARUTION

Guide de la traçabilité

INTRODUCTION

La dématérialisation des documents et des échanges se généralise pour tous les domaines de la vie des entreprises, des autorités administratives et des citoyens : contrats commerciaux et de consommation, documents des entreprises (factures, bulletins de paie, documents RH, …), coffres-forts électroniques, marchés publics, TVA, impôt sur le revenu, documents douaniers, téléservices en passant par le vote dans les assemblées générales d'actionnaires ou les élections des instances représentatives du personnel (IRP). On ne compte plus les applications liées à la dématérialisation et leurs extensions européenne et internationale. Toutes les entités, qu'elles soient privées, associatives ou publiques ont désormais pignon sur web et elles entendent échanger avec leur environnement par le biais des réseaux numériques, sans pour autant se priver de l'utilisation d'autres technologies (à savoir via le mobile - SMS, MMS - les cartes avec et sans contact, les réseaux sociaux, etc.). En 2011, le chiffre d'affaires de l'ensemble des sites de ventes en ligne a progressé de 22% par rapport à l'année 2010 pour atteindre 37,7 milliards d'euros[1]. De plus, la dématérialisation s'inscrit résolument dans une perspective de développement durable des entreprises. Son impact sur l'environnement ne peut être contesté, alors même que les bénéfices en termes environnementaux ne seront véritablement probants qu'au moment où les impressions papier seront devenues marginales et exceptionnelles. Pour soutenir ce mouvement, les pouvoirs publics devraient encourager par des mesures incitatives à la fois la destruction des documents papier d'origine lorsqu'elles ont des copies numériques fidèles et durables et, la réduction progressive des flux de documents papier (incitation fiscale).

Si l'on s'interroge sur la notion de dématérialisation, elle consiste en la transformation d'un document ou d'un flux de documents papiers, ainsi que les traitements qui lui sont appliqués, en document, flux et traitements numériques. Pour atteindre cet objectif, la dématérialisation cherche à conserver en électronique une valeur juridique équivalente aux documents papier, quels que soient leur support et leur moyen de transmission, ainsi que leurs modalités d'archivage.

Aujourd'hui, la dématérialisation représente pour notre société un enjeu majeur dans les domaines économiques, sociaux et technologiques ; elle constitue un important levier de croissance et d'innovation. Mais elle suppose un encadrement au moyen de règles juridiques claires et cohérentes entre elles et par rapport à l'ensemble des règles de droit commun avec lesquelles elles interagissent afin d'instaurer la confiance et la sécurité qu'attendent les utilisateurs de ces techniques. Dans la pratique, cependant, la dimension juridique ne se résume pas à la conformité juridique du procédé ou du service d'échanges électroniques (audit ou opinion juridique) ou au contentieux. Le droit doit également être présent lors des phases de conception et de mise en œuvre du projet aux côtés des aspects informatique, sécurité, métier, marketing et organisation, afin de contribuer à l'établissement des spécifications fonctionnelles et de la documentation juridique et

1. Source : FEVAD, Bilan annuel du e-commerce en 2011, disponible à l'adresse www.fevad.com

technique à préparer (politiques de certification, d'horodatage et d'archivage, contrats avec les clients et les partenaires, analyses de risques et assurances, …). Cette association imbriquée du droit, de la technique et de l'organisation représente un prérequis essentiel pour la bonne fin du projet.
Sur le marché de la dématérialisation, trois éléments majeurs ont marqués les six derniers mois :

- le développement significatif de l'utilisation des signatures électroniques fondées sur des certificats à usage unique dans de nombreux secteurs pour la souscription de contrats de crédit à la consommation, d'assurances ou de mutuelle ;
- la contractualisation par voie électronique en face à face sur le point de vente de produits ou de services (ex : téléphonie, opérations de banque ou d'assurance, financement de biens de consommation, etc.) ;
- la décision du Conseil constitutionnel qui a invalidé les dispositions de la Carte nationale d'identité électronique relatives à la puce contenant des certificats pour les services commerciaux.

Il convient cependant de souligner que l'environnement juridique de la dématérialisation, actuellement en vigueur dans les différents pays de l'Union européenne, issu pour une large part des transpositions de plusieurs directives européennes, va bientôt être modifié. En effet, la Commission européenne va réviser deux directives fondamentales en les remplaçant par des Règlements européens (un même texte dans tous les Etats de l'UE d'application directe) d'une part, la directive européenne 95/46 du 24 octobre 1995 sur la protection des données à caractère personnel et d'autre part, la directive 1999/93/CE du 13 décembre 1999 sur les signatures électroniques. Toutes les modifications et adjonctions à venir auront une incidence importante sur la dématérialisation des échanges.

Une des ambitions de la Fédération Nationale des Tiers de Confiance est de contribuer à présenter la dématérialisation en l'envisageant sous ses différentes composantes, dont le juridique est une donnée majeure tant du point de vue stratégique qu'opérationnel.

Actuellement, on peut estimer que les technologies et les solutions sont disponibles sur le marché, que le cadre juridique est quasiment achevé bien qu'en constante évolution et que tous les documents (hormis encore quelques exceptions résiduelles) peuvent être dématérialisés, que ce soit dans la sphère privée (I°) ou dans la sphère publique (II°).

Eric A. CAPRIOLI
Avocat à la Cour de Paris, Docteur en droit
Membre de la délégation française aux Nations Unies
Vice-président de la FNTC
e.caprioli@caprioli-avocats.com

SOMMAIRE

I/ LA DEMATERIALISATION DANS LA SPHERE PRIVEE (B TO C, B TO B ET C TO C)

A. Le contrat sous forme électronique (acte juridique électronique)

1. La notion d'écrit sous forme électronique

En droit, les actes juridiques tels que les contrats s'envisagent de deux manières : sur le plan de la preuve (*ad probationem*) et sur celui de la validité (*ad validitatem*).

Il est nécessaire de préciser à ce stade que l'article 1341 du Code civil, et un décret modifiant la procédure civile du 20 août 2004, disposent que la preuve de ces actes peut être apportée par tous moyens jusqu'à 1 500 euros et qu'au-delà, une preuve littérale est nécessaire[2].

a) En matière probatoire

« Ne pas être et ne pas être prouvé, c'est tout un » dit l'adage. La preuve est essentielle en droit car toute prétention juridique passe par une exigence de justification des droits. Cela se traduit par l'intervention d'un tiers (le juge) et la nécessité de le convaincre sur la base de faits pertinents qui permettent de déduire les conséquences juridiques posées par une règle de droit. Avec les technologies de l'information et de la communication (TIC), de nouvelles règles ont été posées en matière d'actes juridiques (ex. : les contrats).

La loi n°2000-230 du 13 mars 2000[3] portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique a intégré l'écrit sous forme électronique dans le dispositif probatoire en insérant l'article 1316-1 dans le Code civil. Cet article dispose que : *« 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 »*.

De cette définition, découlent deux fonctions juridiques essentielles de l'écrit sous forme électronique pour être admis en tant que preuve. Premièrement, l'auteur de l'acte doit pouvoir être dûment identifié, c'est-à-dire que le destinataire doit être en mesure de vérifier son identité au moyen d'éléments techniques suffisamment fiables associés au procédé de signature électronique (certificat électronique d'identification d'une personne). Deuxièmement, l'acte doit avoir été établi et conservé dans des conditions de nature à en garantir l'intégrité. L'intégrité des écrits sous forme électronique, qui doit être assurée pendant tout leur cycle de vie, constitue la pierre angulaire du dispositif **probatoire en matière électronique**.

---

2. Décret n° 2004-836 du 20 août 2004 portant modification de la procédure civile, J.O. n° 195 du 22 août 2004 en vigueur le 1er janvier 2005, p. 15032.
3. JO n° 62 du 14 mars 2000, p. 3968. V. E. A. Caprioli, Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000, JCP, éd. E, Cah. Dr. Entrep., n°2, année 2000, p. 1 et s. Sur les aspects juridiques de la signature, de l'écrit sous forme électronique et de l'archivage électronique, voir les études et analyses publiées sur le site : www.caprioli-avocats.com.

b) En matière de validité d'un acte juridique

En ce qui concerne les exigences à des fins de validité des actes juridiques (par exemple, les contrats qui imposent des exigences de forme), la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[4] a introduit, dans le Code civil, les articles 1108-1 et 1108-2 relatifs à la validité des actes juridiques conclus sous forme électronique. Ainsi, l'article 1108-1 du Code civil dispose que : *« Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il 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.*
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 qu'elle ne peut être effectuée que par lui-même »[5]. A défaut d'écrit requis comme condition de validité de l'acte (ex : contrat de crédit à la consommation, statuts de société, etc.), la valeur juridique de ces actes pourrait être remise en cause. Sur ce fondement, le contrat pourrait être annulé et considéré comme n'ayant jamais existé. On peut d'ailleurs remarquer ici que le législateur renvoie aux articles 1316-1 et 1316-4 du Code civil sur la preuve pour caractériser et définir les conditions d'établissement et de conservation d'un écrit à titre de validité.
Toutefois, tous les actes ne peuvent pas être dématérialisés. L'article 1108-2 du Code civil énonce que certains actes sous seing privé considérés comme graves et où l'écrit est exigé pour leur validité, sont exclus de l'électronique. Sont ainsi concernés par cette exception :

- d'une part, *« les actes sous seing privé relatifs au droit de la famille et des successions »* (par exemple : contrat de mariage, adoption, convention préalable au divorce par consentement mutuel,…) ;
- et d'autre part, *« les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession »* (par exemple, le cautionnement).

2. La notion de signature électronique[6]

L'article 1316-4 du Code civil relatif à la signature caractérise, au même titre que l'article 1316-1 du Code civil propre à l'écrit sous forme électronique, la recevabilité d'un acte sous forme électronique. La signature - et plus particulièrement la signature électronique - apparaît donc comme un élément fondamental de l'écrit sous forme électronique.

L'article 1316-4 du Code civil dispose 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*

4. JO du 22 juin 2004, p.11168 et s.
5. Voir Cass. civ. 1ère, 13 mars 2008, note Eric A. Caprioli, C.C.E, Juillet-août 2008, comm. 97 ; C.C.E. Juin 2008, comm. 80.
6. Voir le Guide de la signature électronique, Collection « Les Guides de la confiance de la FNTC », 2008, disponible sur le site www.fntc.org mais aussi Eric Caprioli, Signature et confiance dans les communications électroniques en droit français et européen, in Libre droit, Mélanges Ph. Le Tourneau, Dalloz, 2008, p. 155 et s., disponible sur le site www.caprioli-avocats.com.

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 d'identification de la signature électronique doit être fiable - comme le rappelle la jurisprudence[7] - et doit garantir le lien avec l'acte auquel elle s'attache. Le décret en Conseil d'Etat en question, à savoir le décret n°2001-272 du 30 mars 2001[8] pris pour l'application de l'article 1316-4 du Code civil, a trait à la signature électronique sécurisée bénéficiant de la présomption de fiabilité, une catégorie particulière de signature électronique.

Son article 1er al. 2 énonce qu'une signature électronique sécurisée est une signature électronique qui satisfait 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.

L'article 2 de ce décret pose, quant à lui, les conditions qui permettent de présumer fiable un procédé de signature électronique. Ainsi, pour bénéficier de la présomption, ce procédé doit mettre en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et la vérification de cette signature repose nécessairement sur l'utilisation d'un certificat électronique qualifié. Si la signature électronique sécurisée ne garantit pas ces deux conditions cumulées, alors la présomption ne sera pas reconnue, et elle sera soumise au même régime qu'une signature électronique simple.

Bien qu'il existe une distinction entre la signature électronique « simple » et la signature électronique sécurisée présumée fiable, **les deux types de signature électronique ont la même valeur juridique dès lors qu'elles reposent sur l'utilisation d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache (art. 1316-4 al. 2 du Code civil)**. Seule la charge de la preuve est inversée. Pour une signature électronique sécurisée présumée fiable, la charge de la preuve de l'absence de fiabilité du procédé utilisé repose sur celui qui conteste la valeur juridique de la signature (et plus généralement l'acte signé). Pour une signature électronique simple, la charge de la preuve de la fiabilité du procédé utilisé pour signer l'acte en cause repose sur celui qui se prévaut de la signature électronique.

En outre, il faut bien comprendre que tous les types de signatures électroniques « simples » sont valables dès lors qu'elles répondent aux exigences posées par l'article 1316-4 du Code

---

7. En ce sens, à propos d'une signature scannée (non admise) pour la signature d'une déclaration d'appel, CA Besançon, 20 oct. 2000, JCP éd. G, 2001, II, 10606, p. 1890 et s., note E. A. Caprioli et P. Agosti ; confirmé par la Cour de cassation le 30 avril 2003, Bull. civ. 2003, n°118, p. 101 et s. (disponible sur le site : www.legifrance.gouv.fr). Toutefois, le 17 mars 2011, la Cour de cassation a également eu l'occasion de décider à propos d'une notification de redressement URSSAF par courrier, qu'une signature pré-imprimée n'est pas électronique et de ce fait n'a pas à respecter les dispositions de l'article 1316-4 du Code civil (Cass. civ. 2ème, 17 mars 2011, pourvoi n°10-30501, disponible sur le site www.legifrance.gouv.fr.).

8. Décret 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. Voir Eric A. Caprioli, Commentaire du décret n°2001-272 du 30 mars 2001 relatif à la signature électronique, Revue de Droit Bancaire et financier, Mai/juin 2001, p.155 s. ; v. égal. Laurent Jacques, Le décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique, J.C.P. éd. E, 2001, Aperçu rapide, p. 1601 ; F. Coupez, C. Gailliègue, Vers une signature électronique juridiquement maîtrisée. A propos de l'arrêté du 31 mai 2002, C.C.E.., novembre 2002, p. 8 et s.

civil, à savoir l'identification du signataire, la manifestation du consentement des parties aux obligations découlant de l'acte, la fiabilité du procédé qui garantit le lien (logique) de la signature avec l'acte auquel elle s'attache.

Par exemple, une signature électronique fondée sur un certificat « éphémère » ou « à usage unique » (valable pour une transaction) pourra être reçue devant les tribunaux sous réserve que soient dûment respectées les exigences précédentes. Cette pratique, utilisée de plus en plus fréquemment pour la contractualisation en agence ou à distance de certains produits bancaires (épargne, crédit à la consommation, …) ou dans d'autres domaines (ex : assurances) permet d'assurer une identification suffisamment pertinente pour une opération déterminée d'un client connu de l'établissement (ou identifié par lui en face à face lors de la transaction), et ce, pendant un laps de temps relativement court (de l'ordre de une à trois minutes). Une fois l'opération terminée, le certificat n'est plus valide et ne peut plus être utilisé. Il sera archivé avec le contrat signé dans un fichier de preuve contenant l'ensemble des données démontrant qu'à un instant donné, la signature était valable et qu'elle a produit les effets juridiques escomptés (acceptation des termes du contrat et intégrité, validation des certificats utilisés, …). Ces procédés de signature pourront également être utilisés dans le cadre de la signature d'un contrat en agence en présence physique du client (ex : téléphonie mobile). Le représentant du prestataire technique pourra attester de la fiabilité du processus de contractualisation électronique et du fichier de preuve, le cas échéant, devant le tribunal.

La Commission européenne a organisé une première consultation dans le but de réviser la directive n°1999/93/CE portant sur un cadre communautaire pour les signatures électroniques du 13 décembre 1999[9] et en vue de la préparation d'une initiative concernant la reconnaissance mutuelle des procédés d'identification et d'authentification électroniques. Une évolution du cadre communautaire (un projet de Règlement européen sera diffusé en 2012) et une prise en compte au niveau des organisations de standardisation internationale (ETSI) sont en cours. L'objectif est de contribuer à la confiance sur le marché en développant les signatures électroniques, encore trop peu utilisées, selon la Commission européenne dans les Etats membres.

3. De l'original à la copie électronique

a) Distinction entre l'original et la copie électroniques des actes juridiques

La distinction selon laquelle le document doit être considéré comme un original électronique ou comme une copie est importante car le régime juridique applicable est lui-même distinct et sa conséquence est déterminante en cas de litige (incidence sur la preuve) : **la hiérarchie des preuves place l'original au-dessus de la copie.**

Le titre original se définit comme *« un écrit dressé, en un ou plusieurs exemplaires, afin de constater un acte juridique, signé par les parties à l'acte (ou par le représentant), à la différence de la copie »*[10]. L'ordonnance du 16 juin 2005[11] prise en application de l'article 26 de la LCEN est venue consacrer juridiquement une nouvelle fiction juridique, l'exemplaire d'un original sous forme électronique : *« L'exigence d'une pluralité d'originaux est réputée*

9. JOUE L. 13 du 19 janvier 2000, p. 12
10. Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2003. V° Original.
11. JO n°140 du 17 juin 2005, p.10342.

satisfaite pour les contrats sous forme électronique lorsque l'acte est établi et conservé conformément aux articles 1316-1 et 1316-4 et que le procédé permet à chaque partie de disposer d'un exemplaire ou d'y avoir accès » (art. 1325, al. 5 du Code civil). Cet article renvoie aux articles 1316-1 et 1316-4 du Code civil déjà cités pour les écrits requis à titre de validité. En conséquence, les mêmes conditions d'identification de l'auteur et d'intégrité du contenu de l'acte devront être respectées pour l'établissement et la conservation de l'acte. L'acte doit pouvoir être envoyé (aux) ou mis à disposition des parties signataires.

En ce qui concerne la copie, elle se définit comme *« toute reproduction littérale d'un original qui, n'étant pas revêtue des signatures qui en feraient un second original, ne fait foi que lorsque l'original ne subsiste plus et sous les distinctions établies par l'article 1335 du Code civil, mais dont la valeur est reconnue à des fins spécifiées (notamment pour les notifications), sous les conditions de la loi (copies établies par des officiers publics compétents) »*[12]. Selon l'article 1348 alinéa 2 du Code civil, **à défaut d'original**, la copie, pour pouvoir être retenue par les juges, doit être *« la reproduction non seulement **fidèle** mais aussi **durable** »* du titre original[13]. La **fidélité** n'est pas définie juridiquement ; en revanche, selon la norme AFNOR NF Z 42-013, un document est fidèle *« s'il permet de reconstituer toute l'information nécessaire aux usages auxquels le document d'origine est destiné »*. La copie électronique ou numérique doit donc être fidèle par rapport à l'original papier étant précisé qu'il n'existe pas de régime juridique pour la copie d'un original électronique qui est un original électronique. La **durabilité**, quant à elle, est selon l'article 1348 al. 2 du Code civil *« toute reproduction indélébile de l'original qui entraîne une modification irréversible du support »*. La copie pourrait donc être tout document (Word, pdf, etc.) transitant sur les réseaux, mais dont l'archivage s'opère conformément aux exigences de la nouvelle version de la norme à laquelle la Fédération Nationale des Tiers de Confiance a largement contribué, et qui a pris effet le 3 mars 2009[14]. En vertu des principes issus des versions antérieures de la norme, l'archivage devait s'opérer sur un support non réinscriptible (disque optique numérique, technologie WORM[15]). Au nombre des innovations de cette version de la norme NF Z 42-013 figurent notamment la reconnaissance des WORM logiques (technologie utilisant des supports tels que des disques durs), ainsi que la reconnaissance de la conservation sur des supports réinscriptibles avec les garanties et protections offertes par des moyens technologiques reconnus tels la signature électronique et l'horodatage. Désormais, les écrits originaux, établis sous forme électronique avec les procédés de sécurité associés, sont appréhendés dans toute la diversité des solutions d'archivage électronique utilisées en pratique. La prise en compte de la signature électronique et la définition de plusieurs niveaux d'exigences pour adapter les solutions aux besoins spécifiques constituent dans ce cadre des avancées significatives. La nouvelle norme conserve le chapitre spécifiquement dédié aux Tiers archiveurs qui était déjà présent dans la version antérieure.

L'apport essentiel de la notion d'original sous forme électronique introduite à l'article 1325 alinéa 5 du Code civil est donc d'intégrer un élément distinctif essentiel entre l'original et la copie : la signature électronique à laquelle il est fait référence dans l'article 1316-4 du Code civil, mais aussi à l'article 1316-1 du Code civil. L'original électronique doit rester intègre au moment de son établissement (sa signature) et pendant toute la durée de conservation.

---

12. Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2003. V° Copie.
13. Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2003. « 2. Ecrit en vue de constater un acte juridique ou un acte matériel pouvant produire des effets juridiques ».
14. JO n°48 du 26 février 2009, p. 3444.
15. Pour « Write Once, Read Many », traduit en français dans la norme par «support de stockage permettant de n'écrire qu'une seule fois et de lire plusieurs fois».

b) La jurisprudence et la copie électronique d'un courrier papier

Concernant la valeur probatoire de la copie informatique d'un document, la question a été l'objet de deux décisions de la deuxième chambre civile de la Cour de cassation rendues à trois ans d'intervalle : le 4 décembre 2008[16], saisie d'une affaire dans laquelle la *« copie »* d'une lettre envoyée par la CPAM à un employeur (l'envoi étant contesté) consistait en un fichier reconstitué à partir du contenu de la lettre d'une part, et d'un fond de page faisant apparaître un logo plus récent d'autre part, la Cour de cassation avait indiqué, au visa des articles 1334, 1348 et 1316-4 du Code civil, *« qu'il résulte des deux premiers de ces textes que lorsqu'une partie n'a pas conservé l'original d'un document, la preuve de son existence peut être rapportée par la présentation d'une copie qui doit en être la reproduction non seulement fidèle mais durable ; que selon le troisième, l'écrit sous forme électronique ne vaut preuve qu'à condition que son auteur puisse être dûment identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*. Elle a ainsi jugé que la Cour d'appel privait de base légale sa décision en ne recherchant pas si le document électronique produit (une copie informatique non signée d'un courrier) par une CPAM répondait bien aux exigences des articles du Code civil visés. En l'espèce, ce qu'avait surtout sanctionné la Cour de cassation, c'était le fait qu'il existait un fort indice d'absence de fidélité de la copie produite devant les juges, puisque le logo figurant sur le courrier en principe envoyé en 2003 n'avait été utilisé par la CPAM qu'à partir de 2004.

