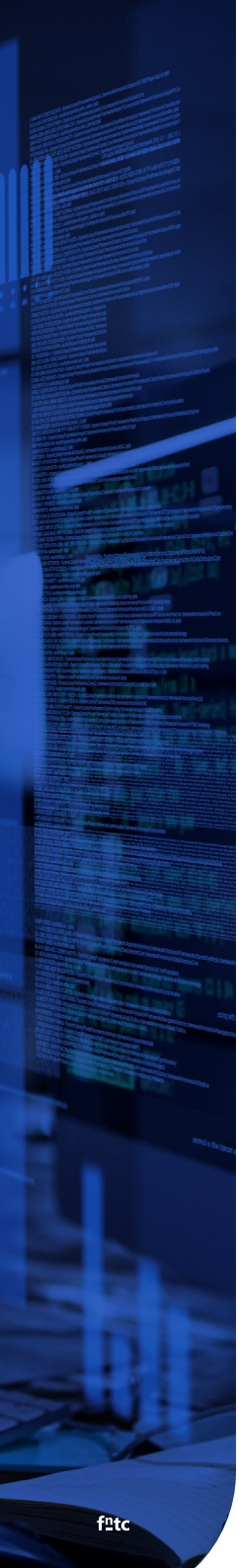
VADE-MECUM JURIDIQUE

de la digitalisation des documents et des échanges

Rédigé par le Cabinet d'avocats CAPRIOLI & Associés,
sous la direction d'Eric A. CAPRIOLI, pour le compte de la FnTC

Sommaire



PRÉFACE

L'essor de la dématérialisation est une réalité.

Sa phase initiale de simple procédé technique de libération d'espace est révolue depuis le bouleversement juridique institué par la Loi du 13 mars 2000.

A cet état réducteur de « *numérisation pour archiver* » a succédé celui plus complexe et sophistiqué de management des contenus sur supports numériques : le « *scan to process* ».

En rendant possible l'usage de multiples traitements numériques, le changement du support des données génère une fluidification des échanges qui amplifie nos performances économiques. Mais d'ores et déjà, il convient d'élargir le champ d'application de la dématérialisation.

Le temps est venu pour l'État d'ouvrir plus largement les vannes des flux dématérialisés, de mobiliser activement chaque citoyen, et d'en faire un partenaire concerné. Pour cela, il va devoir lui fournir les instruments d'une dématérialisation intelligente, susceptible d'approvisionner son quotidien en une palette d'applications ingénieuses et - surtout – conviviales et faciles à utiliser.

Mais, auparavant il doit l'aider à casser ses freins culturels… et le convaincre qu'il n'est pas plus exposé à des dangers dans l'immatériel que dans la « *vraie vie* ».

La Fédération Nationale des Tiers de Confiance contribue largement à la structuration du phénomène mouvant de la dématérialisation.

PRÉFACE

La diversité de ses membres constitue une incontestable richesse technologique et intellectuelle, et les atouts qu'elle tire de sa polyvalence sont de nature à lui permettre de transmettre au public le sentiment de confiance qui conditionnera le succès de la « *dématérialisation 3.0* ».

Toujours griffée FnTC, cette septième édition du « *Vade-mecum juridique de la dématérialisation* » trouvera aisément sa place parmi les références indispensables du domaine.

Alain BOBANT

Président d'honneur de la Fédération des Tiers de Confiance du numérique.

DANS LA COLLECTION LES GUIDES DE LA CONFIANCE DE LA FnTC

- Comprendre le règlement eIDAS – Volume 1 : Qu'est-ce que le règlement eIDAS ? (prochainement)
- Guide pratique de mise en œuvre de la conformité au RGPD par le Sous-Traitant – Volume 1 : Grilles de sélection et Registre de traitement du Sous-Traitant (prochainement)
- La signature électronique III : Conservation à long terme des documents signés (octobre 2022)
- Que faire pour utiliser les services d'archivage numérique d'un Tiers Archiveur quand ceux-ci sont proposés par un intermédiaire ? (décembre 2021)
- Copie fiable - Numérisation fidèle & archivage électronique (octobre 2021)
- KYC - Comment maîtriser et optimiser votre connaissance client (septembre 2021)
- La signature électronique II : Validation et Archivage (août 2021)
- La signature électronique : Définitions et cas d'usage (mai 2021)
- Archivage électronique : Que choisir entre Coffre-Fort Numérique (CFN) et Système d'Archivage Electronique (SAE) ? (janvier 2021)
- Interopérabilité des coffres-forts numériques – L'identifiant de coffre-fort numérique : (ID-CFN) octobre 2020)
- La facture électronique à la portée de tous (octobre 2019)
- Disparition du double électronique (de la facture) et apparition du double numérique : que faire ? (janvier 2019)
- Archivage des preuves de signature électronique à la volée (octobre 2018)
- La numérisation fidèle selon NF Z42-026 et la destruction des originaux papiers (avril 2017)
- Vade-mecum juridique de la dématérialisation des documents – nouvelle édition (juin 2016)
- Guide pratique de mise en œuvre du Relevé d'identité du Coffre-fort numérique (octobre 2015)
- Guide pour la confidentialité des archives numériques (juin 2015)

INTRODUCTION

La « *digitalisation* » des documents et des échanges est le terme qui remplace progressivement celui, sans doute un peu vieillot, de « *dématérialisation* » ; toutes les organisations parlent aujourd'hui du digital alors qu'il n'y a eu aucune rupture technologique. Mais la transformation, la transition est là. Cette substitution, opérée par les marketeurs dénote de la maturité du phénomène et de l'engouement qu'il suscite.

Le digital se généralise dans tous les domaines de la vie des entreprises, des autorités administratives et des citoyens : contrats commerciaux et de consommation, communications interne et externe, documents des entreprises (factures, bulletins de paie, documents RH…), coffres-forts électroniques, téléprocédures administratives et téléservices (impôts et taxes, inscription dans l'enseignement supérieur, démarches au niveau des collectivités locales, relations de collaboration ou de contrôle entre les administrations…), en passant par le vote dans les assemblées générales d'actionnaires ou les élections des instances représentatives du personnel (IRP). La crise sanitaire n'a fait qu'accélérer un phénomène qui était devenu inéluctable.

On ne compte plus les applications liées à la digitalisation 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 ou canaux (à savoir via le mobile - SMS, MMS - les cartes avec et sans contact, les objets connectés, les réseaux sociaux, etc.).

En 2021, le chiffre d'affaires du e-commerce représente 129,1 milliards d'euros, stabilisant ainsi la tendance initiée en 2020 pendant la crise du COVID 19[(1)].

(1) Source : FEVAD, Plaquette chiffres clés 2022, disponible à l'adresse : https://www.calameo.com/read/0071351454b6664e02df2.

De plus, la digitalisation s'inscrit résolument dans une perspective de développement durable des entreprises.

Si l'on s'interroge sur la notion de digitalisation des documents, elle consiste en la génération d'un document ou d'un flux de documents (papier, photos, vidéos, sons), ainsi que les traitements qui lui sont appliqués, en documents, 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. Mais de façon plus générale, il serait également utile de permettre l'interchangeabilité des supports, en ce y compris de la transformation de messages numériques en documents papier sans perte de valeur juridique. Pour ce qui est de la transformation digitale au sens général, elle comprend la numérisation des offres et de toute la chaîne de valeurs associée, elle modifie la stratégie, le fonctionnement, l'organisation et les processus collaboratifs internes de l'entreprise.

Aujourd'hui, la digitalisation représente pour notre société un enjeu fondamental dans les domaines économiques, sociaux et technologiques ; elle constitue un levier incontournable de croissance, d'emploi 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 (« Digital by design ») et de mise en œuvre du projet aux côtés des aspects informatique, sécurité, métier, marketing et organisationnel, afin de contribuer à l'établissement des spécifications fonctionnelles et de la documentation juridique et technique à préparer** (politiques de certification, d'horodatage et d'archivage, contrats

avec les clients et les partenaires, analyses de risques et assurances, conformité des procédures électroniques envisagées au regard des textes applicables…). Cette association imbriquée du droit, de la technique et de l'organisation représente un prérequis essentiel pour mener tout projet de digitalisation à bonne fin.

Sur le marché de la digitalisation, on soulignera quelques éléments marquants plus récents :

+ Le nombre exponentiel de souscriptions par voie électronique (avec signatures électroniques) en présence physique (agences et points de vente) ;
+ Le déploiement de procédés de contractualisation par voie électronique multi signataires, multi et omni canal et asynchrone ;
+ L'entrée en relation à distance dans certains secteurs (pour les prospects) ;
+ L'utilisation encouragée, voire obligatoire, de la voie électronique pour certains échanges, notamment avec les administrations ;
+ La multiplication des contentieux en matière d'écrits, de signatures électroniques et de copies numériques ;
+ Les réflexions et projets utilisant des *blockchains* ou de l'intelligence artificielle.

Il convient cependant de souligner que l'environnement juridique de la digitalisation, actuellement en vigueur dans les différents pays de l'Union européenne, issu pour une large part des transpositions de plusieurs directives européennes, se modifie.

En effet, la Commission européenne a remplacé deux directives 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 par le Règlement (UE) 2016/679 du 27 avril 2016 [dont certaines dispositions ont été précisées en droit français par la loi n° 2018-493 du 20 juin 2018 (2) conformément aux possibilités prévues par ledit

(2) Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, J.O. du 21 juin 2018 modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. 7 janvier 1978.