Le 17 mars 2011, saisie d'une affaire similaire où la preuve de l'envoi du courrier devait également être faite alors que le logo du fond de page avait changé, la Cour de cassation[17] valide l'analyse de la Cour d'appel dans cette affaire : celle-ci n'avait pas parlé de « copie » mais de « réplique informatique » identifiant l'émetteur et corroborée par un second élément de preuve consistant **en l'accusé de réception du courrier en question** : *« Mais attendu que l'arrêt relève que la caisse produit une réplique informatique de l'avis de clôture, faisant apparaître clairement l'auteur de ce document, agent gestionnaire du dossier de Mme X..., et justifie avoir adressé à la société une lettre recommandée, réceptionnée le 17 juillet 2003, ainsi qu'il résulte des mentions inscrites sur l'accusé de réception, lequel porte en outre les mêmes références que celles afférentes au dossier de Mme X... ;*

Que de ces constatations et énonciations, procédant de son pouvoir souverain d'appréciation de la valeur et de la portée des éléments de preuve produits devant elle, la cour d'appel a pu déduire, par un arrêt suffisamment motivé, que la caisse avait satisfait à son obligation d'information à l'égard de la société (…) ».

La notion de « réplique informatique » est une innovation jurisprudentielle. Ce n'est ni un écrit au sens de l'article 1316-1 du code civil, ni une copie fidèle et durable (article 1348 du code civil).Toutefois, cette « réplique » associée aux mentions inscrites sur l'accusé de réception, voit sa force probante reconnue.

---

16. Cass. civ. 2ème, 4 décembre 2008, SNC Continent France c/ CPAM de la Marne, pourvoi n° 07-17.622, Note Eric Caprioli, Communication, Commerce Electronique (Lexisnexis), février 2009, n°19, p. 44 et s.

17. Cass. civ. 2ème, 17 mars 2011, n°10-14.850, F-D, SAS Carrefour hypermarchés c/ Caisse primaire d'assurance-maladie d'Ile-et-Vilaine, JurisData n°2011-003705, Voir E. A. Caprioli, Valeur juridique de la « réplique informatique » d'un courrier d'information de la CPAM, Com. Comm. Electr. n°7, Juillet 2011, comm. 73.

4. La gestion de preuve

L'écrit sous forme électronique est souvent requis à titre de preuve d'un acte. Les utilisateurs, spécialement les entreprises, doivent fournir un document électronique qui puisse être retenu comme preuve par les tribunaux (mais aussi les médiateurs et les arbitres). Or, il est important de pouvoir se prévaloir de l'écrit sous forme électronique et par-là de la signature électronique au moment de la signature dudit écrit. Sans cela, la valeur juridique d'un acte pourrait être remise en cause.

Pour ce faire, la création d'une Autorité de gestion de preuve (A.G.P.) peut être considérée comme un moyen pertinent et efficace pour vérifier la signature électronique le plus tôt possible après son apposition sur l'écrit sur support électronique et gérer dans le temps les traces des vérifications réalisées (signatures du contrat, certificat, chemin de confiance) en établissant un fichier de preuve contenant ces éléments. Ce dernier établit que les vérifications ont été effectuées au moment de la signature (horodatage et scellement du fichier) conformément aux textes en vigueur[18]. Il doit pouvoir emporter la conviction du juge, en cas de litige, quant à la valeur juridique et à la force probante de l'écrit sous forme électronique auquel il est techniquement lié. Il devra être conservé. L'A.G.P. émet une politique de gestion de preuve (P.G.P) pour fixer ses engagements en termes techniques, sécurité et juridiques et ceux de ses composantes et des utilisateurs. Le fichier de preuve, une fois constitué, pourra être versé au service d'archivage électronique.

B. Le contrat par voie électronique (commande en ligne)

1. Le processus de contractualisation en ligne

Introduit par la LCEN[19], les articles 1369-4 et suivants du Code civil consacrent la conclusion d'un contrat par voie électronique lorsqu'une personne commande un bien corporel ou incorporel ou un service sur l'Internet. Ce processus de contractualisation se distingue du dispositif prévu pour les actes juridiques (art. 1316 et s. du Code civil) en ce que la signature électronique n'est pas requise pour disposer d'une preuve (mais rien n'interdit de la prévoir !)[20], dans l'hypothèse où le montant de l'opération est inférieur à 1 500 euros.
Dans un but de protection des acheteurs, l'article 1369-4 du Code civil impose au professionnel (qu'il soit une personne physique ou une personne morale) les éléments constitutifs de l'offre de contracter, à savoir :

- *« Les différentes étapes à suivre pour conclure le contrat par voie électronique ;*
- *Les moyens techniques permettant à l'utilisateur, avant la conclusion du contrat, d'identifier les erreurs commises dans la saisie des données et de les corriger ;*
- *Les langues proposées pour la conclusion du contrat ;*
- *En cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre et les conditions d'accès au contrat archivé ;*
- *Les moyens de consulter par voie électronique les règles professionnelles et commerciales auxquelles l'auteur de l'offre entend, le cas échéant, se soumettre ».*

---

18. Les articles 1316-1 et suivants du Code civil et l'article 8 de l'ordonnance du 8 décembre 2005 (pour la sphère publique, voir infra II/).
19. Ph. Stoffel-Munck, La réforme des contrats du commerce électronique, Comm. Com. Elect., 2004, Etude 30., E. A. Caprioli et P. Agosti, La confiance dans l'économie numérique, Les Petites Affiches, 3 juin 2005, p 4 s.
20. Par exemple en prévoyant que le clic de confirmation active une signature électronique fondée sur un certificat à usage unique.

Notons que l'offre de contracter engagera le professionnel tant qu'elle sera accessible par voie électronique.

Ensuite, l'article 1369-5 du Code civil établit une procédure à suivre lors d'une commande en ligne. En cas de non-respect des conditions posées, le contrat ne sera pas valablement conclu. L'acceptation de l'offre de contracter par le consommateur se concrétise par un geste électronique tout simple : le fameux *« clic »* sur une icône ou sur un *« oui »* ou un *« j'accepte »*. La manifestation du consentement de l'acheteur est l'élément fondamental du contrat.

Outre le fait que l'acceptation de la proposition doit être expresse, elle doit être éclairée. En effet, concernant les commandes en ligne, dès lors que le client a établi sa commande (par une série de clics), qu'il a *« eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation »*, ce dernier doit la confirmer au *« cybervendeur »*, le contrat est formé avec ce nouveau clic. D'où l'idée du *« double clic »* plus protecteur pour le consommateur. Cette confirmation constitue le moment de la formation définitive du contrat.

Au surplus, le vendeur *« doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée »*. Le dernier alinéa de l'article 1369-5 du Code civil précise, en outre, que *« la commande* [de l'acheteur], *la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès ».*
Au côté de ces règles applicables aux transactions conclues par un particulier sur un site marchand, deux exceptions sont posées à l'article 1369-6[21] du même Code civil :

- les contrats conclus uniquement par courrier électronique ;
- les conventions conclues entre deux professionnels (principe de liberté de preuve entre commerçants).

On peut dès lors constater l'existence d'une large palette de modalités de contractualisation en ligne, avec ou sans signature électronique.

2. Le paiement électronique

Le paiement est *« au sens courant, le versement d'une somme d'argent en exécution d'une obligation de somme d'argent[22] »*. Cette définition est applicable aux paiements électroniques. La seule différence notable avec le papier et les échanges physiques consiste en sa rapidité en termes de débit de compte.

Les moyens de paiement électronique se sont multipliés avec l'explosion du commerce électronique. Il s'agit, de nos jours, d'un impératif économique et commercial pour les banques mais aussi pour d'autres acteurs économiques qu'ils soient importants ou plus modestes. Ces moyens de paiement peuvent reposer sur un support matériel (cartes à

21. « Il est fait exception aux obligations visées aux 1° à 5° de l'article 1369-4 et aux deux premiers alinéas de l'article 1369-5 pour les contrats de fourniture de biens ou de prestations de services qui sont conclus exclusivement par échange de courriers électronique.
Il peut, en outre, être dérogé aux dispositions de l'article 1369-5 et des 1° à 5° de l'article 1369-4 dans les conventions conclues entre professionnels ».
22. Voir G. Cornu, Vocabulaire juridique, éd. Quadrige, PUF, 2003. V° Paiement. Selon l'article 1315 du Code civil, « celui qui se prétend libéré (d'une obligation) doit justifier le paiement ou le fait qui a produit l'extinction de son obligation.».

puce et sans contact), l'usage d'un logiciel et une connexion à un réseau de communication (Internet, SMS,…). L'identification de la personne comme le paiement peuvent s'effectuer par le biais de plusieurs canaux.

S'agissant des moyens de paiement se fondant sur un support matériel, la carte bancaire est le moyen traditionnel. La carte à puce est aussi très utilisée, mais sa lecture suppose un lecteur de carte comme les terminaux de paiement ou les distributeurs de billets de banque. Il est important de noter que le Code Monétaire et Financier (CMF) protège les consommateurs en cas d'utilisation frauduleuse de la carte de paiement. L'article L. 133-19 du Code monétaire et financier issu de l'ordonnance n°2009-866 du 15 juillet 2009[23], pose le principe que le porteur n'est pas engagé si les données de la carte (numéro, date d'expiration, pictogramme au verso) ont été frauduleusement utilisées pour un paiement à distance[24]. Il en est de même en cas de contrefaçon de la carte et si, au moment de l'opération, le titulaire se trouvait en possession physique de la carte. Ainsi, dès lors que le porteur signale sans tarder, au plus tard dans les treize mois suivant le débit, une opération de paiement non autorisée, les sommes contestées lui sont restituées immédiatement et sans frais. Le prestataire de services de paiement, *« le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu »*[25]. Le porte-monnaie électronique (ex : le système Monéo) entre également dans cette catégorie. Des unités de valeurs sont stockées sur cette carte à puce pour effectuer progressivement des débits au fur et à mesure des achats. Ce procédé a été l'objet d'un règlement n°2002-13 du Comité de la réglementation bancaire et financière, homologué par un arrêté du 10 janvier 2003[26] et modifié à deux reprises en 2007 et 2009. Ainsi, l'établissement émetteur doit assurer la sécurité du paiement et garantir la traçabilité pendant deux ans des chargements et des encaissements des unités et des transactions suspectes. Toutefois, l'usage de ce type de paiement est limité à de petits montants, la valeur maximale chargée sur la carte étant de 150 euros. Il est également possible d'utiliser d'autres solutions de porte-monnaie électronique (ex : Moneytronic) où les unités de valeur sont stockées sur le disque dur du détenteur du compte ou de l'organisme détenteur de ce solde. Ce procédé sert avant tout aux transactions en ligne.

Quant aux paiements à distance, le moyen le plus utilisé reste la communication en ligne (sécurisée) du numéro de la carte bancaire (ainsi que de la date d'expiration et de certains numéros au verso). Par ailleurs, on constate le développement de moyens de paiement sécurisé associant la messagerie électronique de l'internaute. C'est par exemple le cas de Paypal, Propay… Enfin, un internaute peut payer en ligne sa commande via son fournisseur d'accès à Internet : il s'agit d'une solution de type kiosque.

Notons, d'autre part, que la directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur[27] a été

23. Voir infra.
24. Voir Y. Gérard, L'utilisation frauduleuse des instruments de paiement, JCP Entreprise et Affaire n°2, 14 janvier 2010, 1034.
25. Article L. 133-18 du C.M.F.
26. Voir JO du 1er février 2003, texte n°12 p. 2003 ; A l'heure actuelle la directive 2009/110 doit être transposée et elle remplace la directive 2000/46 à l'origine de l'arrêté du 10 janvier 2003. Il est donc probable que ce texte évolue prochainement.
27. JOUE L. 319 du 5 décembre 2007.

transposée en droit français par l'ordonnance n°2009-866 du 15 juillet 2009[28] susmentionnée, suivie du décret d'application n°2009-934 du 29 juillet 2009[29]. La directive de 2007 tend à harmoniser les règles existantes afin de rendre les paiements électroniques à l'intérieur de l'Union européenne (virements, prélèvements automatiques et paiements par carte) aussi simples et sûrs que les paiements effectués à l'intérieur d'un État membre. L'objectif est de créer dans toute l'Union européenne un marché intégré des paiements (le SEPA : espace unique de paiement en euros). **Les informations à fournir aux utilisateurs, les modalités de contestation des paiements et les responsabilités associées seront similaires d'un Etat à l'autre ce qui devrait assurer une plus grande sécurité juridique aux utilisateurs[30].**

Cette Directive repose essentiellement sur trois éléments :

- **Le droit de fournir des services de paiement au public :**
  L'objectif est d'harmoniser les conditions d'accès au marché applicables aux prestataires de services de paiement autres que les établissements de crédit[31].
- **Les exigences de transparence et d'information :**
  La Directive impose des obligations d'information à l'ensemble des prestataires de services de paiement, que ces derniers proposent des instruments de paiement SEPA ou des instruments de paiement « traditionnels »[32].
- **Droits et obligations des utilisateurs et des prestataires de services :**
  La Directive vise enfin à clarifier les principaux droits et obligations des utilisateurs et des prestataires de services de paiement en harmonisant les règles nationales[33], ce qui devrait contribuer à un renforcement de la sécurité juridique.

De plus, jusqu'alors, chaque Etat membre disposait de son propre secteur bancaire régi par ses propres règles et utilisant ses propres solutions technologiques. La Commission européenne ayant estimé que les initiatives visant à intégrer les infrastructures devaient être menées par le secteur bancaire lui-même, les banques et les organismes de crédit européens se sont regroupés au sein d'un Conseil européen des paiements (EPC). C'est ce Conseil qui a élaboré les instruments de paiement communs du projet SEPA. Ils fonctionneront selon des modalités juridiques, fonctionnelles et techniques communes, qu'ils soient utilisés pour réaliser des paiements nationaux ou transfrontaliers dans la zone SEPA. Ces instruments sont le virement SEPA ou SCT *(SEPA Credit Transfer)*, le

28. Ordonnance n°2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, JO n°0162 du 16 juillet 2009, p.11868 texte n°13 – Voir G. Notté, Fourniture de services de paiement et création des établissements de paiement, JCP Entreprise et Affaires n°31, 30 juillet 2009, act. 358 ; dossier spécial dans le JCP Entreprise et Affaires n°2, 14 janvier 2010, 1031 à 1034 : T. Bonneau, Le domaine d'application de l'ordonnance, Notions d'instruments de paiement, de services de paiement et d'établissements de paiement au sens de l'ordonnance, application dans l'espace et dans le temps, domaine subjectif : consommateurs, professionnels, R. Bonhomme, Le déclenchement de l'opération de paiement : le consentement et l'ordre, S. Torck, L'exécution et la contestation des opérations de paiement et Y. Gérard, L'utilisation frauduleuse des instruments de paiements.

29. Décret n°2009-934 du 29 juillet 2009 pris pour l'application de l'ordonnance n°2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, JO n°0175 du 31 juillet 2009, p. 12744, texte n°12.

30. Voir notamment le Guide « Du mandat au mandat électronique », publié en décembre 2009, suite aux travaux du Groupe de travail e-Finance de la Fédération Nationale des Tiers de Confiance.

31. Art. 5 et s.

32. Art. 30 et s.

33. Art. 51 et s.

prélèvement SEPA ou SDD (SEPA Direct Debit), et la carte bancaire selon les modalités du SCF *(SEPA Card Framework)*.

Le SEPA Direct Debit est destiné à remplacer le prélèvement automatique domestique. Le calendrier de la mise en œuvre des instruments de paiement SEPA étant sans cesse repoussé, le Parlement européen a adopté le 14 février 2012 un Règlement[34] qui fixe une échéance au 1er février 2014. La norme « SEPA Core Debit, Scheme Rulebook », établie par l'EPC[35], définit un ensemble complet de règles opérationnelles pour la gestion du système de prélèvement du SDD dont les formats et protocoles sont les mêmes que ceux préconisés pour le virement SEPA (norme ISO 20022, identification IBAN et BIC). La version 5.0 applicable depuis le 19 novembre 2011 intègre de nouvelles informations relatives à la gestion des mandats (notamment en cas de rejet ou d'anomalie d'une opération). Une version 6.0 a été adoptée le 17 novembre 2011 et sera applicable à compter du 17 novembre 2012, au même titre que la version 4.0 du SDD Business to Business (B2B) Rulebook.

La signature et les certificats électroniques auront leurs rôles à jouer dans l'établissement des mandats sous-jacents pour ces trois moyens de paiement. Les traces des paiements électroniques devront faire l'objet d'un archivage.

Lors de la transposition en droit français de la directive de 2007, par l'ordonnance de 2009, le Code Monétaire et Financier a été profondément modifié. Les services de paiement peuvent désormais être proposés aussi bien par les banques que par des « établissements de paiement », dont le statut est mis en place par l'ordonnance[36]. Par ailleurs, le processus de paiement est réformé, imposant notamment un traitement électronique des ordres de paiement, interdisant la pratique des dates de valeur pour les opérations de paiement électronique et mettant à la charge des prestataires de services de paiement de nouvelles obligations, dont ils devront tenir compte dans le cadre de leurs conditions générales et dans leurs processus de contractualisation en ligne et papier.

De plus, la loi n°2010-1249 du 22 octobre 2010 de régulation bancaire et financière[37] a habilité le gouvernement à prendre dans les six mois de la promulgation de la loi, par voie d'ordonnance, les mesures de transposition de la directive n°2009/110 du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements[38] (remplaçant la directive n°2000/46 du 18 septembre 2000 qui encadrait jusqu'à présent l'activité des établissements de monnaie électronique). Cette ordonnance n'a finalement jamais été adoptée.

En revanche, le gouvernement français a pris l'ordonnance n°2011-398 du 14 avril 2011 portant transposition de la directive n°2009/44/CE du Parlement européen et du Conseil du 6 mai 2009 modifiant la directive n°98/26/CE concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres et la directive

34. Règlement (UE) n°260/2012 du 14 mars 2012 du Parlement européen et du Conseil établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n°924/2009, JOUE L 94 du 30 mars 2012, p. 22–37.
35. http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_direct_debit_(sdd).
36. V. P. Bouteiller, La transposition en droit français des disposition européennes régissant la fourniture de services de paiement et portant création des établissements de paiement, JCP Entreprise et Affaires n°39, 24 septembre 2009, 1897.
37. JO n°0247 du 23 octobre 2010, p. 18984, texte n°1, article 23.
38. JOUE L. 267 du 12 octobre 2009.

2002/47/CE concernant les contrats de garantie financière, en ce qui concerne les systèmes liés et les créances privées[39]. Cette dernière a principalement modifié le Code monétaire et financier.

C. Dispositions communes

1. L'archivage électronique[40]

L'archivage peut être défini techniquement comme *« l'ensemble des actions, outils et méthodes mises en œuvre pour conserver à moyen ou long terme des informations dans le but de les exploiter[41] »*. Une définition légale de l'archivage, applicable pour l'essentiel aux seules personnes publiques ou privées gérant un service public, se trouve à l'article L. 211-1 du Code du patrimoine qui dispose que l'archivage est la conservation de *« l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité »*.

Chaque système d'archivage a des spécificités juridiques, techniques et organisationnelles propres. Un état des besoins prenant en compte ces trois dimensions est un préalable à l'élaboration de politiques d'archivage[42] à mettre en œuvre en fonction des différents documents et de leur finalité juridique ou de gestion (courriers électroniques signés ou non, actes juridiques, conditions générales, documents comptables ou sociaux, photos, plans, états de comptes bancaires, numérisation de documents papier/GED, …).

L'archivage électronique concerne à la fois les actes juridiques signés et les processus contractuels conclus en ligne, dont la signature n'est pas toujours exigée, mais aussi les pièces justificatives diverses (factures, bulletins de paie, etc.) ainsi que l'ensemble des informations de gestion de l'entité, le tout constituant son **patrimoine informationnel. La protection et la sécurité de ces actifs « immatériels » doivent être assurées**[43].

a) Les documents signés

L'archivage d'un contrat signé répond essentiellement à deux finalités juridiques :
- prouver le contenu d'un acte juridique (articles 1316-1 et 1316-4 du Code civil) voire la constatation d'un fait juridique ;
- ou respecter une exigence de forme (article 1108-1 du Code civil relatif à la validité des actes juridiques conclus sous forme électronique).

---

39. JO du 15 avril 2011, p. 6625 et s.

40. E. Caprioli, La conservation électronique des preuves, à paraître dans les Cahiers du CRID (Belgique) en 2012, éd Bruylant et qui sera disponible sur le site www.caprioli-avocats.com.

41. Définition du Dictionnaire du multimédia, AFNOR, 1995.

42. Voir pour les échanges électroniques en droit public. Politique et Pratiques d'archivage (sphère publique), version du 24 juillet 2006, disponible à l'adresse : http://www.ssi.gouv.fr/IMG/pdf/ArchivageSecurise-P2A-2006-07-24.pdf . Cette politique est une trame qui doit être adaptée au contexte (ex : collectivité territoriale, Hopitaux publics, Etablissements publics, …). En outre, pour le privé, cette politique-type devra être adaptée en fonction de l'activité de l'entreprise et des contraintes juridiques afférentes aux documents archivés.

43. E. Caprioli, Introduction au droit de la sécurité des systèmes d'information, in Droit et technique - Etudes à la mémoire du Professeur Xavier Linant de Bellefonds, Ed. Litec, novembre 2007, disponible sur le site www.caprioli-avocats.com.

L'intégrité de l'acte doit être garantie pendant tout le cycle de vie du document, c'est-à-dire de son établissement à sa conservation (et donc à sa restitution). La conservation devra donc préserver les fonctions essentielles de l'acte : identification et intégrité, c'est-à-dire qu'elle devra porter à la fois sur le document signé lui-même ainsi que sur les éléments permettant sa vérification. Aussi, sans entrer dans le détail de la technologie utilisée, la loi lie la preuve des actes sous seing privé à la fiabilité du procédé de signature électronique utilisé dont il est traité à l'article 1316-4 du Code civil. La preuve du consentement émis sera garantie par des moyens fiables de sécurité portant sur la vérification de l'identité du signataire et de l'intégrité informationnelle de l'acte. En ce sens, la *« solidité »* et la durabilité du lien (logique) entre la signature électronique et le message ou le fichier constituent un aspect fondamental.
L'accent doit être mis sur deux éléments importants au niveau de la conservation car la durée et les modalités de conservation sont déterminées en fonction de la nature du document à archiver :

• **La durée de conservation :**

En matière civile, la loi n°2008-561 du 17 juin 2008 portant réforme de la prescription en matière civile[44] a profondément modifié le régime de la prescription. Ainsi, le délai de prescription de droit commun, pour les actions personnelles et mobilières, passe de 30 ans à 5 ans[45] mais peut durer jusqu'à 20 ans (délai butoir)[46]. Les actions réelles immobilières continuent à se prescrire par 30 ans [47]. Il est à noter également que la loi prévoit la possibilité pour les parties d'aménager la prescription dans certains contrats[48].