INTRODUCTION

Règlement] et d'autre part, la directive 1999/93/CE du 13 décembre 1999 sur les signatures électroniques qui a été abrogée définitivement le 1er juillet 2016 et remplacée par le Règlement sur l'Identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur du 23 juillet 2014 (eIDAS [3]), entré en vigueur le 17 septembre 2014 et de manière générale depuis le 1er juillet 2016. Toutes les modifications et adjonctions ont une incidence importante sur la digitalisation des échanges. De plus, il ne faut pas omettre de mentionner l'ordonnance du 10 février 2016 [4] réformant le Code civil sur le droit des obligations, des contrats (y compris par voie électronique) et de la preuve dont les dispositions sont entrées en vigueur le 1er octobre 2016.

La sphère publique connaît une évolution similaire et le déploiement de la digitalisation des relations entre les administrations, les usagers et les professionnels s'adosse à un cadre législatif et réglementaire tout aussi riche.

Une des ambitions de la Fédération des Tiers de Confiance du numérique (FnTC) est de contribuer à présenter la dématérialisation/digitalisation 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, voire doivent, être digitalisés, que ce soit dans la sphère privée (I°) ou dans la sphère publique (II°).

Rédaction
Éric A. CAPRIOLI,

e.caprioli@caprioli-avocats.com

Avocat à la Cour de Paris, Docteur en droit

Membre de la délégation française aux Nations Unies

Vice-président de la FnTC

Paris, le 10 octobre 2022.

(3) Règlement (UE) n°910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance, J.O.U.E n° L. 257 du 28 août 2014, p. 73. Ce règlement devrait évoluer suite à la Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique du 3 juin 2021 – COM (2021) 281 final (dite Proposition de règlement eIDAS) qui est en cours de discussion.

(4) Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations J.O. 11 févr. 2016.

De façon transversale, le règlement européen eIDAS, applicable en droit privé et en droit public sera évoqué dans la mesure où il établit un cadre européen en matière d'identification électronique et de services de confiance au sein du marché unique numérique (III°).

Enfin, parce que l'on ne saurait traiter de dématérialisation sans évoquer la question des données personnelles, le rôle des prestataires de services de confiance en matière de droit de la protection des données personnelles fera l'objet d'un focus particulier (IV°).

Sommaire

fntc

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)[5]

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*).

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. Cette justification des droits est appréciée par un tiers neutre et indépendant (le juge) qu'il s'avère nécessaire de convaincre sur la base de faits et/ou d'actes pertinents au regard des dispositions juridiques applicables. À cet égard, il est toujours indispensable de bien identifier le domaine juridique dans lequel le besoin de preuve s'inscrit.

À cette fin, il est utile de préciser que l'ancien article 1341 du Code civil et le décret n°2004-836 du 20 août 2004 disposaient que la preuve des actes juridiques pouvait être rapportée par tous moyens jusqu'à 1 500 euros et qu'au-delà, une preuve littérale était nécessaire [6]. L'article 1359 nouveau du Code civil n'a pas modifié le principe posé à l'article 1341, seule la formulation a évolué [7].

En outre, avec les technologies de l'information et de la communication (TIC), de nouvelles règles ont été posées en matière d'actes juridiques (exemple : les contrats). En effet, le 16 février 2015, la loi n°2015-177 [8] a autorisé le gouvernement « *à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaires pour modifier la structure et le contenu du livre III du Code civil, afin de moderniser, de simplifier, d'améliorer la lisibilité, de renforcer l'accessibilité du droit commun des contrats, du régime des obligations et du droit de la preuve, de garantir la sécurité juridique et l'efficacité de la norme* ».

Une consultation publique s'est concrétisée par la publication de l'ordonnance du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, applicable depuis le 1er octobre 2016 [9] ainsi que la loi n° 2018-287 du 20 avril 2018 ratifiant l'ordonnance n° 2016-131 du 10 février 2016 [10].

(5) E. A. Caprioli, Signature électronique et dématérialisation, LexisNexis, 2014.

(6) Article 56 du Décret n° 2004-836 du 20 août 2004, J.O. du 22 août 2004 en vigueur le 1er janvier 2005, p. 15032.

(7) Article 1359 nouveau du Code civil : « L'acte juridique portant sur une somme ou une valeur excédant un montant fixé par décret doit être prouvé par écrit sous signature privée ou authentique. Il ne peut être prouvé outre ou contre un écrit établissant un acte juridique, même si la somme ou la valeur n'excède pas ce montant, que par un autre écrit sous signature privée ou authentique. Celui dont la créance excède le seuil mentionné au premier alinéa ne peut pas être dispensé de la preuve par écrit en restreignant sa demande. Il en est de même de celui dont la demande, même inférieure à ce montant, porte sur le solde ou sur une partie d'une créance supérieure à ce montant ».

(8) Loi n° 2015-177 du 16 février 2015 relative à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures (1), J.O. du 17 février 2015 p. 2961.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Initialement, la loi n°2000-230 du 13 mars 2000 [11] portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique avait intégré l'écrit sous forme électronique dans le dispositif probatoire en insérant l'article 1316-1 (ancien) dans le Code civil. Cet article disposait 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).

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**.

Ces principes ont été maintenus par l'ordonnance n°2016-131 du 10 février 2016 qui n'apporte pas de modifications substantielles au régime décrit précédemment. Seule la numérotation a changé et le nouvel article 1366 du Code civil reprend la formulation de l'article 1316-1 (ancien) du Code civil en y intégrant celle de l'article 1316-3 et le principe selon lequel « *l'écrit sur support électronique a la même force probante que l'écrit sur support papier.* »

(9) Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, J.O. du 11 février 2016 (entrée en vigueur au 1er octobre 2016).

(10) J.O. du 24 avril 2018.

(11) J.O. 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.

De plus, depuis l'ordonnance de 2016, seule la référence aux modalités de transmission figurant initialement dans l'article 1316 du Code civil a été supprimée dans la rédaction du nouvel article 1365 issu de l'ordonnance. De même, l'article 1376 du Code civil [12] et le règlement du 23 juillet 2014 sur l'identification électronique et les services de confiance ont repris ce principe de l'équivalence probatoire des supports.

Cela étant, comme l'a rappelé la Cour de cassation, si les règles relatives à l'écrit électronique ont été posées en matière d'actes juridiques, celles-ci ne sont pas applicables à un fait juridique, dont l'existence peut être établie par tous moyens de preuve comme, par exemple le contenu d'un courrier électronique [13].

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 comme un écrit), la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) [14] avait introduit, dans le Code civil, les articles 1108-1 et 1108-2 relatifs à la validité des actes juridiques conclus sous forme électronique [15].

Ces précédentes dispositions ont été reprises dans l'article 1174 du Code civil introduit par l'ordonnance du 10 février 2016 [16] en les actualisant au regard de la nouvelle codification des articles du Code civil auxquels il est renvoyé. Ainsi, il est désormais indiqué :

« *Lorsqu'un écrit est exigé pour la validité d'un contrat, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1366 et 1367 et, lorsqu'un acte authentique est requis, au deuxième alinéa de l'article 1369.*

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. ».

L'équivalence juridique entre les supports papier et électronique en matière de validité des actes juridiques avait été confirmée en

(12) La nouvelle rédaction de l'article 1376 du Code civil n'apporte guère de changement par rapport à la version initiale du 13 mars 2000. Article 1376 du Code civil : « L'acte sous signature privée par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible ne fait preuve que s'il comporte la signature de celui qui souscrit cet engagement ainsi que la mention, écrite par lui-même, de la somme ou de la quantité en toutes lettres et en chiffres. En cas de différence, l'acte sous signature privée vaut preuve pour la somme écrite en toutes lettres. ».

(13) Cass. soc., 25 sept. 2013, n° 11-25.884, F-P+B, Sté AGL finances c/ L., Comm. Com. Elec. n° 12, Décembre 2013, comm. 132, note E. A. Caprioli, ; http://www.caprioli-avocats.com/publications/54-dematerialisation-archivage/275-regime-juridique-du-courrier-electronique-selon-la-cour-de-cassation.

(14) J.O. du 22 juin 2004, p.11168 et s.

(15) Voir Cass. civ. 1ère, 13 mars 2008, Comm. Com. Electr, Juillet-août 2008, comm. 97 ; Comm. Com. Electr. Juin 2008, comm. 80, note Éric A. Caprioli.

(16) Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, J.O. du 11 février 2016.

jurisprudence conformément à l'article 1326 ancien du Code civil. Par exemple, les juges ont admis une reconnaissance de dettes dactylographiée signée électroniquement [17]. De même, selon la première chambre civile de la Cour de cassation, on ne saurait dénier de plein droit la validité d'un contrat d'agent sportif en tant qu'écrit au sens de l'art. L. 222-17 du Code du sport, sous prétexte qu'il résulterait d'échanges électroniques [18].

A défaut d'écrit requis comme condition de validité de l'acte (exemple : 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, dans l'article 1174 du Code civil renvoie aux articles 1366 et 1367 du même code sur la preuve pour caractériser et définir les conditions d'établissement et de conservation d'un écrit à titre de validité.

Toutefois, jusqu'à très récemment, tous les actes ne pouvaient pas être dématérialisés. L'article 1175 du Code civil énonçait ainsi que certains actes sous seing privé susceptibles d'impacter la vie familiale et patrimoniale de la personne et pour lesquels l'écrit est exigé à des fins de validité, étaient exclus de l'électronique. Étaient concernés par cette exception jusqu'au 1er janvier 2022 :

+ D'une part, « *les actes sous signature privée relatifs au droit de la famille et des successions* » (exemple : convention préalable au divorce par consentement mutuel…) ;
+ Et d'autre part, « *les actes sous signature privée 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* » (exemple : le cautionnement).

Concernant les sûretés, la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite « loi PACTE [19] » prévoit en son article 60 que « *Le Gouvernement est autorisé à prendre par voie d'ordonnance, dans un délai de deux ans à compter de la publication de la présente loi, les mesures relevant du domaine de la loi nécessaires pour simplifier le droit des sûretés et renforcer son efficacité, tout en assurant un équilibre entre les intérêts des créanciers, titulaires ou non de sûretés, et ceux des débiteurs et des garants et à cette fin* », et notamment au 13° du même article : « *Moderniser les règles du Code civil relatives à la conclusion par voie électronique des actes sous signature privée relatifs à des sûretés réelles ou personnelles afin d'en faciliter l'utilisation* ».

(17) Voir Cass. 1re civ., 28 oct. 2015, n° 14-23.110, F P+B : Comm. Com. Elec.n°3, mars 2016, comm.30, note Éric A. Caprioli.

(18) Cass. civ. 1ère, 11 juill. 2018, FS-P+B, n° 17-10.458 : « qu'il résulte du dernier texte 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 (devenus 1366 et 1367) du Code civil, alors en vigueur » : Éric. A. Caprioli « Quand le courrier électronique vaut écrit électronique » Comm. com. électr.2018 comm. n° 87.

(19) Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (J.O. 23 mai 2019).

C'est chose faite avec l'ordonnance n °2021-1192 du 15 septembre 2021 qui reconnaît la possibilité d'établir sous forme électronique des sûretés, sous réserve du respect des conditions posées aux articles 1366 et 1367 du Code civil», en supprimant le 2° de l'article 1175 du Code civil.

En outre, les nouveaux articles 1176 et 1177 du Code civil relatifs aux exigences particulières de lisibilité ou de présentation d'un écrit papier reprennent à nouveau à l'identique les dispositions figurant aux articles 1369-10 et 1369-11 du Code civil. Ainsi, l'exigence d'un formulaire détachable est satisfaite dès lors qu'il est possible d'y accéder par un procédé électronique et de le renvoyer par cette même voie.

2. La notion de signature électronique (17)

L'article 1367 du Code civil relatif à la signature caractérise, au même titre que l'article 1366 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 1367 du Code civil dispose que : « *La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*

***Lorsqu'elle est électronique**, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire (22) assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État*.».

(21) Voir La signature électronique et la signature électronique II, Validation et archivage, Collection « Les Guides de la confiance de la FnTC », 2021, disponible sur le site www.FnTC.org mais aussi Éric 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 http://www.caprioli-avocats.com/publications/50-securite-de-linformation/145-signature-et-confiance-dans-les-communications-electroniques.

(22) L'identité du signataire est fondamentale et doit être vérifiée (point de vigilance dans le fichier de preuve). La Cour d'appel d'Aix-en-Provence a condamné un fournisseur pour son manque de diligence et de prudence, au regard d'une relation commerciale installée depuis plusieurs années et du processus de commande inhabituel qui lui était imposé (la société cliente se prévalait d'une usurpation d'identité). En effet, le fournisseur n'avait ni vérifié l'identité du signataire, ni eu recours à un certificat électronique qualifié permettant d'identifier formellement le client : CA d'Aix-en-Provence, 28 mars 2019, Répertoire général n° 17/14221(décision non disponible).

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Le procédé d'identification de la signature électronique doit être fiable – comme le rappelle la jurisprudence [23] - et doit garantir le lien avec l'acte auquel elle s'attache. Le décret en Conseil d'État en question, à savoir désormais le décret n° 2017-1416 du 28 septembre 2017 [24] relatif à la signature électronique renvoie vers le règlement eIDAS (V. infra Chapitre III) et abroge le décret n°2001-272 du 30 mars 2001 [25] pris pour l'application de l'article 1316-4 du Code civil.

Selon le décret du 28 septembre 2017, le procédé de signature électronique est présumé fiable jusqu'à preuve du contraire lorsque :

+ Ce procédé met en œuvre une **signature électronique qualifiée** (SEQ) entraînant un renversement de la charge de la preuve ;
+ Pour être qualifiée, une signature doit être avancée, c'est-à-dire remplir les conditions de l'article 26 du règlement eIDAS et doit avoir été créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement.

Bien qu'il existe une distinction entre la signature électronique « simple » et la signature électronique sécurisée présumée fiable désormais appelée signature électronique qualifiée, **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 (idem avec la SEQ de l'art. 1367 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 incombe à sur celui qui se prévaut de la signature électronique.

(23) 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. n°118, p. 101 et s. (disponible sur le site : www.legifrance.gouv.fr). Dans le même sens à propos de l'apposition d'une signature scannée sur un formulaire papier de dépôt de marque, CA Fort-de-France, ch. civ., 14 déc. 2012, n°12/00311, Comm. Com. Electr. n° 5, Mai 2013, comm. 60, note E. A. Caprioli. 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.) et plus récemment, Cass. civ., 1ère, 6 avril 2016, n°15-10.732, JCP éd. G, n°27, 4 juillet 2016, 783, note Éric A. Caprioli, dans le cadre de l'adhésion à une assurance complémentaire et lorsque le procédé de signature électronique utilise des certificats électroniques à usage unique : CA de Nîmes, 1ère ch., Arrêt du 14 mars 2019, Répertoire général n°17/03531.

(24) V. Pour aller plus loin sur ce point : E. A. Caprioli, Décret n°2017-1416 du 28 septembre 2017 relatif à la présomption de fiabilité de la signature électronique, Comm. com. électr. 2017, comm. n°92 ; T. Douville, Signature électronique, Publication du décret d'application, D. 2017, 1975.

Parfois, à tort, le procédé de signature électronique qualifié est considéré par certains tribunaux comme un prérequis à la validité juridique d'un contrat [26]. Pourtant, hors les cas où un texte impose expressément une signature électronique qualifiée (pour les actes authentiques par exemple), il n'existe pas d'exigence légale pour recourir à ce type de 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 1367 du Code 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 et l'intégrité de ce dernier.

Par exemple, une signature électronique fondée sur un certificat « *éphémère* » ou « *à usage unique* » (valable pour une session de temps relativement brève ou pour une transaction) pourra être reçue devant les tribunaux sous réserve que soient dûment respectées les exigences précédentes [27].

Cette pratique, utilisée de plus en plus fréquemment pour la contractualisation en agence, sur le point de vente ou à distance de certains produits bancaires (ouverture de compte, contrat d'épargne, contrat de crédit à la consommation…) ou dans d'autres domaines (exemple : assurances, mutuelles) 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 quelques minutes).

Une fois l'opération ou la session de temps 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 ou des documents contractuels et intégrité, validation des certificats utilisés…).

(25) Décret pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, J.O. du 31 mars 2001, p. 5070. Voir Éric 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.

(26) En matière de contrat de crédit électronique : CA DiJ.O.n, 2ème Chambre civile, Arrêt du 28 juin 2018, Répertoire général n° 17/01790 ; CA Rouen, ch. prox., 31 mai 2018, n° 17/03404, Éric A. Caprioli, « Charge de la preuve et contrat de crédit à la consommation : errances jurisprudentielles », Comm. com. électr. 2018, comm. n°78.

(27) CA Nîmes, 1ère ch., Arrêt du 14 mars 2019, Répertoire général n°17/03531.

Ces procédés de signature pourront également être utilisés dans le cadre de la signature d'un contrat en agence en présence physique du client (exemple : sur une tablette graphique ou avec un code envoyé via le téléphone mobile/sur-authentification). Le représentant du prestataire technique (interne ou externe) pourra attester de la fiabilité du processus de contractualisation électronique et du contenu du fichier de preuve, le cas échéant, devant le tribunal.

Un arrêt de la cour d'appel de Nancy en date du 14 février 2013, infirmant un jugement du 12 décembre 2011 du Tribunal d'instance d'Épinal, est venu rappeler l'importance du fichier de preuve dans la gestion des litiges postérieurs à une transaction électronique, ainsi que les modalités relatives à l'admission de la preuve électronique devant un juge [28]. En l'espèce, une société de crédit avait consenti à un emprunteur un crédit renouvelable dont le montant avait été augmenté par deux avenants, un troisième ayant été souscrit par voie électronique.

Après plusieurs échéances restées impayées, l'établissement de crédit assigna l'emprunteur en justice pour demander le remboursement des sommes et produisait pour justifier du dernier avenant le document « *fichier de preuve de la transaction* ». Le tribunal d'instance d'Epinal a écarté cet élément en affirmant que « *le document* « *fichier de preuve de la transaction* » *est insuffisant pour s'assurer non seulement de l'engagement de Monsieur X puisqu'aucun élément de la prétendue signature électronique ne permet de faire le lien entre l'offre de prêt non signée et le document produit,* ***en l'état simple fichier imprimé*** *sans garantie d'authenticité, ni justification de la sécurisation employée.* ».