La loi a prévu des dispositions de transition avec les anciens délais de prescription. Ainsi, il est important de noter que les dispositions de la loi qui allongent la durée d'une prescription s'appliquent lorsque le délai de prescription n'était pas expiré au 19 juin 2008 (article 26-I de la loi). Il est alors tenu compte du délai déjà écoulé. S'agissant des dispositions de la loi qui réduisent la durée de la prescription, elles s'appliquent aux prescriptions à compter du 19 juin 2008, sans que la durée totale puisse excéder la durée prévue par la loi antérieure. Enfin, lorsqu'une instance a été introduite avant le 19 juin 2008, l'action est poursuivie et jugée conformément à la loi ancienne (article 26-II de la loi). On comprend bien que les deux régimes (antérieur et postérieur au 19 juin 2008) subsistent et **sont cumulatifs**. La gestion des documents archivés par une entreprise devra donc prendre en compte cette dichotomie chronologique.

Une autre distinction fondamentale s'impose : elle concerne les **délais de conservation obligatoires des documents archivés et les délais de prescription relatifs aux droits et obligations y afférents.** Le délai de conservation des documents est un délai préfix, non-susceptible d'interruption et il ne concerne que l'action tendant à la production des documents (comptables, sociaux, …). En revanche, le délai de prescription (civil

44. JO du 18 juin 2008, p. 9856 et s. V. Eric A. Caprioli, Les apports de la loi n°2008-561 du 17 juin 2008 portant réforme de la prescription en matière civile, Com. Comm. Electr. n°12, Décembre 2008, comm. 141, p. 46 et s, disponible sur le site www.caprioli-avocats.com.
45. Article 2224 du Code civil.
46. Article 2232 du Code civil.
47. Article 2227 du Code civil.
48. Article 2254 du Code civil. La durée de prescription peut donc, avec l'accord des parties, être réduite au minimum à un an ou allongée de 10 ans maximum ; étant noté qu'un tel aménagement conventionnel est toutefois exclu dans les contrats avec les consommateurs (art. L. 137-1 du c. consom.) et avec les mutuelles (art. L. 221-12-1 du code de la Mutuelle).

ou commercial) peut être interrompu par une action en justice, même en référé, par un commandement ou une saisie, signifié, à celui qu'on veut empêcher de prescrire, ou par la reconnaissance que le débiteur ou le possesseur fait du droit contre lequel il prescrivait. Les documents doivent donc être conservés jusqu'à l'expiration des divers délais de prescription légale. Ce qui compte, c'est l'extinction des effets juridiques liés à l'acte. Une fois le temps écoulé, toute action en justice fondée sur cette pièce devient caduque.

TYPE DE DOCUMENTS	*DÉLAI DE CONSERVATION*	*DÉLAI DE PRESCRIPTION*
Contrats	Délai particulier : 10 ans pour les contrats conclus en ligne avec les consommateurs d'un montant supérieur à 120 euros (art L. 134-2 du C. cons).	• 5 ans (pour les contrats établis après le 18 juin 2008) *sauf si les obligations sont soumises à des exigences particulières (art L.110-4 du C. com) (ex : délai de prescription fondée sur un contrat d'assurance : 2 ans à compter de la survenance de l'événement – art. L 114-1 du Code des assurances).*
Factures	Délai commercial : 10 ans (art. L. 123-22 C. com) Délai fiscal : 6 ans (art L. 102-B LPF).	• 5 ans (pour les factures émises après le 18 juin 2008) • 10 ans (avant le 18 juin 2008 et dans un cadre commercial) • Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les factures ou pièces ont été établies.
Livres et registres comptables Bons de commande	Délai commercial : 10 ans (art. L. 123-22 C. com) Délai fiscal : 6 ans (art L. 102-B LPF) dont les trois premières années sous forme électronique.	• 5 ans (pour les documents comptables émis après le 18 juin 2008) • 10 ans (avant le 18 juin 2008 et dans un cadre commercial) • Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les documents ou pièces ont été établis.
Justificatifs comptables (ex. : notes de frais)	Délai commercial : 10 ans (art. L. 123-22 C. com) Délai fiscal : 6 ans (art L. 102-B LPF) dont les trois premières années sous forme électronique.	• 5 ans (pour les documents comptables émis après le 18 juin 2008) • 10 ans (avant le 18 juin 2008 et dans un cadre commercial) • Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les documents ou pièces ont été établis.
Correspondances commerciales liées à une opération comptable	Délai commercial : 10 ans (art L. 123-22 du C. com) .	• 5 ans (pour les correspondances émises après le 18 juin 2008) • 10 ans (avant le 18 juin 2008 et dans un cadre commercial).
Relevé de comptes		• 5 ans (pour les documents établis après le 18 juin 2008) *sauf si les obligations sont soumises à des exigences particulières (art L.110-4 du C. com) (ex. : cf. convention de comptes bancaires).*

TYPE DE DOCUMENTS	*DÉLAI DE CONSERVATION*	*DÉLAI DE PRESCRIPTION*
Comptes annuels	Délai commercial : 10 ans (art. L. 123-22 C. com.) Délai fiscal : 6 ans (art L. 102-B LPF) dont les 3 premières années sous forme électronique.	• 5 ans (pour les documents comptables émis après le 18 juin 2008) • 10 ans (avant le 18 juin 2008 et dans un cadre commercial) Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les documents ou pièces ont été établis.
Statuts, annexes, pièces modificatives		• 5 ans à compter de la radiation du RCS (pour les statuts établis après le 18 juin 2008)
Bulletins de paie	Pour l'employeur : • 5 ans (art. L. 3243-4 du Code du travail) • 10 ans en tant que pièce comptable (art. L. 123-22 C. com.) • 6 ans en tant que pièce fiscale (art L.102-B LPF) dont les 3 premières années sous forme électronique Pour le salarié : celui-ci est incité à le conserver pour une durée illimitée (art. R. 3243-5 du Code du travail), pour l'aider, à sa retraite, dans sa reconstitution de carrière.	
Contrat de travail		• 5 ans à compter de la fin du contrat (pour les documents émis après le 18 juin 2008) • 10 ans (avant le 18 juin 2008 et dans un cadre commercial)
Déclaration URSSAF	• 3 ans suivant l'année de l'envoi litigieux • 5 ans en cas de travail illégal • 2 ans concernant le paiement des majorations de retard (art. L. 244-3 du Code de la sécurité sociale)	

• **Les modalités de conservation :**

Elles peuvent être prescrites par un texte qui impose des modalités spécifiques (ex : comptabilité informatisée, factures électroniques ou EDI, documents liés au droit du travail, …). A défaut, il faudra être en mesure de garantir les exigences juridiques de conformité du droit commun, applicables aux écrits électroniques et aux copies numériques.
Dans la recommandation de la CNIL du 11 octobre 2005[49], il est prévu que les données archivées soient supprimées ou anonymisées au-delà du délai mentionné dans la déclaration.

b) Les processus de contractualisation en ligne

L'article L. 134-2 du Code de **la consommation dispose** que *« lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel **assure la conservation de l'écrit** qui le constate pendant un délai déterminé par ce même décret et **en garantit à tout moment l'accès** à son cocontractant si celui-ci en fait la demande »*. Cet article met à la charge du professionnel une obligation de conserver le contrat conclu par voie électronique avec un consommateur.

Le décret n°2005-137 du 16 février 2005[50] a ainsi fixé **le montant à 120 euros et le délai de conservation à dix ans à compter de la conclusion du contrat** lorsque la livraison du bien ou l'exécution de la prestation est immédiate. Dans le cas contraire, le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci. Le cocontractant professionnel doit en outre garantir l'accès au contrat à son cocontractant, à tout moment, si celui-ci formule une demande en ce sens.

En revanche, il convient de relever que cet article L. 134-2 n'est pas applicable aux relations entre professionnels (B to B).

Il est à noter que le professionnel (vendeur le plus souvent) pourra mettre en place une procédure d'archivage en interne, mais il peut aussi avoir recours à un tiers indépendant, le tiers archiveur[51], prestataire de services d'archivage électronique. Ce tiers devra prendre en compte un certain nombre d'exigences s'il entend être conforme à la norme NF Z 42-013 de mars 2009 précitée. De plus, le Système d'information du tiers archiveur (ou une partie dédiée au service d'archivage) peut faire l'objet d'une certification du système de management de la sécurité de l'information conformément aux normes ISO 27001 à 27005.

49. Délibération CNIL n°2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel. JO n°41 du 18 février 2005, p. 2780.
50. JO n°41 du 18 février 2005, p. 2780.
51. Pour les tiers archiveurs, la Fédération Nationale des Tiers de Confiance a élaboré un label qui prévoit la réversibilité des archives entre les prestataires labellisés. Un autre label de la FNTC s'applique aux coffres-forts numériques.

2. Les conventions sur la preuve

La convention sur la preuve doit être considérée comme une clause contractuelle ayant pour finalité de définir les modes de preuve admissibles entre les parties, la charge de la preuve et les modalités de règlement des conflits de preuve (sous réserve des dispositions du Code de la consommation). Elle garantit la force probante des documents établis et produits par voie électronique en précisant les éléments techniques et de sécurité pris en compte ainsi que les effets juridiques y associés.

Leur validité dans le domaine informatique est reconnue depuis plusieurs années par la jurisprudence[52] (signature informatique par la saisie du code PIN dans les opérations avec carte bancaire).

La loi n°2000-230 du 13 mars 2000 précitée[53] a entériné la pratique des conventions sur la preuve en introduisant un nouvel article 1316-2 dans le Code civil qui dispose *« lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention [sur la preuve] valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support »*. A contrario, si une convention sur la preuve a été conclue entre les parties, le juge doit l'appliquer mais encore faut-il qu'elle soit valable, étant précisé que certaines dispositions peuvent être réputées non écrites.
Il est évident que ces conventions sur la preuve ne doivent pas porter atteinte à des règles d'ordre public (ex : le droit de contester la preuve) ainsi qu'aux dispositions légales et réglementaires sur les clauses abusives. **Ces conventions s'appliquent aussi bien en B to B, qu'en B to C ou C to C**. Elles doivent être considérées comme un gage de sécurité juridique. Il est donc important de préciser ici que les conventions sur la preuve doivent être rédigées de manière équilibrée pour éviter qu'un tribunal ne remette en cause leur valeur juridique et par là, la valeur juridique des documents établis par le système d'information.

D. Domaines d'application de la dématérialisation

1. Le droit social

Il est désormais envisageable de dématérialiser les bulletins de paie, les contrats de travail et les contrats de travail temporaire. D'autres documents RH sont également susceptibles d'être dématérialisés (notes de frais, demande de congés,…) sous réserve de leur conformité juridique.

S'agissant **des contrats de travail temporaires**, deux situations doivent être distinguées :
• le contrat de mise à disposition (contrat entre l'entreprise de travail temporaire et l'entreprise utilisatrice) peut être dématérialisé à condition de respecter les exigences du Code civil ou s'il est conclu dans le cadre d'une convention de preuve ;
• et le contrat de mission (contrat entre le travailleur temporaire et l'entreprise de travail temporaire). Les règles propres à la conclusion de ce type de contrat sont posées aux articles L. 1251-5 et s. du Code du travail. A titre indicatif, la **signature du contrat** de mission est **d'ordre public**. S'il est établi sous forme électronique, il devrait donc être signé

52. Cass. civ. 1ère, 8 nov. 1989, n°86-16.196, Sté Crédicas c/ Cassan : D. 1990, p. 369, note C. Gavalda.
53. JO n°62 du 14 mars 2000, p. 3968.

électroniquement. Son omission entraîne, à la demande du salarié, la requalification du contrat de mission en contrat de droit commun à durée indéterminée.

Le bulletin de salaire se définit comme *« le décompte détaillé des divers éléments de la rémunération du travailleur, obligatoirement délivré par l'employeur lors de la paie »*[54].
Dans sa nouvelle rédaction issue de la loi n°2009-526 du 12 mai 2009[55], l'article L. 3243-2 du Code du travail, relatif au bulletin de salaire dispose que *« lors du paiement du salaire, l'employeur remet aux personnes mentionnées à l'article L. 3243-1 une pièce justificative dite bulletin de paie. Avec l'accord du salarié concerné, cette remise peut être effectuée sous forme électronique, dans des conditions de nature à garantir l'intégrité des données. Il ne peut exiger aucune formalité de signature ou d'émargement autre que celle établissant que la somme reçue correspond bien au montant net figurant sur ce bulletin.*
Les mentions devant figurer sur le bulletin ou y être annexées sont déterminées par décret en Conseil d'Etat ». Le nouvel article L. 3243-4 du même code précise que *« l'employeur conserve un double des bulletins de paie des salariés ou les bulletins de paie remis aux salariés sous forme électronique pendant cinq ans »*. Peu importe la forme électronique ou papier, ce qui compte, c'est la remise de la pièce justificative.

La pratique de la dématérialisation des bulletins de paie a ainsi été consacrée par le législateur. Il reste néanmoins des questions en suspens. Les caractéristiques liées au consentement du salarié et à son expression ne sont pas définies par la loi. Par prudence, il faudrait envisager un consentement individuel par écrit : écrit papier ou écrit électronique. Par ailleurs, les modalités et garanties entourant la remise électronique du bulletin de paie ne sont pas détaillées dans la nouvelle rédaction du Code du travail. Il est simplement demandé à l'employeur une garantie d'intégrité du bulletin lors de la remise.

Force est de constater que la loi n'impose pas d'obligation de signature du bulletin de paie, car c'est une pièce justificative dont la valeur reconnue de jurisprudence constante est celle du commencement de preuve par écrit. En effet, même si le bulletin de paie est souvent utilisé en pratique pour justifier d'une situation patrimoniale vis-à-vis de tiers (banques, etc.), le Code du travail ne prescrit pas la signature de celui-ci et ce n'est pas un acte juridique au sens du Code civil. En conséquence, sur le plan technique, tout procédé permettant d'assurer l'intégrité des données de façon fiable est acceptable au regard du Code du travail (signature électronique sécurisée, horodatage, signature avec un certificat de serveur, fonction de hachage de la pièce justificative, etc.). Toutefois, pour des raisons de sécurité, on peut recommander d'utiliser un procédé de signature électronique d'une personne morale (certificat de serveur qui assure le scellement/intégrité du bulletin de paie). De son côté, le salarié n'a pas à signer la pièce.

Il faudra donc préciser les conditions de la remise dans le document constatant l'accord du salarié. D'autres fonctions importantes devront être également garanties : la confidentialité, la réversibilité et une accessibilité permanente au salarié concerné.
Enfin et concernant la conservation des bulletins de paie par l'employeur pendant une durée de cinq ans, il semble nécessaire que l'intégrité des documents soit assurée pendant cette période, eu égard notamment aux avancées technologiques prévisibles au cours de la durée d'archivage.

54. Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2003. V° Bulletin de paie.
55. Loi n°2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, JO n°0110 du 13 mai 2009, p. 7920, texte n° 1 - E. Caprioli, La dématérialisation des bulletins de paie, Cahier de droit de l'entreprise n°4, juillet 2009, prat. 20.

La FNTC a publié une série de documents dont un guide sur la « e-paie » remis à jour en mars 2012[56], fruit des travaux d'un groupe de travail qui a réfléchi aux meilleures pratiques du marché dans le domaine du bulletin de paie transmis sous forme électronique et qui a pour vocation de sensibiliser et d'accompagner les entreprises dans leur déploiement dans le cadre de projets de « e-paie ».

La FNTC, ainsi que le Cabinet d'avocats Caprioli & Associés ont également apporté leur expertise aux travaux du groupe AFNOR qui a normalisé le bulletin de paie électronique dans la norme NF Z 42-025 (« *Gestion du bulletin de paie électronique* ») publiée en mai 2011.

Le contrat de travail qu'il soit à durée déterminée ou indéterminée est défini comme *« un contrat synallagmatique à titre onéreux caractérisé par la fourniture d'un travail en contrepartie du paiement d'une rémunération et (critère essentiel) par l'existence d'un lien de subordination juridique du travailleur à l'employeur »*[57]. La dématérialisation de ce type de contrat permettrait de le transmettre par voie électronique et de l'intégrer directement dans les systèmes de gestion intégrée des entreprises. Cela entraînerait une réduction des coûts, des délais de traitement et serait susceptible d'accroître l'efficacité des directions de ressources humaines.
Les CDD et les CDI (mais aussi les avenants aux contrats) peuvent donc être dématérialisés, étant entendu que les employeurs doivent prévoir non seulement la mise à disposition des outils permettant la signature électronique de leurs salariés, mais aussi les modalités d'archivage sécurisé et d'accès aux exemplaires destinés aux salariés.

2. La facture électronique

La directive n°77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée a été modifiée par la directive n°2001/115 du 20 décembre 2001[58]. Cette dernière a été ensuite transposée en droit français par l'article 17 de la loi de finances rectificative pour 2002[59]. La directive 2006/112/CE du Conseil du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoutée[60] a remplacé la notion de « transmission » de la facture par la notion de « mise à disposition ». La notion de transmission implique de la part de l'émetteur une remise obligatoire de la facture au destinataire alors que la notion de mise à disposition ouvre l'opportunité à l'émetteur de remettre la facture au destinataire ou d'inviter ce dernier à venir la chercher chez l'émetteur, via une interface internet par exemple.

Depuis, une nouvelle directive modifiant la directive 2006/112 a été adoptée le 13 juillet 2010[61]. Elle a pour but d'accroître l'utilisation de la facturation électronique, de réduire les charges pour les entreprises, de soutenir les petites et moyennes entreprises (PME) et d'aider les États membres à lutter contre la fraude. Pour atteindre ces objectifs, les autorités

56. Téléchargeable sur le site de la FNTC : www.fntc.org.
57. Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2003. V° Contrat de travail.
58. JOCE L 15/24 et s. du 17 janvier 2002. V. le site www.caprioli-avocats.com pour le régime juridique des factures électroniques signées et EDI.
59. Loi n°2002-1576 du 30 décembre 2002, J.O n°304 du 31 décembre 2002, p. 22070.
60. JOUE L 347 du 11 décembre 2006, p. 1–118.
61. Directive 2010/45/UE du Conseil du 13 juillet 2010 modifiant la directive 2006/112/CE relative au système commun de taxe sur la valeur ajoutée en ce qui concerne les règles de facturation, JOUE L 189 du 22 juillet 2010, p. 1 et s.

fiscales doivent accepter les factures électroniques dans les mêmes conditions que les factures sur support papier en vertu de l'application du principe de non-discrimination de l'écrit électronique. Elle vise également à supprimer de la directive 2006/112/CE les obstacles entravant le recours à la facturation électronique, en cessant de faire des signatures électroniques ou de l'échange des données informatisées les seules modalités pour établir des factures électroniques. Seules l'authenticité de l'origine, l'intégrité du contenu et la lisibilité de la facture restent les conditions nécessaires à l'établissement et à la conservation des factures électroniques. Toutefois, cela ne signifie pas la fin des factures électroniques signées ou EDI : ces modes de facturation, qui apportent de telles garanties, restent les modes les plus sûrs et fiables sur le marché. Ces dispositions ne seront applicables qu'à partir du 1er janvier 2013.

En attendant, c'est l'article 17 de la loi de finances rectificative pour 2002 qui est applicable. Il a instauré un régime fiscal spécifique pour les factures électroniques en introduisant la facture électronique signée électroniquement. Il a réformé les articles 289 et 289 bis du Code général des impôts (CGI) relatifs aux règles de facturation. Les modalités d'application de la facturation électronique ainsi que les obligations des assujettis ont été précisées dans l'Instruction du 7 août 2003[62]. L'arrêté du 18 juillet 2003[63], quant à lui, 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. Le décret n°2003-659 du 18 juillet 2003[64] pris pour l'application de l'article 17 de la loi de finances rectificative pour 2002 du 30 décembre 2002 a précisé les conditions propres aux factures électroniques, dotées d'une signature électronique.

Depuis 2002, et en attendant la transposition de la directive précitée, la transmission de la facture électronique sur le territoire français ou entre Etats membres de l'Union européenne peut s'effectuer selon deux modalités sécurisées dont les conditions d'utilisation diffèrent :
- la signature électronique des factures ;
- l'échange de données informatisées (EDI ou *« Electronic Data Interchange »*).

Le système de facturation électronique doit garantir l'authenticité de l'origine des factures ainsi que l'intégrité de leur contenu. Si l'acceptation préalable de ce système de facture électronique par le destinataire est requise (de façon tacite ou par écrit), il est vivement recommandé de l'établir sous la forme d'une convention qui en précisera les modalités. Par ailleurs, les assujettis peuvent transmettre au même destinataire un lot de factures - sous réserve du respect de certaines conditions - en ne mentionnant qu'une seule fois les mentions communes à ces factures mais à condition que la totalité des informations propres à chaque facture soit accessible. Quant à la conservation de l'original de ces factures, elle doit être assurée : sur un support informatique pendant une durée au moins égale au délai de trois ans[65] ; sur tout support, choisi par l'entreprise, pendant les trois années suivantes. On soulignera ici qu'en pratique, il sera difficile de changer le support des factures signées électroniquement, sous peine de perdre leur valeur fiscale (perte de la signature lors du passage au papier). Enfin, la facture émise et celle reçue doivent être identiques et restituables par l'entreprise à qui l'administration en fait la demande[66], dans un format habituellement admis dans les usages commerciaux. L'administration doit donc pouvoir, à des fins de contrôle, accéder en ligne à ces factures et aux données jointes.

62. Instruction de la Direction générale des impôts n°136 du 7 août 2003, 3CA.
63. JO du 20 juillet 2003, p. 12273.
64. JO du 20 juillet 2003, p. 12272.
65. Article L. 169 al. 1er du LPF.
66. Si l'administration le demande, la restitution est effectuée sur support papier.