En effet, il s'est avéré que la preuve avait été mal présentée aux juges [29]. Sur la base de cette constatation, le Tribunal d'instance jugeait l'action de la société de crédit forclose.

La Cour d'appel de Nancy dans son arrêt du 14 février 2013 a infirmé l'ensemble du jugement. Se fondant sur les dispositions de l'article 1316-4 du Code civil et du décret n°2001-272 du 30 mars 2001, dispositions relatives à la signature électronique, la cour a relevé que la société de crédit « *produit aux débats le fichier de preuve de la transaction émis par l'autorité de certification. La mention du numéro de l'avenant sur le fichier de preuve permet de vérifier que c'est bien cet avenant qui a été signé électroniquement par monsieur X.*

(28) D V. Éric A. Caprioli, Première décision sur la preuve et la signature électronique d'un contrat de crédit à la consommation, JCP éd. G n°18, 2013, 497, p.866 à 869 et Comm. Com. Electr. 2013, Juin, Étude 11, p. 13 à 17. Dans une affaire similaire où la signature électronique n'ayant pas été déniée, la Cour a estimé que la preuve de la signature de l'avenant avait été rapportée, CA Douai, 8e ch., 1re sect., 2 mai 2013, v. Comm. Com. Electr. n° 2, Février 2014, comm. 22, note Éric A. Caprioli.

(29) Sur la décision du tribunal d'instance d'Epinal, v. Comm. Com. Electr. 2013, Avril, com. 47, note E. Caprioli

Par conséquent, la preuve de la signature par monsieur X de l'avenant du 4 septembre 2008 est rapportée, contrairement à ce qu'a jugé le tribunal. »

Ces éléments démontrent l'importance de l'administration de la preuve devant le tribunal.

En outre, dans le cadre du recouvrement de créances, plusieurs Cours d'appel ont reconnu la valeur juridique de la signature électronique « *simple* » pour établir un pouvoir [30].

Selon la Cour d'appel de Caen : « *Il importe peu que les dispositions du décret du 30 mars 2001 n'aient pas été respectées* ***dès lors qu'elles n'ont d'implication que sur la charge de la preuve, la fiabilité du procédé imposée par le décret (du 30 mars 2001) étant présumée jusqu'à preuve contraire, tandis que la signature électronique simple doit être démontrée par son auteur.*** » Preuve qui a été rapportée et reconnue en l'espèce.

Au sujet d'un pouvoir électronique donné à un mandataire judiciaire, la Cour d'appel de Nîmes dans un arrêt du 1er octobre 2015 rappelle à nouveau que « *le principe n'est pas qu'à défaut de respecter les exigences du décret la signature est sans valeur mais seulement que la fiabilité du procédé n'est pas présumée* ».

La Cour d'appel confirme ici le jugement du Tribunal de commerce d'Aubenas et la validité du pouvoir électronique qui répondait bien aux critères de fiabilité portant sur l'identification de son auteur et sur l'immutabilité de son contenu imposés par les dispositions de l'article 1316-1 du Code civil, dès lors que le support de transmission électronique utilisé respecte les règles relatives à la souscription des contrats en ligne, par l'utilisation de codes sécurisés.

On notera, en l'espèce, le caractère déterminant du versement aux débats du procès-verbal de constat d'huissier dans la démonstration de la validité du pouvoir électronique et on soulignera donc à nouveau l'importance de l'administration de la preuve devant le tribunal [31].

Plusieurs méthodes peuvent être retenues, et elles varieront en fonction des risques

(30) V. CA Aix en Provence, 26 juin 2014, Comm. Com. Electr. n° 11, Novembre 2014, comm. 90, note E. Caprioli ; La cour d'appel a considéré qu'un pouvoir signé électroniquement était recevable en s'appuyant sur un constat d'huissier de justice venant constater la fiabilité du processus permettant de réaliser un pouvoir en ligne décrivant minutieusement les différentes étapes de validation comprenant l'ensemble du processus par des captures d'écran parlantes tout en étant connecté dans les conditions d'un utilisateur réel et sur une attestation émanant du mandant où ce dernier reconnaît avoir signé la demande de pouvoir électronique au profit de la société de recouvrement de créance ; v. égal. CA Caen, 5 mars 2015. RG n°13/03009, commentaire E. Caprioli, Comm. Com. Electr. n° 5, Mai 2015.

(31) V. CA Nîmes, 1er octobre 2015, Comm. Com. Electr n°2, février 2016, comm. 20, note E. Caprioli. V. aussi en ce sens CA Toulouse, 3e ch., 9 décembre 2015, n°15/01828, SA TKB c/ SARL Chevalier Diffusion.

(litige isolé, action de groupe, contrôle du régulateur).

Enfin, la 1ère chambre civile de la Cour de cassation a eu à juger d'un cas où un individu déniait la signature électronique d'un bulletin d'adhésion à un contrat d'assurance complémentaire : « *que le jugement retient que la demande d'adhésion sous forme électronique a été établie et conservée dans des conditions de nature à garantir son intégrité, que la signature a été identifiée par un procédé fiable garantissant le lien de la signature électronique avec l'acte auquel elle s'attache, et que la demande d'adhésion produite à l'audience porte mention de la délivrance de ce document par la plate-forme de contractualisation en ligne [… ;] permettant une identification et une authentification précise des signataires en date du 25 mai 2011* » et reconnaissant ainsi la valeur probatoire à une signature électronique simple [32].

De même, la Cour d'appel de Chambéry [33] a rendu une décision qui valide le procédé de signature électronique d'un contrat de crédit, en se fondant sur le fichier de preuve fourni par un prestataire de service de confiance qualifié. Dans cette affaire, Carrefour Banque rapportait la preuve de l'existence du contrat par un fichier de preuve de transaction émanant du prestataire, prestataire de service de confiance qualifié au sens du Règlement eIDAS n° 910/2014.

Dans cet arrêt, les juges font explicitement référence à la synthèse du fichier de preuve de la transaction qui indique l'adresse électronique du souscripteur et le code d'identité du certificat électronique permettant d'établir la fiabilité du procédé de signature électronique.

Cette décision place ainsi le prestataire de service de confiance au cœur du procès judiciaire en matière de signature électronique. Dans une telle perspective, il est recommandé de préciser les conditions entourant le recours à ce prestataire en cas de litige portant sur un contrat électronique mais aussi les modalités de restitution et de production d'un tel contrat en mettant en place un macro-process contentieux.

(32) V. CA Aix en Provence, 26 juin 2014, Comm. Com. Electr. n° 11, Novembre 2014, comm. 90, note E. Caprioli ; La cour d'appel a considéré qu'un pouvoir signé électroniquement était recevable en s'appuyant sur un constat d'huissier de justice venant constater la fiabilité du processus permettant de réaliser un pouvoir en ligne décrivant minutieusement les différentes étapes de validation comprenant l'ensemble du processus par des captures d'écran parlantes tout en étant connecté dans les conditions d'un utilisateur réel et sur une attestation émanant du mandant où ce dernier reconnaît avoir signé la demande de pouvoir électronique au profit de la société de recouvrement de créance ; v. égal. CA Caen, 5 mars 2015. RG n°13/03009, commentaire E. Caprioli, Comm. Com. Electr. n° 5, Mai 2015.

(33) CA Chambéry., 2ème ch., 25 janvier 2018, n°17/01050 FM/SD ; Éric A. Caprioli, « Nouvelle décision sur la preuve et la signature électronique d'un contrat de prêt personnel » Comm. com. électr. 2018 comm. 39.

(34) TI Nîmes 18 sept. 2018 CA Consumer Finance SA / Mme X, disponible sur le site www.legalis.net.

Dans le même sens, le Tribunal d'instance de Nîmes a reconnu la validité d'un contrat de crédit à la consommation signé électroniquement, et dont la preuve de la fiabilité du procédé utilisé était rapportée à l'appui d'une synthèse du fichier de preuve émanant du prestataire de services de certification électronique [34].

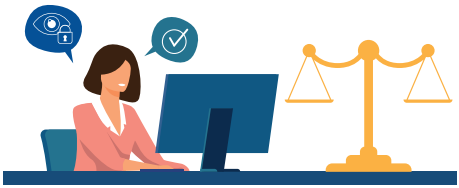
Ce prestataire avait en outre produit au profit de l'établissement de crédit une attestation de fiabilité de ses pratiques au sens du décret du 30 mars 2001. Fort de ces deux documents, le juge d'instance a pu constater l'authentification de la signature électronique du client et la preuve de l'existence du contrat électronique.

Cette décision rendue par des magistrats de première instance permet de considérer que, progressivement, les juges sont de plus en plus au fait de ces pratiques qui doivent être intégrées dans la stratégie judiciaire des entités utilisatrices de telles solutions et des prestataires les proposant.

Par ailleurs concernant les obligations qui engagent le signataire d'un contrat électronique, il conviendra de veiller à ce que les clauses dudit contrat ne soient pas contradictoires avec tous les autres contrats subséquents, et notamment les Conditions générales d'utilisation du service de signature électronique [35].

La jurisprudence en matière de fichier de preuve s'affine au fur et à mesure [36] en identifiant les pièces à apporter par les acteurs pour justifier de l'existence d'un contrat (fichier de preuve créé par un prestataire de services de certification électronique). En outre, certaines décisions prennent en compte des éléments extrinsèques à la signature établissant l'exécution du contrat [37].

D'autres cas d'usage sont concernés par la signature électronique : cession de parts sociales, bail, contrat de travail [38].



(35) Sur la qualité d'une partie qui croyait effectivement disposer de la qualité de co-emprunteur, une Cour d'appel a considéré que : « Madame X était justement fondée à croire qu'elle ne signait qu'en qualité de conjointe de l'emprunteur et non en qualité de co-emprunteur » en raison de contradictions entre le contrat d'assurance et les CGU du service de signature électronique ; CA Colmar, 3ème ch., 26 novembre 2018, n° 17/02457 (non disponible).

(36) CA Paris, ch. 9, 2 sept. 2021, n° 20/01043 , Sté Banque du Groupe Casino, Comm. com. électr. 2021, comm. 77, note Éric A. Caprioli. ; CA Toulouse, 2e ch., 6 janv. 2021, n° 19/02687, inédit : Comm. com. électr. 2021, comm. 26, note Éric A. Caprioli ; CA Rouen, ch. proximité, 4 mars 2021, n° 20/01275 : Comm. com. électr. 2021, comm. 41, note Éric A. Caprioli.

(37) Éric A. Caprioli, La signature électronique dans certains contrats bancaires, in Droit bancaire et financier, Mélanges AEDBF VIII, ss la dir. de Bertrand Brehier, Rev. Banque éd., p.315 s.

(38) V. pour la requalification du CDD en CDI : CA Amiens, 5ème ch., 30 septembre 2021 et CA Douai, cn. Soc., 22 octobre 2021, Comm. com. élect. 2021, comm 99, note Éric A. Caprioli.

D'autres procédés de signature électronique émergent sur le marché comme **les signatures électroniques fondées sur un certificat de cachet**. De nombreuses questions font jour sur ce nouveau process comme les modalités de garantie d'identité et de lien entre la personne qui recourt au cachet de signature (et qui n'est pas le titulaire du certificat de cachet) et le document ainsi scellé.

En outre, désormais, **certaines solutions n'utilisent pas du tout de certificat** (de cachet ou de signature). Les questions relatives à l'intégrité du document mais aussi au lien entre le signataire et le document « *signé* » n'ont pas encore été traitées expressément par la jurisprudence. Gageons que les juges appréhenderont ces solutions avec – en tête – le respect des exigences figurant à l'article 1367 du Code civil.

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** (sauf si elle est fiable selon l'ordonnance du 10 février 2016).

Le titre original

Il se définit comme étant un « *écrit dressé, en un ou plusieurs exemplaires, afin de constater un acte juridique, signé par les parties à l'acte (ou par leur représentant) à la différence d'une copie* » [39].

L'ordonnance du 16 juin 2005 [40] prise en application de l'article 26 de la LCEN a consacré juridiquement une nouvelle fiction juridique, l'exemplaire d'un original sous forme électronique : « *L'exigence d'une pluralité d'originaux est réputée 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 ancien du Code civil).

(39) Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 9ème édition mise à J.O.ur « Quadrige » : août 2011. V° Original.

(40) Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique, J.O. du 17 juin 2005, p.10342.

Cet article renvoyait aux articles 1316-1 et 1316-4 anciens du Code civil déjà cités pour les écrits requis à titre de validité (art. 1108-1 ancien du Code civil). 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.

L'ordonnance du 10 février 2016 modifie les dispositions de l'article 1325 du Code civil et les intègre à l'article 1375. D'une part, son alinéa 1er pose clairement l'exigence d'une condition de preuve, et non de validité, de l'acte sous signature privée. D'autre part, la jurisprudence constante selon laquelle les parties peuvent valablement convenir de la remise de l'exemplaire original unique entre les mains d'un tiers est consacrée [41]. Ainsi, l'exigence de pluralité d'originaux est réputée satisfaite pour un acte sous seing privé portant promesse de vente non établi en double exemplaire mais déposé entre les mains d'un notaire par les parties[42].

De plus, l'alinéa 4 de l'article 1375 du Code civil reprend dans sa globalité la formulation de l'alinéa 5 de l'article 1325 en y ajoutant néanmoins une exigence substantielle.

En effet, le procédé utilisé pour respecter la condition de pluralité d'originaux doit permettre à chaque partie de « *disposer d'un exemplaire sur support durable ou d'y avoir accès* ».

Par analogie avec l'article L. 311-7 [43] du Code monétaire et financier (CMF), on pourrait définir un tel support durable comme tout instrument permettant de stocker l'exemplaire original d'une manière telle que ce dernier puisse être consulté ultérieurement pendant une période adaptée à sa finalité et reproduit à l'identique.

La copie

Elle se définissait 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 ancien du Code civil, mais dont la valeur est reconnue à des fins spécifiées (not. pour les notifications), sous les conditions de la loi (copies établies par des officiers publics compétents, copies certifiées conformes etc.)* [44]».

Selon l'article 1348 alinéa 2 ancien du Code civil, **à défaut d'original**, la copie, pour pouvoir être retenue par les juges, devait être « *la reproduction non seulement fidèle mais aussi durable* » du titre original [45].

(41) En ce sens : Cass. req., 16 mai 1938 : Gaz. Pal. 1938, 2, p. 332. – Cass. 1re civ., 17 oct. 1955 : Gaz. Pal. 1955, 2, p. 394. – Cass. 1re civ., 19 juin 1957 : Bull. civ. 1957, I, n° 291.

(42) V. Cass. 3e civ., 7 juin 2006, n°05-11.936.

(43) L'article L. 311-7 du CMF dispose que « Constitue un support durable, au sens du présent titre, tout instrument offrant au client ou au professionnel la possibilité de stocker des informations qui lui sont adressées personnellement afin de pouvoir s'y reporter ultérieurement pendant un laps de temps adapté aux fins auxquelles les informations sont destinées, et qui permet la reproduction à l'identique des informations conservées ».

(44) V. G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2011. V° Copie.

(45) Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2011. V° Titre. « 2. Écrit en vue de constater un acte juridique ou un acte matériel pouvant produire des effets juridiques (instrumentum) ».

Cette notion de fidélité disparaît avec l'article 1379 du Code civil pour être remplacée par la fiabilité.

Ainsi, désormais, l'article 1379 du Code civil pose le principe selon lequel « ***la copie « fiable » a la même force probante que l'original*** ». Il dispose : « *est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret (…). Si l'original subsiste, sa présentation peut toujours être exigée.* ».

Selon l'article 1er du décret du 5 décembre 2016 [(46)], la fiabilité de la copie est présumée lorsqu'elle résulte :

+ Soit d'un procédé de reproduction qui entraîne une modification irréversible du support de la copie ;
+ Soit, en cas de reproduction par voie électronique, d'un procédé qui répond aux conditions prévues aux articles 2 à 6 dudit décret.

L'intégrité est - quant à elle - définie par l'article 3 du décret du 5 décembre 2016 précité, comme suit : « *L'intégrité de la copie résultant d'un procédé de reproduction par voie électronique est attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable.*
Cette condition est présumée remplie par l'usage d'un horodatage qualifié, d'un cachet électronique qualifié ou d'une signature électronique qualifiée, au sens du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur ».

Les notions de fiabilité et d'intégrité des copies numériques pourront être implémentées grâce notamment à la norme NF Z 42-026 [(47)] qui couvre la définition et les spécifications des prestations de numérisation fidèle de documents sur support papier et prévoit le contrôle de ces prestations.

On assiste à une véritable consécration de la copie fiable électronique et à la confirmation de la possible destruction de l'original papier après avoir procédé à une numérisation à valeur probante. Le rapport au Président de la République sur l'ordonnance du 10 février 2016 le confirme expressément : « *peu important que celui-ci (l'original) subsiste ou pas, et peu important l'origine, le cas échéant de la disparition de l'original*. [(48)]» .

(46) Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du Code civil, J.O. 6 décembre 2016. Éric A. Caprioli, Caractéristiques du procédé permettant de présumer la fiabilité de la signature électronique, (Décret du 28 septembre 2017), JCP. éd. G, n°41, 9 octobre 2017, 1047.

(47) V. en ce sens l'Avis d'expert de la FnTC sur ce sujet : https://FnTC-numerique.com/upload/Communiques_de_presse_pdfs/CP_FnTC_NumFide%CC%80leNZ_0417.pdf.

(48) Rapport au Président de la République relatif à l'ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, J.O. du 11 février 2016.

b. La jurisprudence et la copie électronique d'un document papier

Concernant la valeur probatoire de la copie électronique d'un document, la question a fait l'objet de deux décisions importantes de la deuxième chambre civile de la Cour de cassation rendues à trois ans d'intervalle :

La décision du 4 décembre 2008 [49]

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.

La décision du 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 [50] valide l'analyse de la Cour d'appel dans cette affaire :

(49) Cass. civ. 2ème, 4 décembre 2008, SNC Continent France c/ CPAM de la Marne, pourvoi n° 07-17.622, Note Éric Caprioli, Comm., Com. Electr. (Lexisnexis), février 2009, n°19, p. 44 et s.

(50) 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.

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) conformément à la version du Code applicable au moment des faits. Toutefois, cette « *réplique* » associée aux mentions inscrites sur l'accusé de réception, voit sa force probante reconnue.