Les factures transmises au moyen d'une signature électronique tiennent lieu de facture d'origine en application des articles 286 et 289 du CGI. L'article 96 F-I de l'annexe III du CGI porte sur la définition et les caractéristiques de la signature électronique en matière fiscale. L'exigence requise est l'utilisation d'un certificat électronique fourni par un prestataire de certification électronique afin d'identifier l'émetteur de la facture. Ce certificat n'a pas à être « qualifié » au sens du décret du 30 mars 2001, mais doit présenter un degré de sécurité suffisant. Il est également prévu que les personnes morales puissent signer une facture (certificat de serveur). C'est un moyen visant à garantir que la facture émane bien de l'entreprise émettrice et n'a pas subi d'altération depuis sa création. Cependant, l'administration fiscale peut à tout moment utiliser son droit de contrôle, d'enquête ou de communication pour s'assurer que les normes techniques figurant à l'article 96 F-I du CGI ont bien été respectées.

Pour les factures transmises par EDI, un système de télétransmission de factures répondant à certaines normes techniques[67] doit être utilisé. Deux exigences techniques doivent être respectées. D'abord, le message facture doit comporter au minimum les mentions obligatoires prévues par l'article 242 *nonies* A de l'annexe II du CGI. Ces mentions doivent figurer dans des zones du message facture que le logiciel doit rendre obligatoire. Une vérification doit être faite à l'émission et à la réception du message. Ensuite, une liste récapitulative de tous les messages émis et reçus doit être établie au fur et à mesure, quel que soit le support, et comporter un certain nombre de mentions obligatoires[68] ainsi que les anomalies éventuelles intervenues lors de chaque transmission. Par ailleurs, des contrôles inopinés de la conformité du fonctionnement du système de télétransmission peuvent être effectués par l'administration fiscale[69].

Afin de prendre en compte des pratiques internes aux entreprises en matière d'archivage des factures, l'Administration fiscale a précisé les conditions dans lesquelles les entreprises émettrices de factures électroniques et transmises sur support papier aux destinataires peuvent être dispensées de l'obligation de conserver sous forme papier le double des factures ainsi transmises conformément à l'Instruction fiscale du 11 janvier 2007[70].

Un groupe de travail « E-facture » de la FNTC a étudié la question de la facture électronique signée et a établi un référentiel et une grille d'audit du label COREF FNTC-PFFE relatifs aux plates-formes d'échange de factures électroniques signées[71]. A leurs suites, la FNTC a lancé le 3 février 2010 un guide sur la facture électronique. Les travaux se réfèrent aux meilleures pratiques du marché dans le domaine de la facturation électronique et ont pour vocation de sensibiliser et d'accompagner les entreprises dans leur déploiement dans le cadre de projets de dématérialisation fiscale.

---

67. Ces normes doivent être équivalentes à celle définie à l'article 2 de la recommandation 1994/820/CE de la Commission du 19 octobre 1994 concernant les aspects juridiques de l'échange de données informatisées.

68. Les mentions minimales à indiquer sont : le numéro et la date de la facture, la date et l'heure de constitution du message, les montants hors taxe et toutes taxes de la transaction et éventuellement le code devise, les éléments d'identification de l'émetteur ou du récepteur donnés par le système de télé-transmission et la version du logiciel utilisée.

69. Voir le guide de la FNTC et référentiel pour les plates-formes de facturation, publié en février 2010, www.fntc.org.

70. B.O.I. n°4 du 11 janvier 2007.

71. La label de ces plateformes de factures électroniques est délivré par la FNTC, après avis du Coref ; voir : http://www.fntc.org/content/view/749/86/.

3. Les services de banque électronique : l'exemple des relevés de compte

En vertu de l'article D. 312-5 du Code monétaire et financier, les services bancaires de base comprennent « 5° *l'envoi mensuel d'un relevé des opérations effectuées sur le compte* ». Ce relevé des opérations, récapitulant toutes les opérations enregistrées sur le compte d'un client pendant une période déterminée, généralement mensuelle, a été désigné par la pratique sous le vocable de « relevé de compte » bancaire.

Le Code monétaire et financier ne mentionnant pas expressément le support que doit emprunter le relevé de compte bancaire et, dans le silence de la loi, l'envoi de relevé de compte électronique étant dès lors possible, de plus en plus d'établissements financiers ont proposé à leurs clients de recevoir leur relevé de compte bancaire mensuel par l'Internet à la place de la version papier et ce gratuitement pour les consommateurs (en vertu des dispositions existantes depuis la loi MURCEF[72]).

Ces relevés ont la même valeur juridique que les relevés de compte papier, aucune forme n'étant imposée à la banque pour son obligation de délivrance de ces documents. On ne pouvait toutefois que recommander d'utiliser des moyens techniques permettant d'assurer l'intégrité du relevé de compte établi, afin que d'autres tiers puissent valablement se fier à leur contenu. En effet, les cas sont nombreux en pratique, où le relevé de compte est utilisé pour justifier d'une situation patrimoniale ou de l'absence de crédit grevant la situation financière du titulaire du compte. En pratique, très souvent, les clients des banques en ligne ayant signé une convention de banque en ligne (contenant une convention sur la preuve) peuvent accéder via leur compte personnel à un document à télécharger – sous format pdf – récapitulant les opérations des trente derniers jours, ces documents étant rendus accessibles pour une durée variable en fonction des établissements. Cette procédure vient remplacer l'envoi postal du relevé de comptes.

Depuis, l'ordonnance n°2009-866 du 15 juillet 2009[73] relative aux conditions régissant la fourniture de services de paiement et portant création des « établissements de paiement », qui transpose en droit français la directive « Service de paiement »[74], a notamment pris en compte la dématérialisation du support de l'information que doivent fournir les prestataires de services de paiement à leurs clients.

Prévoyant spécifiquement la fourniture, par le prestataire de services de paiement ou encore l'établissement de crédit, d'avis d'opéré au client à la suite d'un paiement (art. L. 314-14 du Code monétaire et financier), la disposition indique que cette fourniture peut, si elle s'inscrit dans le cadre d'une convention de service, ne s'opérer qu'une fois par mois (art. L. 314- 14- II). Le prestataire ou la banque a ainsi la possibilité en pratique de continuer à délivrer le relevé de compte mensuel intégrant les éléments d'information de l'avis d'opéré précité. Le prestataire ne peut cependant pas refuser de délivrer gratuitement sur papier, au moins une fois par mois, lesdits relevés (article L. 314-14 II alinéa 2 du CMF).

La directive « Service de paiement » ayant prévu la possibilité de la fourniture de ces informations sur « support durable », l'ordonnance de transposition fait de même, définissant également cette notion à l'art. L. 314-1-IV comme *« tout instrument permettant à l'utilisateur*

72. La loi n°2001-1168 du 11 décembre 2001 portant mesures urgentes de réformes à caractère économique et financier, dite loi MURCEF, a été publiée au Journal officiel du 12 décembre 2001.
73. JO n°0162 du 16 juillet 2009, p. 11868.
74. Directive 2007/64/CE du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, JOUE L 319 du 5 décembre 2007, p.1 et s.

de services de paiement de stocker les informations qui lui sont personnellement adressées, d'une manière telle que ces informations puissent être consultées ultérieurement pendant une période adaptée à leur finalité et reproduites à l'identique ».

A l'issue de cette transposition, il n'y a donc pas lieu de modifier la pratique de délivrance par les banques des relevés de compte électronique.

4. Les envois électroniques recommandés

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[75] relative à l'accomplissement de certaines formalités contractuelles par voie électronique (formation et exécution du contrat).
Cette innovation marque un pas en avant formidable dans la dématérialisation des correspondances et des notifications dans la pratique des contrats. On peut regretter que ces dispositions ne s'appliquent pas aux autres envois recommandés prévus dans les lois et règlements, en dehors des contrats.

L'article 1369-8 du Code civil reconnaît juridiquement l'existence du courrier électronique recommandé avec ou sans avis de réception, mais aussi les lettres recommandées « hybrides », envoyées par voie électronique, éditées sur papier et acheminées par voie postale.

Le procédé utilisé pour l'envoi d'un courrier électronique recommandé répond à quatre exigences énumérées à l'alinéa premier de l'article 1369-8 du Code civil :
- le procédé doit identifier le tiers 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.

Par ailleurs, deux modalités de réception du courrier recommandé électronique sont prévues par l'alinéa 2. 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 du courrier électronique recommandé 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, le courrier recommandé est alors adressé 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 »*[76].

La datation de l'expédition et le cas échéant de la réception doivent résulter d'un procédé électronique dont la fiabilité est présumée lorsque ce procédé satisfait à des conditions fixées par décret en Conseil d'Etat (Décret n°2011-434 du 20 avril 2011[77]).

L'avis de réception peut être adressé à l'expéditeur sous forme électronique ou par tout autre moyen, sous réserve qu'il permette sa conservation.

---

75. JO n°140 du 17 juin 2005, p. 10342 et suivants.
76. Article 1369-8 al. 2 du Code civil.
77. JO du 21 avril 2011, p. 7093.

Le décret du 2 février 2011[78] indique les modalités d'envoi des lettres recommandées par courrier 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.

L'ordonnance du 16 juin 2005 a également créé la lettre simple électronique en introduisant l'article 1369-7 du code civil. Ce texte reproduit dans l'électronique le fameux « cachet de La Poste faisant foi ». Ainsi, à titre d'illustration, l'offre de contrat de crédit immobilier qui est subordonnée, aux termes de l'article L. 312-10 du Code de la consommation, au fait que *« le prêteur est tenu de formuler par écrit une offre adressée gratuitement par voie postale à l'emprunteur »* et l'acceptation d'une telle offre qui doit être donnée par lettre *« le cachet de la poste faisant foi »* peuvent désormais être passées par voie électronique, à la condition que le procédé de transmission du courrier permette de garantir la date d'expédition. Les exigences de fiabilité de la datation électronique de la lettre électronique ont également 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[79]. 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[80].

5. Les actes authentiques sous forme électronique

L'acte authentique est un acte qui *« étant reçu ou dressé par un officier public compétent, selon les formalités requises (sur papier ou support électronique), fait foi par lui-même jusqu'à inscription de faux »*[81]. Sont donc des actes authentiques les actes notariés ainsi que leurs annexes, à la condition que celles-ci soient revêtues d'une mention la constatant et signée du notaire, ou encore les actes établis par les huissiers de justice dans le cadre de leur office ministériel, c'est-à-dire les actes de signification, les décisions de justice et les actes de l'état civil.
L'article 1317 du Code civil, introduit par la loi n°2000-230 du 13 mars 2000, dispose que les actes authentiques électroniques peuvent être dressés sur support électronique à la condition qu'ils soient établis et conservés dans des conditions fixées par un décret en Conseil d'Etat. Deux décrets ont été adoptés en application de ce texte : il s'agit des décrets

78. 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, JO n°0029 du 4 février 2011, p. 2274. Rappelons que l'adoption de ce décret, très attendu, fait suite à la décision du Conseil d'Etat du 22 octobre 2010 ordonnant au gouvernement son édiction dans un délai de 6 mois. Pour un commentaire de ce décret, v. Eric Caprioli, La lettre recommandée électronique, un nouveau décret pour la « confiance numérique », Com. Comm. Electr. avril 2011, comm. n°40, p. 41.
79. JO du 21 avril 2011, p. 7094.
80. Sur le régime juridique des recommandées électroniques, v. E. Caprioli, Fiche pratique : Les lettres recommandées électroniques, Cahiers de droit de l'entreprise, Mai-juin 2011.
81. V. G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2003. V° Authentique.

n°2005-972 et 2005-973 du 10 août 2005[82] qui respectivement modifient le décret n°56-222 du 29 février 1956[83] relatif aux huissiers de justice et le décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires. Ils sont entrés en vigueur le 1er février 2006.

Des conditions sont communes aux deux professions :

1/ Les systèmes d'information des huissiers de justice et des notaires, en charge du traitement, de la conservation et de transmission de l'information doivent :

- être agréés par l'autorité dont ils dépendent (le Conseil supérieur du notariat - CSN - pour les notaires, la Chambre nationale des huissiers de justice - CNHJ - pour les huissiers de justice) ;
- garantir l'intégrité et la confidentialité du contenu de l'acte ;
- être interopérables entre eux ainsi qu'avec les organismes auxquels ils doivent transmettre des données.

2/ Les huissiers de justice et les notaires doivent utiliser un procédé de signature électronique sécurisée conforme aux exigences du décret n° 2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique. A ce titre, les notaires ont obtenu la qualification de leur certificat en 2007, renouvelé le 20 août 2010 pour 3 ans, et les huissiers de justice l'ont obtenue le 12 mars 2009[84].

3/ Les huissiers de justice et les notaires peuvent numériser tout document annexé à l'acte, établi sous forme papier, à la condition que ce soit au moyen d'un procédé de numérisation garantissant sa reproduction à l'identique.

4/ La date certaine de l'acte devra être mentionnée en lettres dans l'acte électronique avant sa signature par l'officier public ou ministériel, ce qui exclut l'horodatage électronique des actes.

5/ La conservation des actes authentiques électroniques doit être assurée *« dans des conditions de nature à en préserver l'intégrité et la lisibilité »*. Ils doivent être transmis immédiatement pour les notaires et dans les quatre mois suivant l'élaboration de l'acte pour les huissiers de justice, au *« minutier central »* contrôlé par le CSN ou par la CNHJ. L'officier public ou ministériel qui a dressé l'acte ou qui le détient *« en conserve l'accès exclusif »*. Il convient de pouvoir vérifier les actes conservés ainsi que le processus concourant à sa création en assurant la traçabilité de ces opérations. Le répertoire recensant les actes passés par l'officier public ou ministériel pourra être tenu sur support électronique ou papier.

6/ Enfin, les décrets précisent que les opérations successives justifiées par la conservation de l'acte authentique, notamment les migrations de support, ne retirent pas à l'acte sa nature d'original[85].

Des exigences particulières sont applicables à chaque profession.

---

82. JO du 11 août 2005, en vigueur le 1er février 2006.
83. Décret n°56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, JO du 3 mars 1956.
84. Voir le site de www.lsti-certification.fr.
85. Compte tenu des délais de conservation particulièrement longs exigés pour les actes authentiques (75 ans pour les notaires, 25 ans pour les autres officiers publics ou ministériels d'après l'article 17 du décret n°79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques modifié), cette précision était nécessaire.

6. Le vote électronique[86]

D'un point de vue général, la délibération n°2010-371 du 21 octobre 2010 de la CNIL adopte une recommandation relative à la sécurité des systèmes de votes électroniques qui prend en compte les évolutions des techniques et de la pratique. Trois de ces votes électroniques seront exposés.

a) Le vote électronique au sein des Assemblées générales d'actionnaires

L'article L. 225-107 du Code de commerce dispose que *« tout actionnaire peut voter par correspondance, au moyen d'un formulaire dont les mentions sont fixées par décret en Conseil d'Etat »*. De plus, « II. *Si les statuts le prévoient, sont réputés présents pour le calcul du quorum et de la majorité les actionnaires qui participent à l'assemblée par visioconférence ou par des moyens de télécommunication permettant leur identification et dont la nature et les conditions d'application sont déterminées par décret en Conseil d'Etat* ». Ce vote peut donc s'opérer soit par voie postale, soit par voie électronique pour faciliter la participation du plus grand nombre d'actionnaires.

Selon le nouveau cinquième alinéa de l'article R. 225-77 du Code de commerce : *« La signature, le cas échéant électronique, de l'actionnaire ou de son représentant légal ou judiciaire. Lorsque la société décide, conformément aux statuts, de permettre la participation des actionnaires aux assemblées générales par des moyens de communication électronique, cette signature électronique peut résulter d'un procédé fiable d'identification de l'actionnaire, garantissant son lien avec le formulaire de vote à distance auquel elle s'attache »*. Il en va de même au nouveau deuxième alinéa de l'article R. 225-79 du Code de commerce.

Ces modifications ont une incidence pratique importante sur la signature électronique. En effet, l'ancien décret n°2007-431 du 27 mars 2007 disposait : *« la signature électronique prend la forme soit d'une signature électronique sécurisée au sens du décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, soit, si les statuts le prévoient, d'un autre procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du Code civil »*. Désormais une signature électronique « simple » suffit (C. civ., art. 1316-4, al. 2, première phrase) sans que les sociétés anonymes n'aient à modifier leurs statuts. Il n'est plus nécessaire de disposer d'une signature électronique sécurisée bénéficiant de la présomption de fiabilité conformément à l'article 2 du décret n° 2001-272 du 30 mars 2001[87]. Ainsi, avec le nouveau décret, l'exigence de signature consistera à utiliser un procédé fiable d'identification de l'actionnaire, garantissant son lien (logique) avec un certificat électronique d'identification.

L'article R. 225-63 du Code de commerce dispose que *« Les sociétés qui entendent recourir à la communication électronique en lieu et place d'un envoi postal pour satisfaire aux formalités prévues aux articles R. 225-67, R. 225-68, R. 225-72, R. 225-74, R. 225-88 et R. 236-3 soumettent une proposition en ce sens aux actionnaires inscrits au nominatif, soit par voie postale, soit par voie électronique. Les actionnaires intéressés peuvent donner leur accord par voie postale ou électronique.*

En l'absence d'accord de l'actionnaire, au plus tard trente cinq jours avant la date de la

86. Voir notamment le Guide du vote électronique, Collection Guides de la Confiance, disponible depuis mai 2009 sur le site www.fntc.org.
87. JO du 31 mars 2001, p. 2553. V. Éric A. Caprioli, Commentaire du décret n°2001-272 du 30 mars 2001 relatif à la signature électronique : Rev. Dr. bancaire et fin. 2001, p. 155 et s.

prochaine assemblée générale, la société a recours à un envoi postal pour satisfaire aux formalités prévues aux articles R. 225-67, R. 225-68, R. 225-72, R. 225-74, R. 225-88 et R. 236-3.
Les actionnaires qui ont consenti à l'utilisation de la voie électronique peuvent demander le retour à un envoi postal trente cinq jours au moins avant la date de l'insertion de l'avis de convocation mentionné à l'article R. 225-67, soit par voie postale, soit par voie électronique »[88].

La société doit créer un site exclusivement consacré à cette fin[89]. L'actionnaire qui souhaite voter par voie électronique doit donner son accord par voie postale ou par voie électronique en réponse à la proposition qui lui a été faite en ce sens par la société. Attention, en l'absence d'accord de l'actionnaire dans le délai de trente cinq jours avant la date de la prochaine AG, la société doit alors avoir recours à un envoi postal. Dans le cas contraire, la convocation à l'AG et un *« formulaire électronique de vote à distance »* lui sont alors envoyés. L'actionnaire doit retourner le formulaire **dûment signé** *« à la société jusqu'à 15 heures, heure de Paris, la veille de la réunion de l'assemblée générale »*[90]. En outre, *«Les actionnaires exerçant leur droit de vote en séance par voie électronique ne pourront accéder au site consacré à cet effet qu'après s'être identifiés au moyen d'un code fourni préalablement à la séance »*[91].

b) Le vote électronique au sein des ordres professionnels à travers l'exemple des avocats[92]

Le décret n°2002-1306 du 28 octobre 2002[93] instituant le vote à distance par voie électronique pour l'élection des membres du Conseil national des barreaux est venu modifier le décret n°91-1197 du 27 novembre 1991[94] organisant la profession d'avocat.

Ainsi, aux termes de l'article 28 alinéa 3 *« les électeurs peuvent voter à distance par voie électronique lorsque l'ordre dont ils relèvent a adopté les mesures techniques nécessaires. Dans cette hypothèse, quinze jours au moins avant la date du scrutin, l'ordre porte à la connaissance de ses membres disposant du droit de vote, les modalités pratiques du scrutin et leur adresse un code personnel et confidentiel ».*

c) Les élections de délégués du personnel et des membres du comité d'entreprise

La LCEN instaure à l'article 54 la possibilité de recourir au vote électronique pour les élections des délégués du personnel et des membres du comité d'entreprise. Cet article insère à la première phrase des articles L. 423-13 et L. 433-9 du Code du travail, devenus depuis les articles L. 2314-21 et L. 2324-19, traitant du vote par bulletin-papier, les mots

---

88. Nouvelle version de l'article R. 225-63 du code de commerce, modifié par le Décret n°2011-1473 du 9 novembre 2011 relatif aux formalités de communication en matière de droit des sociétés (JO du 10 novembre 2011 p. 18893).
89. Article R. 225-61 du Code de commerce.
90. Article R. 225-80 du Code de commerce.
91. Article R. 225-98 du Code de commerce.
92. Art. 9 et s. de l'Arrêté du 6 juin 2008 portant agrément des titres Ier, II, III et IV du règlement intérieur de l'ordre des experts-comptables, J.O du 17 juin 2008.
93. JO n°254 du 30 octobre 2002, p. 17994.
94. JO n°277 du 28 novembre 1991, p. 15502.

« ou par vote électronique, dans les conditions et selon les modalités définies par décret en Conseil d'Etat ». Notons ainsi que le décret n°2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise[95] insère un article R. 423-1-2 et un article R. 433-2-2 au Code du travail, devenus depuis les articles R. 2314-8 à R. 2314-21 et R. 2324-4 à R. 2324-17, qui prévoient les modalités d'organisation d'une élection par voie électronique et notamment :

- *la nécessité d'un accord d'entreprise ou d'un accord de groupe comportant un cahier des charges pour recourir à un vote électronique (possibilité de recours cumulatif entre voie électronique et voie papier) ;*
- *le recours éventuel à un prestataire externe ;*
- *la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges ;*
- *la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes ;*
- *le traitement par des systèmes informatiques distincts, dédiés et isolés des données relatives aux électeurs inscrits et à leur vote ;*
- *le scellement du système de vote électronique à l'ouverture et à la clôture du scrutin ;*
- *l'expertise préalable par un tiers du système de vote électronique ;*
- *l'archivage jusqu'au terme du délai de recours ou jusqu'à la décision juridictionnelle devenue définitive des fichiers supports comprenant les programmes sources et exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde.*

Un arrêté du Ministre chargé du travail, pris après avis de la CNIL, est venu préciser les dispositions pratiques de mise en œuvre du vote électronique[96].