En outre, la troisième chambre de la Cour d'appel de Lyon a considéré dans un arrêt du 3 septembre 2015 que les photocopies des originaux fournies par un établissement bancaire étaient des copies fidèles et durables au sens de l'article 1348 al.2 [51].

En effet, un établissement bancaire n'était plus en mesure de produire l'original des contrats, un système d'archivage électronique répondant aux spécifications et exigences de la norme AFNOR NF Z42-013 ayant été mis en place. Cette décision a donc admis la fiabilité d'un système de gestion électronique des documents mis en œuvre conformément à la norme AFNOR NF Z42-013 et le caractère fidèle et durable des copies produites [52].

Notons que dans un arrêt similaire de la Cour d'appel de Paris du 11 février 2016, la production d'une attestation de l'audit confirmant le respect des exigences de ladite norme a notamment permis d'emporter la conviction du juge sur la force probante des copies versées aux débats [53].

(51) CA Lyon, 6e ch., 3 sept. 2015.

(52) Pour aller plus loin : V. E. Caprioli, archivage des copies numériques : Comm. com. électr. novembre 2015, n°11, comm. 95.

(53) CA Paris, 9e ch., 11 février 2016, Comm. com. électr. mai 2016, n°5, comm. 47, note E. Caprioli.

On relèvera donc l'importance pour les sociétés ayant mis en place un dispositif d'archivage électronique, et n'ayant pas conservé les originaux papiers, de réaliser des audits de conformité et se préconstituer ainsi la preuve du respect de l'état de l'art pour pouvoir attester de la fiabilité des copies produites. À défaut, les copies produites ne constitueront qu'un commencement de preuve par écrit [54].

En effet, en l'absence de conservation de l'original, les juges prennent en compte l'ensemble des éléments versés aux débats pour apprécier le caractère fidèle et durable d'une copie [55].

En revanche, la Cour d'appel de Lyon dans un arrêt du 4 juillet 2014 n'a pas tenu compte de la production de telles attestations, dans la mesure où celles-ci ne suffisaient pas à justifier la non-conservation des originaux papiers et qu'en outre, les copies n'avaient pas été versées aux débats [56].

Les juges ont appliqué l'article 1348 al. 1 du Code civil (alors applicable) qui justifiait la perte de l'original par un cas fortuit ou de force majeur sans tenir compte de l'exception de l'alinéa 2 qui traitait quant à lui de la production d'une copie fidèle et durable en l'absence de conservation de l'original.

Concernant la force probante de la copie numérique en matière bancaire, dans un arrêt du 11 février 2016, la Cour d'appel de Paris [57] a reconnu la valeur probatoire des photocopies de la convention d'ouverture du compte et de l'offre préalable de crédit issues d'un **système d'archivage électronique conforme à la norme AFNOR NF Z 42-013**.

(54) V. CA Paris, 9e ch., Pôle 4, 5 mars 2015, pour l'absence de respect de la norme AFNOR NF Z42-013 après examen des copies versées aux débats (absence de numérisation EURO-GDS et absence d'attestation d'audit). « Que les copies de contrats versées aux débats n'apparaissent pas comme des reproductions indélébiles d'originaux au sens de l'article 1348 alinéa 2 du Code civil ; Considérant qu'une copie peut cependant valoir commencement de preuve par écrit s'il s'agit de la copie de l'acte qu'on veut prouver. ».

(55) V. en ce sens CA Douai, 3e ch., 4 avril 2013 « En considération de l'ensemble de ces éléments, c'est à juste titre que les premiers juges ont considéré que les documents fournis par la banque et la compagnie d'assurances constituaient des reproductions fidèles et durables des actes originaux. ».

(56) V. en ce sens CA Lyon, 6e ch., 4 juillet 2014 : « Attendu que la production par la Caisse de Crédit Mutuel de Roanne de l'attestation d'audit NF Z 42013 du 2 juillet 2013 ne suffit pas à démontrer l'existence du cas fortuit qu'elle allègue ; qu'il n'est en effet nullement démontré que les trois offres de crédit litigieuses ont été égarées durant la mise en place par le groupe bancaire d'un système de dématérialisation et d'archivage électronique de documents conforme à la norme NF Z 42-013 ».

(57) CA Paris (Pôle 4, chambre 9), 11 février 2016, n°15/01765.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

La production par la banque de l'attestation d'audit qui confirmait le respect des recommandations de ladite norme a été relevée par le juge. En effet, ces copies conformes à l'image du document d'origine et au contenu desdits documents étaient parfaitement lisibles et exploitables et constituaient donc une preuve écrite suffisante au sens des articles 1316-1 et 1348 al.2 du Code civil (en vigueur alors). De plus, la Cour relève également le versement aux débats de la liste des mouvements en complément de ces copies, dont la production suffisait à elle seule à attester de la réalité de la créance de la banque.

Compte tenu de possibles interprétations divergentes eu égard à la réticence de certains juges, en pratique, nombreux étaient les professionnels qui attendaient une confirmation dans les textes de la reconnaissance élaborée par certains tribunaux d'une équivalence entre les documents numérisés ou des documents imprimés à la suite de l'émission du document par voie électronique et des originaux [58].

Cependant, à l'exception d'un léger infléchissement dans le cadre de la gestion du Registre National du Commerce et des Sociétés [59] il aura fallu attendre l'ordonnance du 10 février 2016 pour que les pouvoirs publics reconnaissent l'équivalence probatoire de la copie fiable numérique avec l'original [60].

Concernant l'importance des normes, dans un arrêt du 14 juin 2018, la Cour d'appel de Lyon [61] a reconnu l'admissibilité des copies numérisées d'une convention de découvert de compte à titre de preuve. Une banque avait assigné un souscripteur en paiement de sommes non acquittées. L'existence et la validité de la convention de découvert de compte et les autres crédits ont été constatées par les juges au motif qu'il s'agissait de « *reproductions fidèles et durables* » au sens de l'article 1348 alinéa 2 (ancien) du Code civil, pièces résultant de la « *numérisation des originaux réalisée conformément à la norme AFNOR NF Z42-013* ».

Aujourd'hui, plus rien ne s'oppose donc à la production de copies numérisées devant les juridictions, permettant aux organisations de procéder à la destruction de leur originaux papier après les avoir numérisés sous réserve de respecter les normes Z 42-026 et Z 42-013.

(58) V. en ce sens, FnTC, le Guide du Document Hybride et de la Certification 2D (nov. 2011).

(59) Décret n° 2012-928 du 31 juillet 2012 relatif au registre du commerce et des sociétés, J.O. du 2 août 2012, dont la notice précise notamment « […] l'INPI a pour obligation de centraliser au RNCS l'ensemble des doubles originaux des RCS tenus par les greffiers des tribunaux de commerce et des tribunaux civils statuant commercialement. Il pourra désormais archiver électroniquement les documents reçus des greffes. Ces documents, qui ne sont plus matériellement des doubles, sont assimilés à des originaux. […] »

(60) Voir supra.

(61) CA Lyon, 14 juin 2018, n° 17/05750 .

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 validité de la signature électronique, du cachet électronique le plus tôt possible après son apposition sur l'écrit sur support électronique et gérer dans le temps les traces des vérifications réalisées (cachet électronique, signatures du contrat, certificats, chemin de confiance). Cela permet d'établir que les vérifications ont été effectuées au moment de la signature ou du cachet (horodatage et scellement du fichier) conformément aux textes en vigueur [62].

L'ensemble des traces collectées constitueront le fichier de preuve (V. Supra Chapitre I point 1.2). Ces opérations doivent 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. Elles devront être conservées. 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.

Toutefois, cette A.G.P. n'a pas prospéré dans les faits, certains prestataires étrangers évitant ainsi de matérialiser ici une prise directe de responsabilité technique.

Les tribunaux sont plus sensibilisés que jamais aux problématiques relatives à la force probante de la signature électronique.

Les tribunaux analyseront si le fichier de preuve permet d'établir la fiabilité du procédé de signature électronique, s'il est possible d'identifier le signataire (identité vérifiée) et dans quelle mesure le consentement a été exprimé.

Des recoupements au cas par cas pourront être effectués (par exemple les CGU du service de signature et le contrat) afin de corroborer les exigences du Code civil [63]. Les magistrats utilisent donc un faisceau d'indices que les prestataires de service de confiance doivent anticiper pour que la confiance dans leur solution soit la plus optimale possible.

Pour être produit en justice, le fichier de preuve devra être suffisamment intelligible pour un profane. Une synthèse du fichier de preuve peut donc être utilement jointe au fichier de preuve dans le cadre d'un litige.

(62) Les articles 1366 et suivants du Code civil et l'article 8 de l'ordonnance du 8 décembre 2005 (pour la sphère publique, voir infra II/).

(63) T.I. Bonneville jugement du 10 avril 2019, RG :11-18-000497.