7. La billetterie dématérialisée

L'article 104-IV de la loi de finances rectificative pour 2006 du 30 décembre 2004[97] a modifié la réglementation sur la billetterie, codifiée à l'article 290 quater du Code général des impôts, pour prendre en compte les nouveaux procédés technologiques employés par les professionnels du spectacle. Désormais, ces derniers peuvent utiliser une billetterie imprimée ou dématérialisée issue de caisses ou systèmes informatisés.

De plus, l'article 50 sexies B de l'annexe 4 du CGI énonce : *« Toute entrée sur les lieux où sont organisés des spectacles visés au I de l'article 290 quater du code général des impôts doit être constatée par la remise d'un billet extrait d'un carnet à souches ou d'un distributeur automatique ou, à défaut de remise d'un billet, être enregistrée et conservée dans un système informatisé, avant l'accès au lieu du spectacle.*
II. - Les exploitants de spectacles qui utilisent des systèmes de billetterie informatisée comportant ou non l'impression de billets doivent se conformer aux obligations prévues au cahier des charges annexé à l'arrêté du 8 mars 1993 modifié.
III. - L'entrée doit faire l'objet d'un contrôle manuel ou électronique. Lorsqu'un billet est imprimé, il doit rester entre les mains du spectateur. Si ce billet comporte deux parties, l'une reste entre les mains du spectateur et l'autre est retenue au contrôle.

---

95. JO du 27 avril 2007, p. 7492.
96. Arrêté du 25 avril 2007 pris en application du décret n°2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise, J.O du 27 avril 2007, p. 7494.
97. Loi n°2006-1771 du 30 décembre 2006 de finances rectificative pour 2006, J.O. du 31 décembre 2006, p. 20228 et s.

Chaque partie du billet, ainsi que la souche dans le cas d'utilisation de carnets, doit porter de façon apparente ou sous forme d'informations codées :
1° Le nom de l'exploitant ;
2° Le numéro d'ordre du billet ;
3° La catégorie de la place à laquelle celui-ci donne droit ;
4° Le prix global payé par le spectateur ou s'il y a lieu la mention de gratuité ;
5° Le nom du fabricant ou de l'importateur si l'exploitant a eu recours à des carnets ou à des fonds de billets préimprimés.
Si les billets comportent des mentions codées, le système doit permettre de restituer les informations en clair.
Les billets provenant d'un carnet à souches ou émis sur des fonds de billets préimprimés doivent être numérotés suivant une série ininterrompue et utilisés dans leur ordre numérique.
Les billets pris en abonnement ou en location doivent comporter, outre les mentions prévues ci-dessus, l'indication de la séance pour laquelle ils sont valables.
Les billets émis par le biais de systèmes informatisés doivent comporter un identifiant unique mémorisé dans le système informatisé.
Chaque billet ne peut être utilisé que pour la catégorie de places qui y est indiquée.
IV. - Les obligations concernant les mentions à porter sur les billets d'entrée dans les établissements de spectacles cinématographiques, la fourniture et l'utilisation de ces billets sont fixées par la réglementation de l'industrie cinématographique. ».

8. Le Contrat d'assurance

Les sociétés d'assurance sont présentes sur l'internet. Leurs sites étaient le plus souvent des vitrines ou permettaient simplement de préremplir un formulaire de souscription avant l'envoi postal du dossier contenant les documents justificatifs ainsi que le formulaire signé. Toutefois, certaines d'entre elles ont mis en place des services de souscription en ligne pour leurs contrats d'assurance automobile ou moto. Or, malgré l'aspect consensualiste du contrat d'assurance (qui ne nécessite pas un écrit en tant qu'exigence liée au formalisme juridique), les sociétés d'assurance doivent prendre la précaution de préconstituer les preuves de l'engagement des clients. Tel est l'apport de l'arrêt de la Cour de cassation du 27 mai 2008[98] :
Claude X avait souscrit un contrat d'assurance sur l'Internet pour garantir sa motocyclette. Huit jours après, il a un accident de la route et est accusé d'homicide involontaire. La société d'assurance a refusé de verser la moindre somme au motif que, lors de la souscription, il a été précisé à Claude X que le contrat ne serait valable que **si, dans un délai de trente jours suivant la souscription, il envoyait un relevé d'information du précédent assureur confirmant qu'il n'avait pas eu d'accident.** Or, Claude X ayant payé mais n'ayant pas fourni le document, l'assureur a annulé le contrat postérieurement à la date de l'accident. La Cour d'appel de Paris, dans un arrêt du 8 novembre 2007, avait néanmoins condamné l'assureur à payer *in solidum* avec l'assuré des dommages et intérêts pour les préjudices matériels et moraux subis par les membres de la famille du défunt. Ses motivations étaient les suivantes. Tout d'abord, l'absence d'envoi du document est justifiée par le fait que l'assuré vivait aux Etats-Unis et que le système d'assurance américain est différent du système français. L'assureur ne peut donc pas lui reprocher de ne pas avoir fourni un document qu'il était dans l'impossibilité matérielle d'obtenir. Ensuite, la déclaration faite lors de la souscription s'est avérée parfaitement exacte. Enfin, l'éventuelle annulation opérée

98. Disponible sur www.legifrance.gouv.fr, pourvoi n°07-88176. Voir note Eric A. Caprioli, Rev. Dr. banc. et Finan, Novembre Décembre 2008, n°183, p. 50 et s.

par l'assureur ne peut pas avoir d'effet rétroactif au jour de l'accident. A cette date, Claude X était donc assuré.

L'assureur s'est pourvu en cassation en arguant essentiellement du fait que Claude X n'avait opéré sur l'Internet qu'une demande d'assurance nécessitant une acceptation de l'assureur. Cette acceptation n'aurait pu avoir lieu qu'à la fin du délai de trente jours, dans l'hypothèse où le document demandé aurait été fourni. Sans acceptation, il n'y a pas de contrat, et donc pas de garantie au jour de l'accident. L'assureur a également mis en avant le fait que Claude X avait été mis au courant par courrier de l'annulation encourue en l'absence de fourniture du document dans le délai imparti, et précisé que ceci était une condition à la formation du contrat.

Dans son arrêt du 27 mai 2008, la Cour a rejeté le pourvoi en jugeant que, suite à la demande en ligne de Claude X d'être assuré immédiatement, il lui a été répondu que, *« sous réserve de l'exactitude de vos déclarations et dans un délai de trente jours de l'envoi d'un relevé d'informations confirmant vos déclarations et de l'encaissement de [la] prime, [il était] assuré à compter du jour de la demande »*. La Cour considère en effet, que *« la demande d'assurance a été acceptée le jour où elle a été formée »*. Il est également important de noter que le moyen selon lequel le contrat n'aurait pas été formé faute d'acceptation de l'assureur n'est pas fondé. En effet, puisque l'assureur *« n'a pas, avant toute défense au fond, soulevé d'exception fondée sur une cause de nullité ou sur une clause du contrat »*, le pourvoi ne pouvait qu'être rejeté.

La fiabilité de la procédure de souscription est donc nécessaire et les sociétés d'assurance réfléchissent aujourd'hui à l'ouverture de services de souscription en ligne pour leurs contrats, y compris pour des prestations plus engageantes comme les assurances portant sur la vie. Pour des raisons de sécurité juridique et technique, elles auront sans doute recours à des moyens et des prestations de signature électronique (comme des certificats à usage unique par exemple), fournis par des prestataires de services de certification électronique.

9. La gestion et l'archivage des courriers électroniques[99]

Les services de messagerie connaissent une croissance exponentielle au sein des entreprises (et des organisations) et les volumes des contenus échangés par voie électronique dépassent très largement ceux des flux papier. Ils correspondent à environ deux tiers des données transmises. Or, le plus souvent, les courriers électroniques sont mal gérés et mal archivés. Dans les grands groupes, plusieurs systèmes de messagerie peuvent être utilisés, ce qui complexifie leur gestion. Mais certains courriers électroniques doivent être archivés par l'entreprise car ils sont susceptibles de l'engager ou de constituer des éléments de preuve d'un engagement commercial.

La gestion et l'archivage des courriers électroniques doivent faire l'objet d'un traitement spécifique par l'élaboration d'une politique visant à les encadrer juridiquement en corrélation avec la charte informatique, le règlement intérieur et la Politique de sécurité de l'information de l'entreprise. Par exemple, lors d'un litige entre commerçants où la preuve est libre ou à l'occasion d'un litige avec un salarié où la preuve doit être collectée de façon loyale et licite,

99. La problématique a été l'objet de nombre d'études intégrant les dimensions juridiques et techniques. Citons par exemple le guide du Forum des Compétences « Vers une politique d'Archivage électronique des documents », avril 2009.

ces éléments de preuve, dès lors qu'ils sont organisés et accessibles, peuvent être très utiles pour éclairer le juge dans sa décision.

Une Politique de gestion et d'archivage des courriers électroniques[100] - différente de la Politique d'archivage des documents - pourra être mise en œuvre. Elle consistera à veiller au respect de la vie privée des salariés et à encadrer les exigences propres de l'entreprise (traçabilité des échanges internes et externes) conformément aux textes applicables.

10. Les jeux de hasard et d'argent en ligne

La loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne[101] a pour ambition, face au développement croissant d'un marché illégal de jeux et paris en ligne, de créer une offre légale sous le contrôle d'une autorité administrative indépendante nouvelle, à savoir l'ARJEL (Autorité de Régulation des Jeux en Ligne).

La régulation des jeux en ligne appelait une adaptation des obligations et règles de contrôle de l'activité. Ainsi, a-t-il été prévu un régime d'agrément préalable des opérateurs, permettant de vérifier auprès de ces derniers le respect de plusieurs objectifs, dont :

- la prévention de l'accoutumance ;
- la protection des publics vulnérables ;
- la lutte contre le blanchiment d'argent ;
- la garantie de la sincérité des compétitions sportives et des jeux.

Le décret n°2010-509 du 18 mai 2010 relatif aux obligations imposées aux opérateurs agréés de jeux ou de paris en ligne en vue du contrôle des données de jeux par l'Autorité de régulation des jeux en ligne[102] prévoit un certain nombre d'exigences techniques liées à la dématérialisation des jeux de hasard et d'argent. En outre, les opérateurs agréés doivent se doter d'un coffre-fort d'archivage, dont la conception est vérifiée par l'ANDSI (label de l'ANDSI : Certification de Sécurité de Premier Niveau des coffres forts électroniques). Dans ce coffre-fort doivent être stockées les données relatives à l'activité de jeu ou de pari, et dont le contenu ne peut être lu, modifié ou déchiffré que par les seuls agents de l'ARJEL. L'article 5 du décret précise également les données concernées par cette obligation de conservation et d'archivage (login, pseudo, adresse IP), dont la durée de conservation est fixée à cinq ans par l'article 8 du même décret. La traçabilité des opérations joue un rôle important dans le dispositif légal et règlementaire mis en place par l'Etat.

11. La dématérialisation des déclarations de créances

La loi n°2011-331 du 28 mars 2011 de modernisation des professions judiciaires ou juridiques et de certaines professions réglementées[103] modifie certaines dispositions du

100. Voir Eric A. Caprioli, Gestion et archivage des mails : une problématique juridique délicate, disponible sur le site www.journaldunet.com - Eric A. Caprioli, L'archivage électronique : de la dématérialisation à la politique d'archivage, l'omniprésence du droit, http://www.caprioli-avocats.com – E. Caprioli, L'archivage électronique, JCP Ed. G. n°38, 14 septembre 2009, n°251.
101. JO n°0110 du 13 mai 2010, p. 8881.
102. JO n°0114 du 19 mai 2010, p. 9223.
103. JO du 29 mars 2011.

Code de commerce (articles L. 814-2 et L. 814-13) relatives aux administrateurs judiciaires et aux mandataires judiciaires. Elles ont pour objectif d'introduire la dématérialisation des procédures collectives et posent le principe de la mise en place par le Conseil National des Administrateurs judiciaires et des Mandataires Judiciaires (CNAJMJ), et sous sa responsabilité, du *« portail électronique offrant des services de communication électronique sécurisée en lien avec l'activité des deux professions. Ce portail permet, dans des conditions fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, l'envoi et la réception d'actes de procédure par les administrateurs judiciaires, les mandataires judiciaires et les personnes désignées en application du deuxième alinéa de l'article L. 811-2 ou du premier alinéa du II de l'article L. 812-2. »* Le Conseil national rend compte de l'accomplissement de ces missions dans un rapport qu'il adresse chaque année au garde des sceaux, ministre de la justice. L'échéance de la mise en service est fixée au plus tard le 1er janvier 2014 ».

Plusieurs décrets doivent encore être publiés.

- 2 décrets d'application de l'article L. 814-13 C. Com. :
  - Un décret simple fixant la liste des actes de procédure envoyés ou reçus par les Administrateurs judiciaires, les Mandataires judiciaires et les personnes visées au 2ème alinéa de l'article L. 811-2 ou du 1er alinéa du II de l'article L. 812-2 qui peuvent être communiqués par voie électronique ;
  - Un décret en Conseil d'Etat pris après avis de la CNIL fixant les modalités d'utilisation du portail électronique par les Administrateurs judiciaires et les Mandataires judiciaires.
- Un décret d'application en Conseil d'état de l'article L. 814-2 C. Com sera pris après avis de la CNIL ; il fixera les conditions d'envoi et de réception des actes de procédures via le portail par les administrateurs et les mandataires judiciaires et les personnes visées au 2ème alinéa de l'article L. 811-2 ou du 1er alinéa du II de l'article L. 812-2.

Le portail permettra de centraliser les déclarations de créances effectuées par voie électronique en un lieu unique et sécurisé. Néanmoins, ces déclarations dématérialisées ne pourront être effectuées qu'à la condition que *« les tiers destinataires ou émetteurs des actes auront expressément demandé ou consenti qu'il soit procédé par cette voie. A cette fin, ils utilisent le portail mis à leur disposition par le conseil national en application de l'article L. 814-2 »*.

12. Dématérialisation des procédures judiciaires

Progressivement, les procédures tant civiles que pénales font l'intégration de dispositifs dématérialisés. Cette intégration s'est traduite par la dématérialisation progressive des échanges mais surtout par la consécration récente de la signature électronique[104].

Ainsi en matière pénale, l'arrêté du 21 juin 2011[105] est venu compléter le dispositif décliné par

104. E. Caprioli, Procédure pénale et signature numérique, Communication Commerce électronique n°10, Octobre 2010, comm. 103. Cet article fait le point sur toutes les procédures judiciaires en cours de dématérialisation.
105. Arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale, JO du 25 juin 2011.

le décret du 18 juin 2010[106] et la loi du 12 mai 2009[107]. L'article 801-1 du Code de procédure pénale créé par la loi du 12 mai 2009 dispose que *« Tous les actes mentionnés au présent code, qu'il s'agissent d'actes d'enquête ou d'instruction ou de décisions juridictionnelles, peuvent être revêtus d'une signature numérique ou électronique, selon des modalités qui sont précisées par décret en Conseil d'Etat »*. L'arrêté du 21 juin 2011 indique, à présent, les éléments techniques relatifs tant à la signature proprement dite (électronique ou numérique) qu'à l'archivage. Il impose notamment la conformité du procédé de signature électronique au référentiel général de sécurité[108].

Enfin, le décret n°2012-366[109] du 15 mars 2012 relatif à la signification des actes d'huissier de justice par voie électronique et aux notifications internationales encadre la faculté de signifier par voie électronique. Cette signification ne peut être effectuée qu'avec le consentement du destinataire et doit faire l'objet d'un avis électronique de réception indiquant l'heure et la date de celle-ci (horodatage). L'acte signifié doit porter mention de ce consentement et les originaux de l'acte doivent indiquer les dates et heures de l'avis de réception émis par le destinataire. Le destinataire qui consent à ce mode de signification doit envoyer une déclaration à la Chambre Nationale des Huissiers de justice. Toutefois l'application concrète de cette signification électronique nécessite encore la publication d'un arrêté par le garde des Sceaux définissant les garanties que devront présenter les procédés utilisés pour cette signification, arrêté attendu au plus tard pour le 1er septembre 2012.

E. Protection des données à caractère personnel

La réglementation sur la protection des données à caractère personnel a vocation à s'appliquer aux prestataires de services de certification électronique (PSCE). Ainsi, l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée (dite Loi « Informatique et Libertés »)[110], qui est une reprise de l'article 8 de la directive 1999/193/CE du Parlement européen et du Conseil du 13 décembre 1999[111], les vise expressément[112]. Le prestataire de services de certification électronique se définit comme *« toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique »*. Cet article impose aux PSCE de collecter les données à caractère personnel nécessaires à la délivrance et la conservation d'un certificat électronique directement auprès des personnes concernées. Il est précisé que les données ne peuvent être traitées *« que pour les fins en vue desquelles elles ont été recueillies »*,

---

106. Décret n°2010-671 du 18 juin 2010 relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale, JO du 20 juin 2010, texte n°4.

107. Loi n°2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, JO du 13 mai 2009 p.7920.

108. Article A. 53-2 à A. 53-4 du Code de procédure pénale créé par l'arrêté du 21 juin 2011.

109. JO du 17 mars 2012 p. 4899.

110. JO du 7 janvier 1978, p. 227. Selon l'article 33 : « Sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par les prestataires de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies. »

111. JOUE L. 13 du 19 janvier 2000, pp. 12-20.

112. Article 1-11 du décret 2001-272 du 30 mars 2001. Cet article est repris de l'article 2-11) de la directive 1999/193/CE : « les « prestataires de service de certification » sont : « toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques ».

c'est-à-dire la délivrance et la conservation des certificats liés aux signatures électroniques. Les PSCE sont astreints au respect des principes *« Informatique et Libertés »* lorsqu'ils ont la qualité de responsable de traitement. Dans ce contexte, outre le respect du principe de finalité, ils doivent également veiller à :

- conserver les données pour une durée limitée (durée liée à la validité du certificat, et, le cas échéant les délais de prescriptions applicables) ;
- accomplir les formalités obligatoires auprès de la CNIL ;
- assurer la sécurité et la confidentialité des données. A ce titre, aux termes de l'article 34 de la loi « Informatique et libertés », il est spécifiquement prévu que le *« responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »* ;
- garantir les droits « informatique et Libertés » (droit d'accès aux données traitées, droit d'opposition au traitement, droit de rectification/suppression des données) ;

Les manquements aux obligations prescrites sont passibles de sanctions pécuniaires de la CNIL ainsi que de sanctions pénales.

Par ailleurs, le PSCE peut agir en qualité de sous-traitant, c'est-à-dire que le traitement des données est mis en œuvre pour le compte et sous les instructions d'un responsable de traitement. Dans ce contexte, le PSCE doit se conformer aux prescriptions de l'article 33 de la loi « Informatique et Libertés » eu égard à la collecte des données et au respect de la finalité. La seule autre obligation qui leur incombe a trait à la sécurité et la confidentialité des données. En effet, selon l'article 35 de cette loi :

« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.
Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.
Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement ».

Un projet de Règlement européen va bientôt modifier la directive européenne de 1995 sur la protection des données personnelles.

II. LA DEMATERIALISATION DANS LA SPHERE PUBLIQUE

Avec le développement de l'administration électronique, la dématérialisation est une préoccupation de plus en plus forte dans la sphère publique. Elle constitue l'une des composantes du processus de modernisation de l'Etat. Les téléprocédures en sont une parfaite illustration. La dématérialisation est aujourd'hui devenue une réalité pour les administrations et les usagers. Si elle avait, en 2008, trouvé tout naturellement sa place dans le plan de développement de l'économie numérique « France numérique 2012 » d'Eric Besson[113], elle demeure, au sein du plan « France numérique 2012-2020 », parmi les 50 objectifs prioritaires[114].

A. L'ordonnance du 8 décembre 2005 et les décrets relatifs au Référentiel général d'interopérabilité (RGI) et au Référentiel général de sécurité (RGS)[115]

L'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives[116] précise le cadre juridique relatif aux échanges électroniques dans la sphère publique. Elle assure les fondations du développement de l'administration électronique, un des piliers de la réforme et de la modernisation de l'Etat.

L'ordonnance s'applique aux autorités administratives définies à l'article 1-I comme *« les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351- 21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif ».*

Dans un souci de simplification des relations entre administrations et usagers, l'ordonnance du 8 décembre 2005 a adopté plusieurs mesures :

• Tout usager peut adresser une demande, une déclaration ou produire des documents par voie électronique. Sauf dérogation[117], l'administration, qui doit avoir accusé réception de la demande ou de l'information de l'usager (si l'accusé de réception n'est pas instantané, elle doit émettre un « accusé d'enregistrement »)[118], est alors régulièrement saisie et doit traiter la demande sans exiger de l'usager une confirmation ou la répétition de son envoi sous une autre forme. De même, tout paiement opéré dans le cadre d'un téléservice peut être

113. V. tout particulièrement les actions 120 à 127 de ce plan qui est disponible à l'adresse : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//084000664/0000.pdf.
114. V. le bilan du plan « France numérique 2012 » à l'adresse suivante : http://www.economie.gouv.fr/france-numerique-2012-2020-bilan-et-perspectives
V. les actions 35 à 27 du plan « France numérique 2012-2020 » disponible à l'adresse suivante : http://www.economie.gouv.fr/files/files/import/2011_france_numerique_consultation/2011_francenumerique2020objectifs.pdf.
115. La version en cours du RGS a été mise en ligne à la suite de la publication de l'arrêté RGS du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, JO n°0113 du 18 mai 2010, p.9152 (V. 1.0). Elle est disponible à l'adresse : http://www.references.modernisation.gouv.fr/rgs-securite.
116. JO n° 286 du 9 décembre 2005, p. 18896 et s.
117. L'article 3 de l'ordonnance prévoit en effet qu'un décret doit fixer les cas dans lesquels, en raison d'exigences particulières de forme ou de procédure, il peut y avoir dérogation à cette règle.
118. Article 3 et article 5-1 de l'ordonnance du 8 décembre 2005.

effectué en ligne et doit faire l'objet d'un accusé de réception et, le cas échéant, d'un accusé d'enregistrement. Il est à noter que l'accusé de réception ou d'enregistrement doit être émis selon un procédé conforme aux règles fixées par le RGS et que la non transmission de l'accusé de réception ou son caractère incomplet rendent en principe inopposables les délais de recours à l'auteur de la demande. Par ailleurs, un décret qui n'a toujours pas été adopté à ce jour, doit préciser les conditions et les délais d'émission de ces accusés ainsi que les indications devant y figurer.