Sommaire

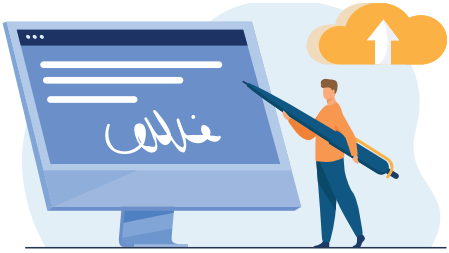
B. Le contrat par voie électronique (commande en ligne)

fntc

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

1. Le processus de contractualisation en ligne

Introduits par la LCEN [64], les articles 1369-4 (anciens) et suivants du Code civil dont la numérotation a été modifiée dernièrement par la Réforme 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. 1366 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 !) [65], dans l'hypothèse où le montant de l'opération est inférieur à 1 500 euros. Dans un but de protection des acheteurs, l'article 1127-1 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 au destinataire de l'offre, avant la conclusion du contrat, d'identifier d'éventuelles erreurs commises dans la saisie des données et de les corriger ;*
- *Les langues proposées pour la conclusion du contrat au nombre desquelles doit figurer la langue française ;*
- *Le cas échéant, les modalités d'archivage du contrat 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 ».*

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

Ensuite, l'article 1127-2 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.

(64) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O. du 22 juin 2004, p.11168 et s,. v. Ph. Stoffel-Munck, La réforme des contrats du commerce électronique, Comm. Com. Elect., 2004, Étude 30, E. A. Caprioli et P. Agosti, La confiance dans l'économie numérique, Les Petites Affiches, 3 juin 2005, p. 4 s.

(65) Par exemple en prévoyant que le clic de confirmation active une signature électronique fondée sur un certificat à usage unique ou à la volée.

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 pour choisir les produits), 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 « *cybercommerçant* » ; 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. 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 bouton mentionnant « *je confirme* » ou « *j'accepte* ». La manifestation du consentement de l'acheteur est l'élément fondamental 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 1127-2 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* ».

A côté de ces règles applicables aux transactions conclues par un particulier sur un site marchand, deux exceptions sont posées à l'article 1127-3 [66] 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.

Ceci étant précisé, l'article 1127-1 du Code civil impose de proposer la langue française parmi les langues pour la conclusion du contrat conclu par voie électronique. Il s'agit d'une consécration d'un état de l'art et d'une pratique déjà courante inspirée par la loi Toubon relative à l'emploi de la langue française [67].

(66) « Il est fait exception aux obligations visées aux 1° à 5° de l'article 1127-1 et aux deux premiers alinéas de l'article 1127-2 pour les contrats de fourniture de biens ou de prestation de services qui sont conclus exclusivement par échange de courriers électroniques. Il peut, en outre, être dérogé aux dispositions des 1° à 5° de l'article 1127-1 et de l'article 1127-2 dans les contrats conclus entre professionnels ».

(67) Loi n°94-665 du 4 août 1994 relative à l'emploi de la langue française.

2. Les services de paiement électronique

a. Généralités

Le paiement est « *l'exécution volontaire d'une obligation quel qu'en soit l'objet (versement d'une somme d'argent, livraison de marchandises…). Le paiement est un fait qui peut être prouvé par tous les moyens* [68] ». 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 puce et cartes sans contact), l'usage d'un logiciel et une connexion à un réseau de communication électronique (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 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 [69] 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 [70].

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 pour une somme supérieure à cinquante euros, et 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* [71] ».

(68) Voir Dalloz, Lexique des termes juridiques, 2011, Dalloz, 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.».

(69) Voir infra.

(70) Voir Y. Gérard, L'utilisation frauduleuse des instruments de paiement, JCP Entreprise et Affaire n°2, 14 janvier 2010, 1034.

(71) Article L. 133-18 du C.M.F.

Selon la jurisprudence, la preuve de la négligence grave de l'utilisateur incombe bien souvent à la banque [72]. Pour que cette négligence soit caractérisée, l'utilisateur doit a priori faillir à son obligation de préserver la sécurité de ses dispositifs de sécurité personnalisés [73] Cependant, la preuve de la négligence grave du client par la banque n'empêche pas que sa responsabilité contractuelle soit engagée à propos notamment du respect de la convention de compte de son client [74].

Le porte-monnaie électronique entre également dans cette catégorie. Des unités de valeur 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 [75] et modifié à deux reprises en 2007 [76] et 2009 [77] puis abrogé par l'arrêté du 2 mai 2013 portant sur la règlementation prudentielle des établissements de monnaie électronique [78].

Le 28 janvier 2013, la loi n° 2013-100 [79], transposant les dispositions de plusieurs directives et en particulier celles de la directive 2009/110/CE [80], a introduit non seulement la définition de la monnaie électronique au sein du Code monétaire et financier [81] mais également

(72) Voir Cass. com., 21 nov. 2018, n° 17-18.888, inédit, Éric. A. Caprioli, Négligence grave de l'utilisateur de services de paiement Comm. com. électr. 2019, comm. n° 13 ; Cass. com., 18 janv. 2017, n° 15-18.102, P+B+I , Éric A. Caprioli, La preuve de la négligence de l'utilisateur d'un service de paiement incombe à la banque, Comm. com. électr. 2017, comm. n° 39. Sur la négligence grave d'une victime d'hameçonnage, v. CA Colmar, 3ème ch. civ., 12 avril 2021 (2 affaires), Cass. com. 24 novembre 2021, Comm. com. électr. 2022, Comm. 15, note Éric A. Caprioli.

(73). Cass. com., 6 juin 2018, n° 16-29.065, V. Éric. A. Caprioli Responsabilité du particulier en cas d'hameçonnage, Comm. com. électr. 2018, comm. n° 68.

(74) Cass. com., 17 mai 2017, n° 15-28.209, V. Éric. A. Caprioli, La négligence grave du client ne l'empêche pas d'engager la responsabilité contractuelle de sa banque, Comm. com. électr. 2017, comm. 77.

(75) Arrêté du 10 janvier 2003 portant homologation du règlement n° 2002-13 du Comité de la réglementation bancaire et financière, J.O. du 1er février 2003, p. 2003.

(76) Arrêté du 20 février 2007 modifiant les règlements du Comité de la réglementation bancaire n° 90-02, n° 90-15, n° 91-05, n° 92-12, n° 93-05 et n° 95-02 et les règlements du Comité de la réglementation bancaire et financière n° 96-15, n° 97-02, n° 97-04, n° 98-04, n° 99-06, n° 99-07, n° 99-15, n° 99-16, n° 2000-03 et n° 2002-13, en application de l'arrêté du 20 février 2007 relatif aux exigences de fonds propres applicables aux établissements de crédit et aux entreprises d'investissement, J.O. du 1 mars 2007. Arrêté du 29 octobre 2009 relatif à la réglementation des établissements de monnaie électronique modifiant les règlements n° 92-14 du 23 décembre 1992 et n° 2002-13 du 21 novembre 2002, J.O. n°0253 du 31 octobre 2009.

(77) Arrêté du 29 octobre 2009 relatif à la réglementation des établissements de monnaie électronique modifiant les règlements n° 92-14 du 23 décembre 1992 et n° 2002-13 du 21 novembre 2002, J.O. n°0253 du 31 octobre 2009.

(78) Arrêté du 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique, J.O. du 4 mai 2013, p. 7651.

(79) Loi n° 2013-100 du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière économique et financière, J.O. du 29 janvier 2013.

(80) Directive 2009/110/CE 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, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE, J.O.U.E n° L 267/7 du 10 octobre 2009.

nombre de dispositions encadrant tour à tour l'émission et la gestion de monnaie électronique ainsi que les émetteurs et la distribution de monnaie électronique.

En outre, le décret n° 2013-383 du 6 mai 2013 pris pour l'application de la loi n° 2013-100 du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière économique et financière [82] modifie le Code monétaire et financier afin de transposer les dispositions de nature réglementaire de la directive 2009/110/CE 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.

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 sécurisés associant la messagerie électronique de l'internaute. Tel 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.

(81) Article L315-1 du code monétaire et financier : « I. - La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique. II. - Les unités de monnaie électronique sont dites unités de valeur, chacune constituant une créance incorporée dans un titre. »

(82) J.O. du 8 mai 2013 p. 7820.

b. Les apports de la Directive Services de Paiement 2

Notons, d'autre part, que la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n°1093/2010, et abrogeant la directive 2007/64/CE (DSP 2) a été transposée en droit français par l'ordonnance **n°2017-1252 du 9 août 2017**, suivie de la loi de ratification n°2018-700 du 3 août 2018 [83].

Ainsi, sont codifiées les exigences de la DSP 2 qui complètent les conditions d'octroi de l'agrément des établissements de paiement, à savoir des personnes morales autres que les établissements de crédit et de monnaie électronique qui fournissent à titre de profession habituelle des services de paiement, tels que les versements ou retraits d'espèces, les prélèvements, les opérations de paiement effectuées avec une carte, les virements, ou les transmissions de fonds.

Un agrément simplifié est ouvert aux établissements dont la moyenne mensuelle de la valeur totale des opérations de paiement est inférieure à 3 millions d'euros. Ces conditions s'appliquent également aux établissements de monnaie électronique.

Les pouvoirs de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) sont étendus.

Il est désormais possible pour elle de prendre des mesures conservatoires en cas d'urgence, pour un établissement agréé dans un autre État de l'Union européenne et exerçant en France. Ces mesures ont pour objectif de contrer une menace grave et immédiate qui contrevient aux intérêts des utilisateurs de ces services de paiement.

La DSP 2 met aussi à jour le marché SEPA qui reposait, dès la DSP 1 abrogée [84] sur trois éléments essentiels :

+ **Le droit de fournir des services de paiement au public** : l'objectif était d'harmoniser les conditions d'accès au marché applicables aux prestataires de services de paiement autres que les établissements de crédit [85].