• La création d'un service public chargé de mettre à disposition de l'usager un espace de stockage accessible en ligne (un coffre-fort numérique) permettant à ce dernier de conserver ses informations et documents pour leur communication aux autorités administratives dans le cadre de l'accomplissement de ses démarches est prévue. Cet espace, placé sous son contrôle exclusif, est ouvert et clos à sa demande et peut même devenir un véritable espace d'échanges avec les administrations. Sur son autorisation, elles pourront y déposer des documents ou obtenir transmission d'informations ou de documents dont elles ont à connaître, étant noté qu'un décret[119] et un arrêté du 18 juin 2009[120] sont venus préciser les modalités de mise en œuvre et d'exploitation de ce service appelé « mon.service-public.fr ».

• Toute autorité administrative peut créer des téléservices dont elle doit fixer le niveau de sécurité et à condition de respecter les dispositions de la loi du 6 janvier 1978[121] ainsi que les règles de sécurité et d'interopérabilité fixées dans le RGS[122] et le RGI[123]. La décision de création du téléservice et ses modalités d'utilisation doivent être accessibles depuis ce service et s'imposent aux usagers.

A cet égard, le RGI fixe un ensemble de règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des systèmes d'information du service public, pour assurer la simplicité d'intégration de nouveaux systèmes et pour faciliter l'évolution du système global ainsi que son utilisation par tous les acteurs.

Le RGS, quant à lui, détermine les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives (notamment les fonctions d'authentification, de signature électronique, de confidentialité

119. Décret n°2009-730 du 18 juin 2009 relatif à l'espace de stockage accessible en ligne pris en application de l'article 7 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, J.O. du 20 juin 2009, p.10111.

120. Arrêté du 18 juin 2009 portant création par la direction générale de la modernisation de l'Etat d'un téléservice dénommé « mon.service-public.fr », J.O. du 20 juin 2009, p.10112.

121. Loi n°78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; J.O du 7 janvier 1978 et rectificatif au JO du 25 janvier 1978, modifiée par la loi du 4 août 2004. Egal. Décret du 20 octobre 2005 et décret du 25 mars 2007.

122. Décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, J.O. du 4 février 2010, p. 2072 ; Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, JO n°0113 du 18 mai 2010, p.9152.

123. Décret n°2007-284 du 2 mars 2007 fixant les modalités d'élaboration, d'approbation, de modification et de publication du référentiel général d'interopérabilité, JO n°53 du 3 mars 2007, p. 4060 ; Arrêté du 9 novembre 2009 portant approbation du référentiel général d'interopérabilité, JO n°0262 du 11 novembre 2009, p.19593.

et d'horodatage). Des niveaux de sécurité sont proposés aux autorités administratives afin qu'elles déterminent pour leurs téléservices le niveau adapté en fonction de la sensibilité des opérations.

Par ailleurs, l'ordonnance prévoit que les actes des autorités administratives pourront désormais faire l'objet d'une signature électronique[124]. A cet égard, l'article 8 de l'ordonnance précise que la signature *« n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte »*. On peut remarquer que cette définition reprend les mêmes fonctions que la signature prévue par le Code civil pour les actes juridiques en droit privé.

Avec l'adoption de l'arrêté relatif au RGS, l'ordonnance est donc pleinement applicable et constitue désormais la référence en matière d'échanges électroniques dans la sphère publique.

B. Procédure de vérification des informations d'état civil

Le décret du 10 février 2011[125], en modifiant le décret du 3 août 1962[126], a institué une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'état civil. Il n'est pas rare que les usagés soient obligés de produire, à l'appui de leurs démarches administratives, des actes d'état civil. Ce décret permet d'organiser une nouvelle procédure permettant aux administrations et organismes légalement fondés à requérir des actes de l'état civil de demander directement, notamment par voie électronique[127], auprès des officiers de l'état civil dépositaires des actes, la vérification des données déclarées par les usagers. L'arrêté du 23 décembre 2011[128] est venu préciser les éléments techniques relatifs à la mise en œuvre de cette vérification et notamment les éléments relatifs à la plate-forme de routage COMEDEC[129] ainsi que les éléments relatifs au dispositif sécurisé de création de la signature électronique fourni aux collectivités locales[130], l'ensemble de ces éléments devant être conforme au RGS[131].

---

124. E. A. Caprioli, Des échanges électroniques entre les usagers et les autorités administratives d'une part, et entre ces dernières d'autre part, JCP éd. A et CT, 2006, n°1079, p. 432 et s.
125. Décret n°2011-167 du 10 février 2011 instituant une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'état civil, JO du 12 février 2011.
126. Décret n°62-921 du 3 août 1962 modifiant certaines règles relatives aux actes de l'état civil, JO du 9 août 1962 page 7918.
127. Article 13-5 du décret n°62-921 du 3 août 1962 modifiant certaines règles relatives aux actes de l'état civil.
128. Arrêté du 23 décembre 2011 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil, JO du 29 décembre 2011.
129. V. Article 2 à 8 de l'arrêté du 23 décembre 2011 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil.
130. V. article 9 à 13 de l'arrêté du 23 décembre 2011 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil.
131. V. article 5, 10 et 11 de l'arrêté du 23 décembre 2011 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil.

TÉLÉPROCÉDURES	DESCRIPTIF DE LA TÉLÉPROCÉDURE
Télé TVA	- Elle permet l'envoi et le règlement des déclarations de la TVA par voie électronique. - Elle est obligatoire pour l'entreprise, sous peine de pénalités, si son chiffre d'affaire est supérieur à 760 000 euros. - Elle est accessible à toutes les entreprises assujetties à la TVA du régime réel. - Elle est obligatoire pour l'entreprise, sous peine de pénalités, si son chiffre d'affaire est supérieur à 500 000 euros - Elle est obligatoire pour l'entreprise, sous peine de pénalités, si son chiffre d'affaire est supérieur à 230 000 euros - Elle sera obligatoire pour l'entreprise, sous peine de pénalités, si son chiffre d'affaire est supérieur à 230 000 euros ou si elle est soumise à l'impôt sur les sociétés, quel que soit le montant de son chiffre d'affaires - Elle sera obligatoire pour l'entreprise, sous peine de pénalité, si son chiffre d'affaire est supérieur à 80 000 euros ou si elle est soumise à l'impôt sur les sociétés, quel que soit le montant de son chiffre d'affaires - Elle sera obligatoire pour toute entreprise - Deux modes de transmission : > soit directement sur internet (mode EFI) > soit par l'intermédiaire d'un comptable ou d'un autre prestataire (mode EDI)
Site du Système d'Immatriculation des Véhicules (SIV)[5]	Cette téléprocédure permet pour les professionnels : - la réalisation de certaines opérations relatives à l'immatriculation des véhicules (ex : déclaration d'achat). - les déclarations de prise en charge et de destruction pour les véhicules hors d'usage. Pour les particuliers, elle permet : - de demander des certificats de situation, - d'effectuer une pré-demande de changement de titulaire de carte grise, - de suivre où en est sa demande de carte grise.
Téléprocédure[6] URSSAF	• Elle permet aux entreprises, aux établissements du secteur public et aux professions libérales la déclaration et éventuellement le paiement de leurs cotisations sociales. • Les entreprises redevables de plus de 7 millions d'euros doivent obligatoirement, sous peine de pénalités, payer leurs cotisations par virement. • Obligation de dématérialiser les déclarations sociales, sous peine de pénalités : Pour les entreprises redevables de plus de 800 000 euros ; Pour les entreprises redevables de plus de 400 000 euros ; Pour les entreprises redevables de plus de 150 000 euros.
TéléIR	Elle permet aux particuliers de déclarer leurs impôts sur le revenu en ligne. Un accusé de réception numéroté et horodaté est adressé lors du « dépôt en ligne ». L'authentification de l'usager s'effectue lors de sa première connexion à partir des éléments d'identification : n° du télédéclarant, n° fiscal personnel, revenu fiscal de référence.

1. Article 53 I C de la loi n°2011-1978 du 28 décembre 2011 de finances rectificative pour 2011 (1), JO du 29 décembre 2011 p. 22510.
2. JO n°37 du 13 février 1994, p. 2493.
3. Article R.123-121-4 alinéas 2 du Code du commerce : « Le dépôt des documents comptables peut être effectué par voie électronique dans les conditions prévues à l'article 4 de la loi n°94-126 du 11 février 1994 ».
4. Décret n°2010-1706 du 29 décembre 2010 relatif à l'entrepreneur individuel à responsabilité limitée, JO du 31 décembre 2010 p. 23450.
5. V. http://www.ants.interieur.gouv.fr/siv/-immatriculation-.html.
6. V. le site des URSSAF : http://www.urssaf.fr.
7. JO n°0295 du 21 décembre 2010, p. 22409.
8. JO du 13 novembre 2001 p. 18024.
9. JO n°13 du 16 janvier 2007.
10. JO n°80 du 4 avril 2008.

DATE DE MISE EN VIGUEUR	TEXTES LÉGISLATIFS APPLICABLES	TEXTES RÉGLEMENTAIRES APPLICABLES
- depuis le 1er mai 2001 - depuis le 1er janvier 2007 - depuis le 1er octobre 2010 - depuis le 1er octobre 2011 - à partir du 1er octobre 2012[1] - à partir du 1er octobre 2013 - à partir du 1er octobre 2014	• L'article 4 de la loi n°94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle[2] fixe un cadre général à la transmission électronique des déclarations aux administrations par les entreprises. • L'article 123-121-4 du Code du commerce[3], créé par le décret du 29 décembre 2010[4]. • Articles 1649 quater B bis et s., 1695 quater B quarter et 1738 du CGI. • Article 29 de la loi n°2009-1674 du 30 décembre 2009 de finances rectificative pour 2009	• La circulaire AFB n°97/193 du 7 mai 1997 décrit les spécifications et modalités de mise en œuvre des télérèglements de type A et B. • Le décret n° 2000-1036 du 23 octobre 2000 pris pour l'application des articles 1649 quater B bis et 1649 quater B quater du code général des impôts et relatif à la transmission des déclarations fiscales professionnelles par voie électronique : il autorise la transmission des déclarations professionnelles, de leurs annexes et de tout document les accompagnants par voie électronique à la DGI. • Instruction de la DGI du 11 septembre 2001 (BOI n° 171 du 25 septembre 2001) relative à la transmission par voie électronique des déclarations et des paiements de la TVA.
• depuis 2003 • depuis juillet 2006		
• depuis le 1er janvier 2007 • depuis le 1er janvier 2007 • depuis le 1er juillet 2007 • depuis le 1er janvier 2008 • depuis le 1er janvier 2009	• Article L. 243-14 du Code de la sécurité sociale modifié par loi n°2010-1594 du 20 décembre 2010 de financement de la sécurité sociale pour 2011[7] du Code de la sécurité sociale.	Articles R. 243-13 et R. 243-17 du Code de la sécurité sociale.
Depuis le 11 mars 2002, la Direction Générale des Impôts a mis à disposition des internautes un portail dédié à la télé-déclaration des impôts sur le revenu.		• L'arrêté du 12 novembre 2001 portant création d'un service à compétence nationale dénommé « programme Copernic » chargé de la mise en place du système d'information relatif au compte fiscal simplifié[8] (TéléIR s'inscrit dans ce programme). • L'arrêté du 22 décembre 2006 modifiant l'arrêté du 12 novembre 2001 portant création d'un service à compétence nationale dénommé « programme COPERNIC » chargé de la mise en place du système d'information relatif au compte fiscal simplifié.[9] • Arrêté du 3 avril 2008 modifiant l'arrêté du 12 novembre 2001 modifié portant création d'un service à compétence nationale dénommé « programme COPERNIC » chargé de la mise en place du système d'information relatif au compte fiscal simplifié.[10]

C. Les téléprocédures

L'ordonnance du 8 décembre 2005 et l'adoption du RGI et du RGS devraient faciliter la création de nouvelles téléprocédures, qui permettent, tant aux autorités administratives qu'aux usagers, un gain de temps et qui simplifient les démarches administratives. Il est à noter que, dans la mise en place de ces téléprocédures, les administrations devront, en tout état de cause, assurer l'accessibilité des sites à tous les citoyens, y compris les personnes handicapées. A cet égard, dans un souci d'harmonisation des différents sites publics et conformément à l'article 47 de la loi n°2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées[132], un référentiel général d'accessibilité pour les administrations (RGAA) a été publié en octobre 2009[133]. De la même manière, et dans le cadre de l'action 125 du plan numérique 2012, une charte ergonomique a été validée dans sa version 2.0 le 19 décembre 2008[134], charte dont l'objet consiste à définir un ensemble de règles ergonomiques communes aux interfaces des sites Internet publics. Toutefois, l'Etat n'a pas attendu ladite ordonnance de 2005 pour mettre en place certaines téléprocédures. Le tableau ci-dessus présente, de façon non exhaustive, quatre exemples de téléprocédures existantes : TéléTVA, le site du Système d'immatriculation des véhicules (SIV), la téléprocédure URSSAF et TéléIR.

D. Les marchés publics passés par voie électronique

Le Code des marchés publics du 1er août 2006[135] a transposé les directives dites « Marchés publics » de 2004[136]. Si le principe de la dématérialisation des marchés publics a été introduit dès le Code de 2001, à la différence du Code de 2001 et de celui de 2004, la dématérialisation et les procédures y afférentes sont dorénavant traitées dans le corps du texte réglementaire et non plus dans le seul article 56. Quelques modifications ont déjà été apportées à cette dernière version du Code des marchés publics par le décret du 17 décembre 2008[137] ainsi que le décret du 26 août 2011[138]. L'article 56, largement modifié par le décret du 17 décembre 2008, continue toutefois à traiter des communications et des échanges d'informations par voie électronique mais c'est surtout un arrêté du 14 décembre

---

132. JO du 12 février 2005, p. 2353 et s.

133. Décret n°2009-546 du 14 mai 2009 pris en application de l'article 47 de la loi n°2005-102 du 11 février 2005 sur l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées et créant un référentiel d'accessibilité des services de communication publique en ligne et arrêté du 21 octobre 2009 relatif au référentiel général d'accessibilité pour les administrations, JO du 29 octobre 2009, p. 18329.

134. Voir sur le site http://www.references.modernisation.gouv.fr/.

135. Décret n°2006-975 du 1er août 2006 portant code des marchés publics ; JO n°179 du 4 août 2006 p. 11627, texte n°20.

136. Directive 2004/17/CE du Parlement européen et du Conseil du 31 mars 2004 portant coordination des procédures de passation des marchés dans les secteurs de l'eau, de l'énergie, des transports et des services postaux (JOUE L 134 du 30/04/2004, p. 1 et s.) et directive 2004/18/CE du Parlement européen et du Conseil du 31 mars 2004 relative à la coordination des procédures de passation des marchés publics de travaux, de fournitures et de services (JOUE L 134 du 30/04/2004, p. 114 et s.).

137. Décret n°2008-1334 du 17 décembre 2008 modifiant diverses dispositions régissant les marchés soumis au code des marchés publics et aux décrets pris pour l'application de l'ordonnance n° 2005-649 du 6 juin 2005 relative aux marchés passés par certaines personnes publiques ou privées non soumises au code des marchés publics, JO du 18 décembre 2008, p. 19367 et s.

138. Décret n°2011-1000 du 25 août 2011 modifiant certaines dispositions applicables aux marchés et contrats relevant de la commande publique, JORF du 26 août 2011.

2009[139] abrogeant en grande partie celui du 28 août 2006[140] (sauf pour les dispositions relatives à la signature électronique), qui donne des précisions sur les conditions et les modalités de mise en œuvre de la dématérialisation.

Les principaux éléments concernant la dématérialisation des marchés publics sont les suivants[141] :

• Généralités concernant les marchés publics électroniques :

> Dans toutes les procédures de passation des marchés publics, les écrits peuvent être remplacés par un échange électronique mais également par la production de supports physiques électroniques[142]. Par ailleurs, il est prévu la possibilité pour les candidats d'envoyer une copie de sauvegarde de leur candidature et de leur offre dans les conditions fixées par l'arrêté du 14 décembre 2009 (il est à noter que contrairement à l'arrêté du 28 août 2006, celui-ci est applicable à l'ensemble des procédures de passation des marchés publics et non pas seulement aux procédures formalisées). Cette copie de sauvegarde, qui doit nécessairement être envoyée dans les délais impartis pour la remise des candidatures et des offres[143], peut être sur support physique électronique ou sur support papier. Elle ne pourra être ouverte par la personne publique que dans deux cas expressément prévus à l'article 7 de l'arrêté :
- Lorsqu'un programme informatique malveillant (virus ou autres vers) a été détecté par la personne publique dans la candidature ou l'offre du soumissionnaire transmise par voie électronique ;
- ou lorsque la candidature ou l'offre transmise par voie électronique n'est pas parvenue à temps au pouvoir adjudicateur ou qu'elle n'a pas pu être ouverte par ce dernier.
Il est à noter que la cour administrative d'appel de Bordeaux a précisé que cette copie de sauvegarde ne peut être utilisée pour régulariser une offre irrégulière[144].

> Que la transmission électronique des offres soit obligatoire ou facultative, il est fait obligation au pouvoir adjudicateur d'assurer la confidentialité et la sécurité des transactions sur un réseau informatique qui doit être accessible à tous les candidats de façon non discriminatoire, selon des modalités fixées par arrêté. Il est précisé, toutefois, que dans les marchés passés selon une procédure adaptée, ces modalités tiennent compte des caractéristiques du marché, notamment de la nature et du montant des travaux, fournitures ou services en cause. Les frais d'accès au réseau sont, en revanche, à la charge des candidats[145].

> L'arrêté du 14 décembre 2009 prévoit en outre que le dépôt des candidatures et des offres

---

139. Arrêté du 14 décembre 2009 relatif à la dématérialisation des procédures de passation des marchés publics, JO n°295 du 20 décembre 2009, p. 22028.
140. Arrêté du 28 août 2006 pris en application du I de l'article 48 et de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics formalisés, JO n°199 du 29 août 2006, p. 12766 et s.
141. Pour plus d'information se reporter au guide pratique relatif à la dématérialisation des marchés publics publié en 2010 par la Direction des affaires juridiques du Ministère de l'économie, de l'industrie et de l'emploi : http://www2.economie.gouv.fr/directions_services/daj/marches_publics/conseil_acheteurs/guides/guide-pratique-dematerialisation-mp.pdf.
142. Article 56-I alinéa 1 du Code des marchés publics.
143. Article 56-V du Code des marchés publics et article 6 de l'arrêté du 14 décembre 2009.
144. CAA Bordeaux, 31 mars 2011, n°10BX01752.
145. Article 56-IV du Code des marchés publics.

transmises par voie électronique ou même sur support physique électronique doit donner lieu à un accusé de réception indiquant la date et l'heure de réception[146].

> Enfin, pour les appels d'offres ouverts ou les concours ouverts, le même arrêté prévoit les modalités de destruction des offres sous forme électronique ou sur support physique électronique ainsi que des copies de sauvegarde, dès lors que la candidature a été rejetée[147].

• Dispositions relatives à l'organisation de la publicité et à l'information des candidats :

> Le Code des marchés publics de 2006 modifié a introduit quelques innovations comme, par exemple, la publication de l'avis de pré-information sur le *« profil d'acheteur du pouvoir adjudicateur »*[148]. La circulaire du 14 février 2012 relative au Guide de bonnes pratiques en matière de marchés publics[149] précise qu'il s'agit *« d'un site, généralement une « plate-forme », accessible en ligne, par l'intermédiaire du réseau internet, offrant toutes les fonctionnalités nécessaires à la dématérialisation des procédures. Il doit permettre, au minimum, de mettre en ligne les avis de publicité et les DCE, de recevoir des candidatures et des offres électroniques de manière sécurisée et confidentielle et de gérer les échanges d'information entre le pouvoir adjudicateur et les opérateurs économiques pendant la procédure de passation de marché. Le site internet d'une collectivité ne peut tenir lieu de profil d'acheteur que s'il offre l'accès à ces fonctionnalités. »*[150].

> Il prévoit également une réduction des délais de réception des candidatures et des offres en cas d'envoi électronique de l'avis d'appel public à la concurrence et de mise à disposition des documents de la consultation par voie électronique.

> Il est fait désormais obligation au pouvoir adjudicateur, depuis le 1er janvier 2010 et pour les marchés publics d'un montant supérieur à 90 000 H.T. :
- de publier l'avis de publicité sur son profil d'acheteur[151] ;
- de publier les documents de la consultation sur son profil d'acheteur[152], selon des modalités fixées par l'arrêté ministériel du 14 décembre 2009. Ces documents doivent ainsi *« être d'accès libre, direct et complet »* et l'adresse de téléchargement de ces documents doit figurer dans l'avis d'appel public à la concurrence s'il existe[153].

On notera que la simple mise à disposition ne dispense pas l'acheteur public de ses obligations en matière d'information. En cas de modification du marché en cours de procédure, l'acheteur public ne peut se contenter de mettre à disposition les documents modifiés, il est tenu d'en informer l'ensemble des candidats. Ainsi, les tribunaux ont pu sanctionner un acheteur public pour manquement à ses obligations de publicité et de mise en concurrence pour ne pas s'être assuré de l'information d'un candidat sur l'introduction d'un additif aux documents de la consultation[154]. En l'espèce, le candidat avait été prévenu

146. V. l'article 5 de l'arrêté du 14 décembre 2009.
147. V. l'article 8 de l'arrêté du 14 décembre 2009.
148. V. l'article 39-I du Code des marchés publics.
149. JO du 15 février 2012 page 2600.
150. V. l'article 10.2.1.2. La publication obligatoire sur le profil d'acheteur de la circulaire du 14 février 2012 relative au Guide de bonnes pratiques en matière de marchés publics.
151. Articles 40-III, 40-IV et 150-III, 150-IV du Code des marchés publics.
152. Article 41 alinéa 3 du Code des marchés publics.
153. V. l'article 1 de l'arrêté du 14 décembre 2009.
154. Ord. Ref. TA Toulouse, du 29 mars 2010, n°1001105.

par courriel mais les tribunaux ont estimé que ledit courriel ne présentait aucun élément de nature à attirer l'attention de son destinataire. Cette vision rigoureuse n'est cependant pas unanime, d'autres juridictions ayant statué que l'obligation d'information avait été remplie par l'émission d'un courrier électronique[155]. Il revient donc à l'acheteur public de veiller à la transmission effective des informations relatives au marché.

> Suite au rejet d'une candidature à un appel d'offres ouvert ou à un concours ouvert, la personne publique doit informer le candidat de la destruction de son offre transmise sous forme électronique[156].

• **Mode de transmission des candidatures et des offres :**

> Le pouvoir adjudicateur doit indiquer dans l'avis d'appel public à la concurrence, ou dans la lettre de consultation pour les marchés négociés sans publicité préalable, le mode de transmission qu'il retient pour les candidatures et les offres[157] ; étant noté que jusqu'au 1er janvier 2010, les candidats à un marché passé selon une procédure formalisée pouvaient opter, sauf exceptions, pour un autre mode de transmission que celui prescrit par la personne publique[158].

> Les candidats doivent, en revanche, s'en tenir au même mode de transmission pour l'ensemble des documents (candidature et offre) qu'ils adressent à la personne publique[159], sans préjudice des dispositions applicables à la copie de sauvegarde.

> Depuis le 1er janvier 2010, les acheteurs publics peuvent imposer la transmission par voie électronique des documents mentionnés au premier alinéa du I de l'article 56, y compris les candidatures et les offres[160]. De plus, cette transmission par voie électronique s'impose aux candidats pour les marchés relatifs à des achats de fournitures de matériels informatiques et de services informatiques d'un montant supérieur à 90 000 euros H.T.

> Enfin, depuis le 1er janvier 2012, les acheteurs publics ne peuvent plus refuser les candidatures et les offres des candidats transmises par voie électronique pour les marchés de fournitures, de services ou de travaux d'un montant supérieur à 90 000 euros H.T.

• **Présentation des candidatures et des offres :**

> L'article 48 alinéa 3 du Code des marchés publics, modifié par le décret du 26 août 2011, indique que le candidat doit transmettre son offre en une seule fois, sans préjudice des dispositions relatives à la copie de sauvegarde, et que seule la dernière offre reçue dans les délais par l'acheteur public sera prise en compte.

155. Ord. Ref. TA Poitiers, du 3 janvier 2012, n°112784.
156. V. l'article 8-I de l'arrêté du 14 décembre 2009.
157. Article 56-I alinéa 2 du Code des marchés publics.
158. Article 56-I alinéa 4 du Code des marchés publics dans sa rédaction issue du décret n°2008-1334 du 17 décembre 2008.
159. Article 56-I alinéa 3 du Code des marchés publics.
160. Article 56-II-1° du Code des marchés publics dans sa rédaction issue du décret n°2008-1334 du 17 décembre 2008.

• **Signature électronique de l'acte d'engagement :**

> La signature électronique de l'acte d'engagement[161] est maintenue. L'article 48 alinéa 2 du Code des marchés publics précise désormais que l'acte d'engagement pour un marché ou un accord-cadre passé selon une procédure formalisée, lorsque l'offre est transmise par voie électronique, est signé électroniquement dans des conditions fixées par arrêté du ministre chargé de l'économie[162]. On notera qu'il en est de même pour la candidature[163]. En cas de groupement, l'acte d'engagement doit être signé, soit par l'ensemble des entreprises membres du groupement, soit par le mandataire du groupement dûment habilité pour représenter ces entreprises[164]. La jurisprudence a précisé, à cet égard, que les documents contenus dans un fichier « zip » doivent être signés individuellement et que la seule signature du fichier « zip » n'est pas suffisante, dans la mesure où *« le fichier zip doit être considéré comme un acte distinct des documents qu'il contient »*[165]. Les articles 5 à 7 de l'arrêté du 28 août 2006, toujours en vigueur en attendant l'adoption d'un nouvel arrêté suite à la publication du RGS[166], en donnent des précisions. Outre le visa de l'arrêté faisant référence aux articles 1316 à 1316-4 du Code civil, l'article 6 dudit texte prévoit que les catégories de certificats de signatures utilisables doivent non seulement être conformes au RGS mais également être référencées sur une liste établie par le ministre chargé de la réforme de l'Etat[167].

Outre la dématérialisation des procédures « classiques » de passation des marchés publics, le Code des marchés publics de 2006 a :

• d'une part, maintenu la possibilité pour la personne publique d'organiser des enchères électroniques mais uniquement pour les marchés de fournitures formalisés[168].

• d'autre part, prévu une nouvelle procédure[169] entièrement électronique limitée aux achats de fournitures courantes et dans le temps (durée maximale de quatre ans) : le système d'acquisition dynamique[170]. Les opérateurs sont d'abord pré-sélectionnés sur la base d'une offre indicative conforme au cahier des charges, puis le pouvoir adjudicateur attribue, après mise en concurrence, un ou plusieurs marchés à l'un des opérateurs.

La dernière réforme du Code des marchés publics confirme l'objectif affiché en 2006 de favoriser la dématérialisation des marchés publics et même de l'imposer en grande

161. Article 48-I du Code des marchés publics.
162. A l'heure actuelle, la consultation au sujet de cet arrêté est terminée.
163. Article 44-II du Code des marchés publics.
164. Article 51-IV alinéa 2 du Code des marchés publics.
165. Ord. Réf., TA de Toulouse, n°1100792, 9 mars 2011, Société MC²I c/ CNRS. Pour un commentaire de cette ordonnance, v. Marché public en ligne. Signer électroniquement un fichier zip ne revient pas à signer son contenu, Eric A. Caprioli et Noëlle Jean-Pierre, Expertises des systèmes d'information, Mai 2011, p.189-190.
166. En effet, une fiche explicative relative à l'arrêté du 14 décembre 2009 précise : « Un arrêté spécifique viendra ultérieurement préciser les règles applicables à la signature électronique compte tenu du référentiel général de sécurité qui doit être adopté en application de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques.».
167. Liste publiée à l'adresse suivante : http://www.entreprises.minefi.gouv.fr/certificats/.
168. Cette procédure est détaillée dans un seul article du Code : l'article 54.
169. Transposition de l'article 33 de la directive 2004/18/CE du Parlement européen et du Conseil du 31 mars 2004 relative à la coordination des procédures de passation des marchés publics de travaux, de fournitures et de services (JOUE L 134 du 30/04/2004, p. 114 et s.).
170. Article 78 du Code des marchés publics.

partie depuis le 1er janvier 2010. D'un point de vue plus pragmatique, il faut dire que la dématérialisation permet, d'une part, la réalisation d'économies par la baisse des dépenses liées à la transmission et à l'élaboration des documents sur support papier, ainsi que par la diminution des coûts de transactions. D'autre part, elle est un gain de temps dans la préparation du dossier, les formulaires étant remplis et envoyés par courrier électronique. Enfin, la dématérialisation est un facteur de concurrence. Elle permet d'étendre plus largement l'accès à la commande publique aux entreprises. Elle assure ainsi une meilleure égalité de traitement des candidats, les petites entreprises ayant dorénavant un accès plus facile aux offres de marchés publics[171]. Le retour des expérimentations qui sont maintenant achevées dans ce domaine sera donc très intéressant et permettra de déterminer si cette mouture du Code des marchés publics connaîtra le succès escompté en matière de dématérialisation.

Pour terminer, il est important de signaler une communication récente de la Commission européenne qui propose de faire de la passation électronique des marchés publics la règle plutôt que l'exception : **les marchés publics par voie électronique deviendront la méthode standard dans toute l'UE en 2016**[172].

E. Consultation préalable à un acte réglementaire

L'article 16 de la loi du 17 mai 2011[173] de simplification et d'amélioration de la qualité du droit a introduit, pour une autorité administrative tenue de procéder à la consultation d'une commission consultative préalablement à l'édiction d'un acte réglementaire, la possibilité d'organiser une consultation ouverte permettant de recueillir, sur un site internet, les observations des personnes concernées. Le décret du 8 décembre 2011 relatif aux consultations ouvertes sur l'internet[174] est venu fixer les contours de cette consultation électronique. Il prévoit notamment que la publication de la consultation est assortie du projet d'acte concerné et d'une notice explicative précisant l'objet et le contenu de celui-ci ainsi que, le cas échéant, la ou les dates prévues pour l'entrée en vigueur des mesures envisagées[175]. Il prévoit également que la synthèse des observations recueillies dans le cadre de la consultation ouverte est rendue publique par l'autorité organisatrice au plus tard à la date de la signature de l'acte ayant fait l'objet de la consultation[176].

F. Les données de santé

La loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé[177] a consacré le droit des patients à disposer de la totalité de leur dossier médical. En réalité, le droit des malades consistera plutôt *« à accéder à l'ensemble des informations concernant leur santé »* détenues par des professionnels de santé et des établissements de santé et qui sont formalisées. Puis, la loi n°2004-810 du 13 août 2004 relative à l'assurance

171. E. Caprioli et A. Cantéro, L'entreprise face à la dématérialisation des marchés publics, La Semaine juridique, éd. E, éd. (LexisNexis), 3 novembre 2005, pp.1887-1891.
172. Comm. UE, communiqué IP/12/389, 20 avril 2012.
173. Loi n°2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, JO du 18 mai 2011 p. 8537.
174. Décret n°2011-1832 du 8 décembre 2011 relatif aux consultations ouvertes sur l'internet, JO du 9 décembre 2011 p. 20869.
175. article 2 du décret n°2011-1832 du 8 décembre 2011.
176. V. article 3 du décret n°2011-1832 du 8 décembre 2011
177. JO du 5 mars 2002, p. 4118, texte n° 1.

maladie[178] a instauré le dossier médical personnel (DMP) dont les dispositions ont été codifiées aux articles L. 1111-14 et s. du Code de la santé publique. Ce dossier est la propriété du patient et il doit être distingué du dossier professionnel qui, lui, rassemble de manière plus large l'ensemble des données « métier » des professionnels de santé.

Le DMP a été créé pour favoriser la prévention, la coordination, la qualité et la continuité des soins. Il permet au bénéficiaire de l'assurance maladie qui le souhaite de partager avec les professionnels de santé qu'il a autorisés des informations de santé sous forme électronique et ce, de manière sécurisée. Il pourra être fermé à la demande du patient, et sera alors archivé sur une période de dix ans à compter de sa clôture. Le DMP est ouvert auprès d'un hébergeur qui a été choisi par l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) à l'issue d'un appel d'offres et agréé par décision du ministre de la santé le 10 novembre 2010, après l'avis de la CNIL du 30 septembre 2010 et du Comité d'agrément des hébergeurs du 1er octobre 2010. Après une période d'expérimentation en 2006, le projet avait été suspendu avant d'être relancé en 2009. La CNIL a autorisé, le 2 décembre dernier[179], les traitements nécessaires à la première phase de déploiement généralisé du DMP sur l'ensemble du territoire, déploiement sous la responsabilité de l'ASIP Santé. Toutefois, le décret relatif aux modalités d'accès et de gestion de ce dossier est toujours en attente.

Parallèlement à la mise en place du DMP, une loi du 30 janvier 2007 a créé le dossier pharmaceutique qui vise à favoriser la coordination, la qualité, la continuité des soins et surtout la sécurité de la dispensation des médicaments, produits et objets définis à l'article L. 4211-1 du Code de la santé publique. Des précisions ont été apportées par un décret du 15 décembre 2008[180]. Sauf opposition du patient, le pharmacien est tenu d'alimenter ce dossier. Ces informations ont vocation, à terme, à être intégrées dans le DMP dès lors que celui-ci sera opérationnel.

Du côté des professionnels, le dossier médical peut être informatisé. Dans la mesure où ce dernier constitue un traitement de données à caractère personnel, il doit faire l'objet d'une déclaration[181] auprès de la CNIL sous peine de sanctions pécuniaires et/ou pénales. Les médecins libéraux bénéficient d'une procédure de déclaration simplifiée[182], sous réserve que les données ne soient pas déposées chez un hébergeur de données de santé. La procédure simplifiée n'est pas applicable aux établissements de santé dont les traitements de données restent soumis au régime de la déclaration normale ou de l'autorisation en fonction de la finalité poursuivie. Les droits et obligations issues de la loi n°78-17 du 6 janvier 1978 modifiée, dite loi « Informatique et libertés » trouvent à s'appliquer dans ce contexte. Ainsi, le responsable du traitement des données est tenu à une obligation d'information[183] stricte envers le patient, il doit également garantir la sécurité[184] et la confidentialité des données et fixer des durées de conservation limitées des données. A côté du droit d'accès

178. JO n°190 du 17 août 2006.
179. Voir à cet égard le site de la Cnil : http://www.cnil.fr/dossiers/sante/actualites/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-lensemble-du-territoire/.
180. Décret n°2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique, J.O. du 17 décembre 2008, p. 19237.
181. Article 22 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
182. Délibération de la CNIL n°2005-296 du 22 novembre 2005 portant adoption d'une norme simplifiée (n° 50) relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestions de leur cabinet.
183. Article 32 de la loi n°78-17 du 6 janvier 1978.
184. Article 34 de la loi n°78-17 du 6 janvier 1978.

à ses données, la loi « Informatique, Fichiers et Libertés » reconnaît au patient un droit d'opposition[185] au traitement des données qui le concernent et un droit de rectification [186] et de suppression des données inexactes ou incomplètes.

L'article L. 1111-8 du Code de la santé publique, issu de la loi du 4 mars 2002, définit, quant à lui, l'encadrement de l'activité d'hébergement des données de santé. Des précisions sur les modalités d'accès et d'hébergement pour l'ensemble de ces données ont ensuite été apportées par le décret n°2006-6 du 4 janvier 2006[187] (articles R. 1111-1 et s. du Code de la santé publique).

Ainsi, pour les dossiers actifs, les professionnels de santé ou les établissements de santé peuvent déposer des données de santé auprès d'un hébergeur agréé qui a respecté les exigences des articles R. 1111-9 et s. du Code de la santé publique. Cet hébergement ne peut avoir lieu qu'avec le consentement exprès du patient. La prestation d'hébergement fait l'objet d'un contrat avec le médecin et/ou l'établissement de santé qui doit contenir certaines clauses obligatoires définies à l'article R. 1111-13 du Code de la santé publique. L'hébergeur agréé doit mettre en place une série de mesures propres à assurer la pérennité, la confidentialité et la sécurité de ces données.

En principe, le secret médical tel que posé par l'article 226-13 du code pénal fait obstacle à ce que le dossier médical informatisé soit partagé. Toutefois, l'article L. 1110-4 du Code de la santé publique autorise de manière exceptionnelle l'échange d'informations relatives au patient entre les professionnels de santé chargés de sa prise en charge et ce, exclusivement afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. Le patient doit avoir été dûment averti de cet échange et de la possibilité de s'y opposer [188]. Pour les établissements de santé, en revanche, le patient est réputé confier ses données à l'ensemble de l'équipe et il n'existe qu'un dossier unique partagé.

Il est à noter que pour l'accès ou la transmission par voie électronique de données de santé, l'article R. 1110-3 du Code de la santé publique fait obligation au professionnel d'utiliser sa carte de professionnel de santé, délivrée par l'ASIP Santé et comportant plusieurs certificats (authentification, signature, confidentialité) émis par l'ASIP Santé en tant qu'autorité de certification.

A cet égard, la confidentialité des informations médicales transmises par voie électronique est encadrée par l'article L. 1110-4 du Code de la santé publique et le décret du 15 mai 2007[189] relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique, dont les dispositions ont notamment été codifiées aux articles R. 1110-1 et s. du Code de la santé publique. Il est à noter que le fait d'obtenir ou de tenter d'obtenir la communication d'informations médicales à caractère personnel en violation des dispositions de l'article L. 1110-4 du Code de la santé publique est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

Le développement de la télémédecine instaurée par la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires[190] et dont le

185. Article 38 de la loi n°78-17 du 6 janvier 1978.
186. Article 40 de la loi n°78-17 du 6 janvier 1978.
187. JO n°4 du 5 janvier 2006 p. 174.
188. Article L. 1110-4 alinéa 3 du Code de la santé publique.
189. JO du 16 mai 2007, p. 9362.
190. JO 22 juillet 2009, p. 12184. Voir l'article L. 6316-1 du Code de la santé publique.

décret d'application[191] est paru en octobre 2010, devrait également favoriser les échanges électroniques de données médicales.

G. L'archivage électronique des archives publiques

La loi n°2008-696 du 15 juillet 2008 relative aux archives[192] reprend en majeure partie les grands principes généraux d'organisation des archives des collectivités locales fixés par le Code du patrimoine et par le décret n°79-1037 du 3 décembre 1979, modifié par le décret n°2009-1124 du 17 septembre 2009[193] (et récemment abrogé et codifié par le décret n°2011-574 du 24 mai 2011[194] au sein de la nouvelle partie réglementaire du Code du patrimoine), et n'aborde pas spécifiquement la question des archives électroniques. Toutefois, certaines de ces dispositions ont une incidence directe et significative sur l'archivage électronique.
Les définitions existantes étant déjà suffisamment larges pour englober les archives électroniques, la loi du 15 juillet 2008 n'a fait qu'apporter quelques légères modifications au Code du patrimoine.

L'article L. 211-4 du Code du patrimoine définit désormais les archives publiques comme :
«a) Les documents qui procèdent de l'activité de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public ou des personnes de droit privé chargées de la gestion d'un service public, dans le cadre de leur mission de service public. Les actes et documents des assemblées parlementaires sont régis par l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires;(…)
c) les minutes et répertoires des officiers publics ou ministériels ».

De plus, la circulaire du 2 novembre 2001[195] précise que *« les archives publiques comprennent l'ensemble des documents qui, quels qu'en soient la date, la forme ou le support, procèdent de l'activité de l'Etat, des collectivités locales, des établissements et des entreprises publiques, et des organismes de droit privés chargés de la gestion d'un service public ou d'une mission de service public, ainsi que les minutes et répertoires des officiers publics ou ministériels ».* Les archives publiques ne font donc pas l'objet de prescriptions juridiques particulières quant à leur date, leur forme ou leur support. L'archivage électronique est ainsi compatible avec le cadre juridique applicable aux archives publiques. D'ailleurs, la Direction des Archives de France, aujourd'hui le Service Interministériel des Archives de

191. Décret n°2010-1229 du 19 octobre 2010 relatif à la télémédecine, JO n°0245 du 21 octobre 2010. Il a introduit notamment les articles R. 6316-1 et s. dans le Code de la santé publique.
192. JO du 16 juillet 2008, p.11322 et s. V. Eric Caprioli, Ilène Choukri, Noëlle Jean-Pierre, Décryptage de la loi du 15 juillet 2008, Gazette des communes, du 1er décembre 2008, p. 68 et s.
193. JO du 18 septembre 2009, p. 15251,
194. Décret n°2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (livres Ier à VI) Les dispositions réglementaires du code du patrimoine font l'objet d'une publication spéciale annexée au Journal officiel de ce jour, JO du 26 mai 2011 p. 9084,
Et son annexe : Annexe au décret n°2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres) et au décret n°2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (livres Ier à VI), JO du 26 mai 2011 p. 3.
195. Circulaire du 2 novembre 2001 relative à la gestion des archives dans les services et établissements publics de l'Etat , JO n°256 du 4 novembre 2001, p.17359 et s.

France[196], s'intéresse de plus en plus à la question de l'archivage électronique et a déjà publié des notes d'information et des instructions très riches en la matière[197].

Dans la sphère publique, l'archivage a essentiellement deux finalités : une finalité informationnelle, historique, statistique ou une finalité juridique[198].

L'archivage des documents à finalité informationnelle, historique ou statistique par l'administration a pour objectif la préservation du patrimoine informationnel et culturel de la France. Cet archivage est distinct et souvent postérieur à l'archivage à finalité juridique. Lorsque la finalité de l'archivage est seulement patrimoniale, les documents électroniques archivés ne doivent plus nécessairement remplir les conditions exigées par le droit pour admettre leur valeur juridique. L'archivage devra cependant garantir au minimum l'intégrité des documents conservés, leur disponibilité et leur accessibilité (au sens de lisibilité). Toutefois, en pratique, l'archivage des documents au titre d'archives publiques recouvre le plus souvent une finalité juridique. Dans cette finalité, l'archivage doit permettre de prouver certains droits ou de démontrer que les exigences de légalité imposées aux documents conservés ont été respectées. L'enjeu d'utiliser un archivage électronique fiable et sécurisé n'est donc pas anodin[199]. Par ailleurs, du fait de leur caractère public, les archives conservées par l'administration doivent impérativement, pendant une certaine période, rester consultables. L'archivage électronique de ces archives doit donc prendre en compte deux contraintes : la durée de conservation du document et les règles de communication du document archivé, surtout depuis que le régime de communicabilité des archives publiques a été modifié par la loi du 15 juillet 2008.

Habituellement, on distingue trois étapes d'utilisation des archives publiques[200] :
- Les archives courantes qui sont *« les documents qui sont d'utilisation habituelle pour l'activité des services, établissements et organismes qui les ont produits ou reçus»* ;
- Les archives intermédiaires qui sont « *les documents qui : a) ont cessé d'être considérés comme archives courantes ; b) ne peuvent encore, en raison de leur intérêt administratif, faire l'objet de sélection et d'élimination »* conformément à l'article R. 212-14 du Code du patrimoine ;
- Les archives définitives qui sont les *« documents qui ont subi les sélections et éliminations définies aux articles R. 212-13 et R. 212-14 et qui sont à conserver sans limitation de durée. ».*

Ces périodes dépendent de la durée d'utilité administrative (D.U.A.)[201] du document conservé. La durée d'utilité administrative dépend de l'utilisation du document et de la nature du droit auquel il se rapporte. Il peut s'agir de très courtes durées ou de durées infinies.

Les délais de communication prévus par le législateur imposent, quant à eux, que les

196. Ce service est rattaché à la direction générale des patrimoines. L'organisation de cette direction est décrite dans l'arrêté du 17 novembre 2009 relatif aux missions et à l'organisation de la direction générale des patrimoines, JO du 5 décembre 2009.
197. V. sur le site de la Direction des Archives de France la rubrique « Archives électroniques » disponible à l'adresse suivante : http://www.archivesdefrance.culture.gouv.fr/gerer/textes/.
198. V. l'article L. 211-2 du Code du patrimoine.
199. Il est à noter toutefois qu'un document qui n'aurait pas de valeur juridique dès son établissement n'en aura pas non plus du fait d'un archivage électronique sécurisé.
200. V. les articles R. 212-10 à R. 212-12 du Code du patrimoine.
201. Cette durée correspond au délai minimal pendant lequel les documents doivent être conservés dans les locaux des établissements ou services producteurs en tant qu'archives courantes ou intermédiaires. Ces dernières peuvent être prises en charge par les services publics d'archives.

archives restent consultables pendant une certaine période. De ce point de vue, la loi du 15 juillet 2008 a largement modifié le régime de communicabilité des archives dans un but de simplification et d'harmonisation avec la loi « CADA » du 17 juillet 1978[202]. Désormais, le principe est celui de la libre communicabilité des archives au public[203], sauf exceptions qui sont prévues à l'article L. 213-2 du même Code. Ce dernier impose des délais spéciaux, globalement plus courts qu'auparavant[204], pour les documents non immédiatement communicables.

L'affirmation du principe de libre communicabilité des archives et l'abrègement des délais de communicabilité (qui restent toutefois relativement longs) ont des conséquences majeures sur la mise en place d'un système d'archivage électronique. En effet, le service d'archives devra mettre en place un système de gestion des archives (gestion électronique de documents) permettant de retrouver de manière rapide et efficace tous les documents faisant l'objet d'une demande de consultation ou de communication. De plus, compte tenu des délais de conservation, l'archivage électronique devra prendre en compte ces contraintes de temps, ce qui implique que le procédé d'archivage soit capable d'évoluer à moyen ou à long terme.

Qui plus est, avec le développement de l'administration électronique, les personnes publiques seront de plus en plus confrontées au besoin d'archiver des documents créés sous forme électronique et qui seront alors des « originaux électroniques ». Pour ce faire, elles devront mettre en place un système d'archivage fiable et sécurisé. Jusqu'ici, l'externalisation de l'archivage des documents des collectivités était proscrite, mais la loi du 15 juillet 2008 offre désormais la possibilité pour les collectivités locales de recourir à des tiers archiveurs privés dans certaines conditions.

Ces conditions sont celles posées par l'article L. 212-4 II du Code du patrimoine et surtout celles décrites dans le décret du 3 décembre 1979 modifié par le décret n°2009-1124 du 17 septembre 2009 et récemment codifié au sein de la partie réglementaire du Code du patrimoine par le décret n° 2011-574 du 24 mai 2011 :
- Le recours à un tiers archiveur n'est possible que pour les archives courantes ou intermédiaires, ce qui exclut les archives définitives. De même, lorsqu'un texte prévoit expressément que les archives publiques doivent être obligatoirement versées dans un service public d'archives, il sera impossible de passer par un tiers.
- Le tiers archiveur devra au **préalable être agréé par l'administration des archives**. Les conditions d'attribution et de retrait de cet agrément sont détaillées aux articles R. 212-19 à R. 212-31 du Code du patrimoine. L'article R. 212-27 du Code du patrimoine définit plus spécifiquement les éléments que le prestataire doit fournir pour pouvoir conserver des archives sur support électronique (description des lieux, description de la typologie et de la topographie du réseau, description des infrastructures logicielles et matérielles…) ; étant noté que dans ce cas l'agrément n'est accordé, comme le précise l'article R. 212-29 du Code du patrimoine, que pour une durée de trois ans contrairement à la durée d'agrément pour une conservation sur support papier. Par ailleurs, un arrêté du 4 décembre 2009[205] précise les normes auxquelles les prestataires d'archivage électronique devront se référer

202. Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et le public et diverses dispositions d'ordre administratif, social et fiscal, JO du 18 juillet 1978, p. 2851 et s.
203. V. article L. 213-1 du Code du patrimoine.
204. Ils varient désormais de 25 à 120 ans.
205. Arrêté du 4 décembre 2009 précisant les normes relatives aux prestations en archivage et gestion externalisée, JO du 12 décembre 2009.

dans le cadre de l'exercice de leur activité : il s'agit de la norme NF Z 42-013 de mars 2009 précitée et de la *« norme ISO 14721 : 2003/CCSDS, juin 2005, qui constitue un modèle de référence pour un système ouvert d'archivage (OAIS) »*.

- La collectivité devra procéder à une déclaration auprès de l'administration des archives et surtout devra conclure **avec la société privée un contrat de dépôt dont les clauses minimales sont imposées par l'article L. 212-4-II du Code du patrimoine** (conditions de sécurité et de conservation des documents déposés, modalités de leur communication et de leur accès, du contrôle de ces documents par l'administration des archives et de leur restitution au déposant à l'issue du contrat). L'article R. 212-21 du Code du patrimoine précise également que ce contrat est nécessairement conclu par écrit, qu'il est soumis au contrôle de la personne chargée du contrôle scientifique et technique de l'Etat sur les archives qui doit formuler ses observations dans le mois de la transmission du projet de contrat et qu'il ne peut contenir de clause prévoyant un droit de rétention des archives déposées. Par ailleurs, l'article R. 212-22 du Code du patrimoine détaille les clauses minimales devant figurer dans le contrat et qui sont les suivantes :

« 1° La nature et le support des archives déposées ;
2° La description des prestations réalisées : contenu des services et résultats attendus ;
3° La description des moyens mis en œuvre par le dépositaire pour la fourniture des services ;
4° Les dispositifs de communication matérielle et d'accès aux archives par le déposant ;
5° Si le dépositaire procède à des modifications ou à des évolutions techniques, ses obligations à l'égard du déposant ;
6° Une information sur les garanties permettant de couvrir toute défaillance du dépositaire ;
7° Les dispositifs de restitution des archives déposées à la fin du contrat de dépôt, assortis d'un engagement de destruction intégrale des copies que le dépositaire aurait pu effectuer pendant la durée du contrat ;
8° Une information sur les conditions de recours à des prestataires externes ainsi que les engagements du dépositaire pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité de conservation ;
9° Les polices d'assurance que le dépositaire souscrit pour couvrir les dommages et pertes que pourraient subir les archives déposées le contrat prévoit que celles-ci excluent expressément les archives déposées du champ d'application de la clause de délaissement ;
10° La durée du contrat et les conditions d'un éventuel renouvellement. »

L'adoption du décret d'application de la loi du 15 juillet 2008 publié en 2009 était très attendue et a permis de donner tout son sens à l'externalisation de la gestion des archives publiques. Qui plus est, il a permis de mettre fin à certains conflits possibles avec d'autres textes réglementaires allant dans le sens contraire à la loi du 15 juillet 2008 puisque l'article 22 du décret du 3 décembre 1979, aujourd'hui abrogé par le décret du 24 mai 2011, prévoyait que *« Toutes dispositions contraires au présent décret sont abrogées et notamment le décret du 21 juillet 1936 réglementant les versements dans les dépôts et archives de l'Etat des papiers des ministères et des administrations qui en dépendent. »*.

En tout état de cause, que la collectivité décide de recourir ou non à un tiers archiveur,

pour être considéré comme sécurisé[206], le système d'archivage devra garantir l'intégrité, l'intelligibilité, la durabilité et l'accessibilité du document archivé. Toutes les archives et les opérations y afférentes devront nécessairement être tracées et la disponibilité du service ainsi que l'interopérabilité entre les différents systèmes d'archivage (collectivités, archives de France, etc.) devront être assurées. Enfin, la mise en place d'un archivage électronique sécurisé doit reposer sur l'adoption d'un certain nombre de documents importants (politique d'archivage, déclaration des pratiques d'archivage, cahier des charges, grilles d'audit). De plus, les recommandations de la Direction générale des patrimoines dans ce domaine seront également à prendre en compte. Un standard d'échange conforme aux normes internationales, applicable également dans les entreprises, a été élaboré par l'ancienne Direction des Archives de France avec la Direction Générale de la Modernisation de l'Etat du Minefi et a fait l'objet d'une évolution[207].

H. Le permis de conduire électronique

Il existe à ce jour 110 modèles de permis de conduire dans l'Union européenne. Pour garantir au mieux les libertés de circulation et d'établissement des citoyens de l'Union, le législateur européen a pris l'initiative en 2006[208] d'une réforme instituant un permis de conduire unique à l'échelle européenne, visant à faciliter la reconnaissance mutuelle, améliorer la sécurité routière, tout en limitant le risque de fraude documentaire. La transposition des mesures adoptées devra intervenir avant le 19 janvier 2013[209].

Ce permis de conduire unique, adapté aux spécificités linguistiques de chaque Etat membre, devra répondre à certaines exigences visant à lutter contre la fraude (falsifications notamment) et améliorer la sécurité routière (contrôle médical). Il devra également être doté d'un support de mémoire informatique (microprocesseur).

Le 9 novembre 2011[210], le décret n°2011-1475 a transposé diverses mesures réglementaires de la directive 2006/126/CE relative au permis de conduire. Ce décret organise notamment le remplacement progressif des anciens permis de conduire par le nouveau modèle de permis à partir du 19 janvier 2013 et jusqu'au 19 janvier 2033[211]. Ce nouveau permis aura une durée de validité de quinze ans à compter de sa délivrance[212]. Les conditions de son renouvellement seront fixées par arrêté. Ce décret entrera en vigueur le 19 janvier 2013[213].

---

206. V. à titre informatif l'étude publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI qui est devenue l'ANSSI puis l'ANDSI) relative à l'archivage électronique sécurisé dans la sphère publique (http://www.ssi.gouv.fr/site_article48.html). Celle-ci traite de la problématique de l'archivage électronique à des fins juridiques dans la sphère publique. Ont participé à cette étude et à la rédaction de la politique d'archivage type pour la sphère publique : le bureau conseil de la DCSSI, la DGME et la DAF. Cette étude a été réalisée sur la base de travaux du Cabinet d'avocats Caprioli & Associés, de la société Oppida et de JMR Consultants.

207. Version 0.2 disponible à l'adresse : http://www.references.modernisation.gouv.fr/presentation.

208. Directive 2006/126/CE du Parlement européen et du Conseil du 20 décembre 2006 relative au permis de conduire, JOUE L 403 du 30 décembre 2006, p. 0018.

209. Cf. Projet FAETON de modernisation du fichier des permis de conduire (dématérialisation) : http://www.senat.fr/rap/l09-101-310/l09-101-31067.html.

210. Décret n°2011-1475 du 9 novembre 2011 portant diverses mesures réglementaires de transposition de la directive 2006/126/CE relative au permis de conduire, JO du 10 novembre 2011.

211. Article 6-III du décret n°2011-1475 du 9 novembre 2011 modifiant l'article R. 221-4 du Code de la route.

212. Article 2 et 4 décret n°2011-1475 du 9 novembre 2011 modifiant les articles R. 211-1 et R. 221-1 du Code de la route.

213. Article 18 du décret n°2011-1475 du 9 novembre 2011.

Objectifs / Moyens	Lutte contre la fraude documentaire	Reconnaissance mutuelle	Sécurité routière
Permis de conduire unique	- Carte plastifiée en polycarbonate dotée d'un support de mémoire électronique.	- Harmonisation du contrôle des connaissances et des procédures de délivrance.	- Durée de validité limitée à 15 ans et extension aux cyclomoteurs. - Visite médicale obligatoire.
Dématérialisation du support	- Intégration d'une signature électronique permettant de renforcer l'identification - Interconnexion des fichiers européens du permis de conduire.	- Homologation CE du traitement des données par le microprocesseur.	- Recouvrement des contraventions à l'échelle européenne.
Applications	- L'authenticité d'un permis de conduire délivré par un Etat membre pourra être vérifiée en temps réel dans les autres Etats membres.		- Identification pour le paiement à distance des contraventions. - Consultation du capital de points et de l'historique (retraits, récupération, motifs).

I. La Carte Nationale d'Identité Electronique

La carte Nationale d'Identité est un document individuel délivré par l'Etat, permettant d'établir et de vérifier l'identité de son porteur, voire de le contrôler. Les enjeux sociaux, culturels et juridiques du passage à l'électronique sont très importants[214]. C'est dans cette optique que les programmes INES (Identité Nationale Electronique Sécurisée) ont été lancés par le Ministère de l'Intérieur. Ce programme devait consister à :

- Fusionner les procédures de demande de carte d'identité et de passeport (le passeport électronique est aujourd'hui disponible pour un grand nombre de citoyens) ;
- Améliorer la gestion des titres dans de nouvelles applications ;
- Délivrer des titres conformes aux exigences internationales ;
- Offrir des moyens d'identification et de signature électronique aux citoyens.

La Carte Nationale d'Identité Electronique (CNIE) devait voir le jour en 2006. Elle devait comprendre les principales données relatives à l'état civil de son titulaire (nom, prénom, sexe, date et lieu de naissance), la mention de sa nationalité, son adresse, la date de délivrance et de caducité de la carte, le numéro d'identification du document, le code de la commune qui l'a délivré, la signature numérisée du titulaire ainsi qu'également des informations imprimées sur la carte, en particulier la photo et deux empreintes digitales.

214. V. l'Etude d'impact AFNOR, La signature électronique et les infrastructures à clé publique dans le contexte de l'identité numérique : quels usages pour les titres sécurisés émis par l'Etat dans le monde de l'économie sécurisée, décembre 2007, disponible sur le site www.caprioli-avocats.com.

La CNIE avait notamment pour objectifs de :

- Mieux garantir l'identité contre les risques d'usurpation ou de détournement ;
- Lutter contre le terrorisme ;
- Autoriser l'authentification du porteur en vue de l'utilisation de téléservices dans les relations avec les administrations et la signature électronique pour les services commerciaux sur l'internet ;
- Simplifier les demandes de documents d'identité électronique (un seul dossier pour la CNIE et le passeport) et leur renouvellement.

Après une large concertation sur le sujet (action du Forum des droits sur l'internet) le projet a été provisoirement suspendu. Mais étant donné que le déploiement du passeport électronique est en bonne voie *(cf. supra)*, la CNIE devrait être lancée et son rôle peut être décisif en termes de confiance pour le développement du commerce dématérialisé et sécurisé. D'ailleurs, le projet a été partiellement repris dans la proposition de loi relative à la protection de l'identité, déposée en juillet 2010 par les sénateurs Jean-René Lecerf et Michel Houel[215]. Cette proposition de loi relative à la protection de l'identité énonce à l'article 2 :

« La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :
a) Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;
b) Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;
c) Son domicile ;
d) Sa taille et la couleur de ses yeux ;
e) Ses empreintes digitales ;
f) Sa photographie.
Les dispositions du présent article ne s'appliquent pas au passeport délivré selon une procédure d'urgence ».

Cette proposition, après plusieurs amendements, a fait l'objet de débats devant le sénat et l'assemblée nationale. La loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité rappelle que *« L'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier. »* (art.1)[216]. En outre, les modalités de vérification des données contenues dans la CNIE et les conditions entourant l'usurpation d'identité y sont détaillées. La loi a été censurée partiellement par le Conseil constitutionnel (Décision du 22 mars 2012[217]). Les sages ont notamment censuré **l'art. 3** qui offrait la possibilité d'intégrer à la carte nationale d'identité des fonctions de signature électronique dans un cadre plus large de e-services, ainsi que **l'art. 5** qui prévoyait la création d'un fichier centralisé des identités. Même si, pour le Conseil, la création de celui-ci était justifiée par un motif d'intérêt général, **vu l'ampleur du traitement, les caractéristiques techniques et les conditions de consultation, l'atteinte portée au droit au respect de la vie privée ne pouvait pas être proportionnée au but poursuivi.**

Il est essentiel que la CNIE contienne au minimum un certificat d'authentification de la

215. V. le site du sénat à l'adresse : http://www.senat.fr/leg/ppl09-682.html.
216. JO du 28 mars 2012, p.5604.
217. Décision n°2012-652 DC du 22 mars 2012, disponible sur http://www.conseil-constitutionnel.fr/decision/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html.

personne et un certificat de signature pour les relations avec les autorités administratives (ce qui serait en quelque sorte un container régalien). Cela permettra notamment d'utiliser l'authentification forte délivrée par l'Etat pour identifier des personnes qui souhaitent disposer d'autres certificats électroniques ou faire des opérations sur l'internet. Mais on était également en droit d'envisager que la CNIE soit en mesure d'intégrer un certificat de signature et un autre pour l'authentification pour les usages privés, en fonction des besoins et à la demande de la personne titulaire. Selon l'Agence Nationale des Titres Sécurisés (ANTS), la CNIE permettra de réaliser des économies sur le cycle de production global des titres sécurisés et un fichier commun sera mis en place pour la délivrance de la CNIE et du passeport biométrique afin de faciliter les démarches, sécuriser la fabrication et la délivrance de ces documents.

J. Le Label IDéNum

En 2010, le Secrétariat d'état à l'Economie Numérique a décidé de mettre en œuvre avec une vingtaine de partenaires parmi lesquels la FNTC, la CDC ou encore certains adhérents de la FNTC comme le Cabinet d'avocats Caprioli & Associés, une solution alternative à la CNIE : le label IDéNum[218].

Lancé, à l'initiative du Secrétariat d'Etat à l'Economie Numérique, le 1er février 2010, le label IDéNum consiste à fédérer les outils d'authentification émis par différents acteurs, en garantissant un niveau homogène de sécurité et d'interopérabilité.

Ce label sera spécifié, testé et validé par les acteurs de l'économie numérique eux-mêmes et viendra compléter la liste des solutions de signature électronique déjà certifiées et régulées par le ministère de l'économie et des finances en prévoyant les produits IDéNum. Ce produit se présente sous la forme d'un dispositif physique sécurisé dans lequel se trouvent des *« éléments propres »* à son propriétaire, que ce dernier peut déverrouiller par un code PIN : il s'agit de deux bi-clés cryptographiques – l'une dédiée à l'authentification, l'autre à la signature électronique – pour lesquelles chaque clé publique a été certifiée. En tant que tel, il pourrait être constitué comme une solution provisoire dans l'attente de la CNIE.

Le produit IDéNum devrait pouvoir être obtenu auprès des prestataires de services de certification électronique (PSCE) dont l'offre IDéNum sera attestée comme étant conforme aux exigences techniques, figurant dans le cahier des charges.

Du fait de sa référence expresse au RGS, les produits et les téléservices référencés par l'ordonnance du 8 décembre 2005 seront automatiquement acceptés par toutes les autorités administratives qui disposent des services électroniques. Les services privés seront également autorisés à accepter les produits selon qu'ils sont référencés ou non. Le label IDéNum s'affichera sur les sites qui le reconnaissent et les internautes pourront choisir librement leur fournisseur. Ainsi, le label permettra de fournir aux internautes un moyen fiable d'authentification pour simplifier leurs démarches en ligne (accès à ses comptes administratifs, abonnement à des services payants, souscription de services ou de contrats, etc.), en unifiant le marché et en facilitant les formalités quotidiennes des administrés et des citoyens. Qui plus est, le label permettra au public de bénéficier de produits d'authentification

218. V. la présentation de lancement du Label IDéNum en date du 1er février 2010 par le Secrétariat d'Etat à l'Economie Numérique : http://www.gouvernement.fr/gouvernement/label-idenum-plus-de-securite-et-plus-de-facilite-pour-l-usage-des-services-sur-interne http://www.gouvernement.fr/sites/default/files/fichiers_joints/CP_IDeNum.pdf.

et de signature électronique de qualité garantie et d'identifier facilement les services en ligne qui acceptent ces produits.

Le 31 mai 2011, ont été annoncés la création d'un consortium IDéNum ainsi que le lancement d'une étude de préfiguration pour établir les modalités de constitution de ce consortium. Quatre grandes entreprises (France Télécom/Orange, La Poste, SFR et la Fédération bancaire française) ont signé avec le ministre chargé de l'industrie un accord cadre pour la mise en œuvre du projet et se sont dites prêtes à proposer, avec l'aide de l'État, les premières offres d'ici à quelques mois[219]. Les acteurs du marché restent toujours dans l'attente …

219. V. la présentation de lancement du consortium et de son étude de préfiguration : http://www.gouvernement.fr/gouvernement/identification-sur-internet-le-label-idenum-sur-les-rails http://www.minefe.gouv.fr/actus/11/IDEnum.html.

A PROPOS DE LA FEDERATION NATIONALE DES TIERS DE CONFIANCE

La Fédération Nationale des Tiers de Confiance (FNTC) est un acteur majeur 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.

Créée en 2001, la FNTC regroupe les professionnels de la dématérialisation, à savoir : 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.

La FNTC a pour but d'établir la confiance dans l'espace numérique, de promouvoir la sécurité et la qualité des services et de veiller au respect d'une charte d'éthique de la profession.

LES ADHÉRENTS FNTC*:

Accelya ; ACOSS ; ADEN ; Adminium ; AFCDP ; Alexandre Diehl ; AllPerf ; Almerys ; Alphacode ; APECA ; Aproged ; Argus DMS ; Atos Worldline ; Bernard Starck ; Bruno Couderc Conseil ; Bull ; Cabinet Caprioli & Associés ; Cecurity.com ; Cedricom ; Celtipharm ; CertEurope ; ChamberSign ; Chambre Nationale des Huissiers de Justice ; Compagnie Nationale des Commissaires aux Comptes ; Conex ; 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 ; DPII Telecom ; Ecosix ; Edificas ; Edokial ; EESTEL ; eFolia ; ESI ; Esker ; Esopica ; Everial ; Extelia ; Forum Atena ; G.L.I. Ingénierie et Services ; Gdoc Lasercom ; Hervé Schauer Consultants ; Imprimerie Nationale ; Info Service Europe ; Interb@t ; Isilis ; jedeclare.com ; Kahn & Associés ; Keynectis ; Lettranet ; Lex Persona ; Locarchives ; Maileva ; MiaXys ; Microlist ; MIPIH ; Neuflize OBC ; Odyssey Services ; Office des Postes et Télécommunications Polynésie Française ; OFSAD ; Omnikles ; OPUS Conseils ; Pauline Le More ; Perfect Memory ; Pitney Bowes Asterion ; PPI ; Primobox ; Sagemcom ; Scala ; SealWeb ; Sogelink/DICT.fr ; Stocomest ; Syrtals ; TESSI Ged ; UIHJ ; Univers Monétique ; Valerian ; Voxaly Electionneur ; Wacom ; Xeonys.

** Liste arrêtée au 1er juin 2012*

Fédération Nationale des Tiers de Confiance
19, rue Cognacq-Jay
75007 – Paris
Tel. 01 47 50 00 50
info@fntc.org - www.fntc.org

Conception graphique et illustration : www.idsg.fr