+ **Les exigences de transparence et d'information** : la DSP 1 imposait 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* » [86]

(83) Loi n° 2018-700 du 3 août 2018 ratifiant l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (J.O. 5 août 2018).

(84) Directive abrogée 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE (J.O.UE n°L319/1, 5 déc. 2007).

+ **Les droits et obligations des utilisateurs et des prestataires de services** : la Directive visait enfin à clarifier les principaux droits et obligations des utilisateurs et des prestataires de services de paiement en harmonisant les règles nationales [87], ce qui aurait dû contribuer à un renforcement de la sécurité juridique.

Jusqu'alors, chaque État membre disposait de son propre secteur bancaire régi par ses propres règles et utilisant ses propres solutions technologiques.

La DSP2 met à jour ce service moins onéreux et plus sûr avec la possibilité de faire intervenir des services agréés comme les services d'initiation de paiement qui permettent le bon déroulement de l'opération entre l'utilisateur, la banque et le bénéficiaire.

Ces derniers services permettent aux utilisateurs de régler leurs achats en ligne par simple virement et garantissent l'initiation du paiement au bénéficiaire.

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 [88] qui fixe une échéance au 1er février 2014.

La norme « *SEPA Core Debit, Scheme Rulebook* », établie par l'EPC [90] 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). L'EPC publie régulièrement des lignes directrices sur ces différents points. La version 2021 SDD *Core rulebook* v. 1.1 publiée en novembre 2021 sera applicable jusqu'en novembre 2023.

La signature et les certificats électroniques ont 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.

(85) Art. 5 et s.

(86) Art. 30 et s.

(87) Art. 51 et s.

(88) 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, J.O.U.E. L. 94 du 30 mars 2012, p. 22–37 modifié par le Règlement (UE) n°248/2014 du parlement européen et du conseil du 26 février 2014 modifiant le règlement (UE) n° 260/2012 en ce qui concerne la migration vers un système de virements et de prélèvements à l'échelle de l'Union.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Les services de paiement pouvaient dès lors être proposés aussi bien par les banques que par des « *établissements de paiement* », dont le statut a été mis en place par l'ordonnance [89] .

Par ailleurs, le processus de paiement était 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.

Deux nouveaux services de paiement ont été reconnus et introduits par l'ordonnance n° 2017-1252 du 9 août 2017 et ceux-ci doivent désormais respecter les exigences de protection de données et de sécurité prescrites. Les services de paiement sont définis aux articles R. 314-1 et D. 314-1 du Code monétaire et financier et précisent l'article L. 314-1 du même code :

- Le service d'initiation de paiement (PSIP) [90] pour la réalisation de virements rapides, sûrs et peu onéreux ;
- Le service d'information sur les comptes (PSIC) [91] (ou agrégateurs de paiement) qui permettent aux utilisateurs d'avoir une vue d'ensemble sur l'état de leurs finances.

Ainsi, les agrégateurs [92] ont vu leur existence consacrée et l'obtention d'un agrément (article 5) et un enregistrement auprès des autorités nationales compétentes (ACPR en France) leur sont imposés. De plus, l'article 36 de la directive détermine que les établissements de paiement doivent avoir un accès objectif, non discriminatoire et proportionné aux services de comptes de paiement des établissements de crédit [93].

En somme, les établissements bancaires auront l'obligation de transmettre à ces nouveaux acteurs les informations des comptes de leurs clients, ce qui ne les satisfait guère et pose question en termes de sécurité.

De plus, la DSP 2 a consacré le rôle de l'Autorité Bancaire Européenne (ABE) en matière de services de paiement.

(89) http://www.europeanpaymentscouncil.eu/index.cfm/sepa-direct-debit/sepa-direct-debit-core-scheme-sdd-core/.

(90) Article 4. 15) de la Directive (UE) 2015/2366 : un service d'initiation de paiement est un service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement.

(91) Article 4. 16) de la Directive (UE) 2015/2366 : un service d'information sur les comptes est un service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement.

(92) Les agrégateurs sont des prestataires de service de paiement permettant aux clients multi-bancarisés de bénéficier d'une version consolidée de l'ensemble de leurs comptes sur une seule interface.

(93) Article 36 de la Directive (UE) 2015/2366 du Parlement européen et du conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

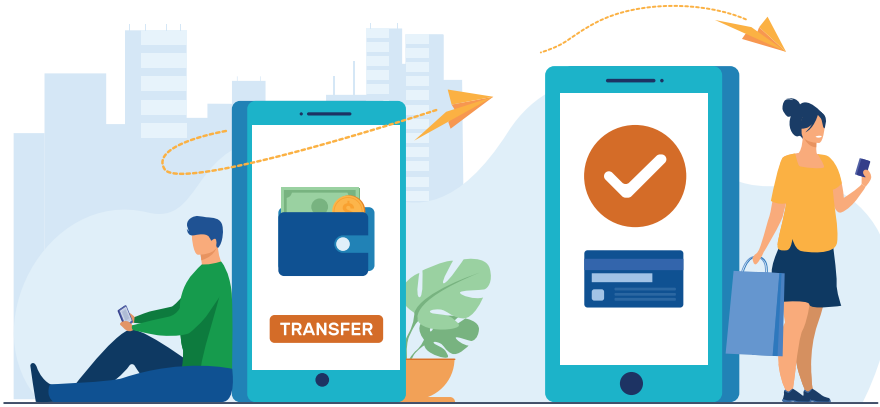
En outre, elle crée des obligations en termes de gestion des risques et de sécurité, met en place une procédure de notification des incidents et systématise l'authentification forte du client pour renforcer la sécurité pour les paiements électroniques et la protection des données financières des consommateurs. La mise en place de cette solution technique, peu faillible, est aussi un moyen de démontrer plus facilement la négligence grave du client quant à son obligation de préserver la sécurité de ses dispositifs de sécurité personnalisés en cas de prélèvement non autorisé [(94)] .

L'authentification forte pourra reposer sur l'utilisation de deux éléments ou plus appartenant aux catégories « *connaissance* » (quelque chose que seul l'utilisateur connaît), « *possession*» (quelque chose que seul l'utilisateur possède) et « *inhérence* » (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en cause la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification.

Ainsi, l'OTP SMS est progressivement abandonné au profit de solutions innovantes de la place bancaire.

L'ABE est chargée d'émettre des *guidelines* afin d'assurer la sécurité des nouveaux services de paiement, protéger les parties et les consommateurs contre le risque de fraude.

Le règlement n° 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, a quant à lui pour objet d'établir « *des exigences techniques et commerciales uniformes pour les opérations de paiement liées à une carte au sein de l'Union Européenne, à condition qu'y soient situés à la fois le prestataire de services de paiement du payeur et le prestataire de service de paiement du bénéficiaire* » [(95)].



(94) V. supra partie B. 2

(95) Article 1er du règlement (UE) n°2015/1751, , J.O.U.E n° L 123, 19 mai 2015, p.7.

Contrairement à la DSP 2, le règlement du 29 avril 2015 ne traite que des opérations liées aux cartes bancaires et plafonne les commissions interbancaires qui assurent le financement du système. Il favorise donc la concurrence et les relations transfrontalières en interdisant notamment les licences nationales et en imposant l'interopérabilité des systèmes des entités de traitement (opérateurs qui gèrent les flux au quotidien).

De plus, la hiérarchie des acteurs qui participent aux opérations de paiement liées à une carte a été redéfinie avec dans l'ordre les marques de paiement, les émetteurs de carte et les entités de traitement.

Le décret d'application du règlement relatif aux commissions d'interchange pour les opérations de paiement liées à une carte du 7 décembre 2015 limitait les commissions d'interchange exigées lors de chaque paiement par carte bancaire par les banques et autres prestataires de service de paiement à 0,23% de la valeur de la transaction jusqu'au 9 décembre 2016 (96).

À partir de cette date, la commission interbancaire de paiement devait être fixée à hauteur de 0,2 % pour les opérations par carte de débit et 0,3% pour les opérations par carte de crédit en France.

c. Évolution du Know Your Customer (KYC)

La 5ème directive LCB-FT (97) étend les obligations de la 4ème directive en matière de crypto-monnaies et de cartes prépayées. Elle étend également les prérogatives de l'ACPR en renforçant la coopération et l'échange d'informations entre superviseurs LCB-FT et entre superviseurs LCB-FT et prudentiels. Ainsi, la 5ème directive prévoit que soit mis en place l'accord multilatéral d'échange d'informations.

Les dispositions en matière d'élargissement du champ des obligations à certains prestataires des service liés aux crypto-actifs ont été transposées en droit français par la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite « *loi PACTE* » (98).

(96) Décret n° 2015-1591 du 7 décembre 2015 pris pour l'application de certaines dispositions du règlement (UE) n°2015/751 du Parlement européen et du conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, J.O. 8 décembre 2015, p.22525.

(97) Directive 2018/843 du 30 mai 2018 modifiant la directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (J.O.UE 19 juin 2018, n° L546/43).

(98) Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (J.O. 23 mai 2019).

Concernant ces prestataires de service de paiement (PSP), un règlement délégué est également entré en vigueur concernant la désignation d'un représentant permanent au sein des PSP européens exerçant dans un autre État membre en ayant recours à des agents ou des distributeurs de monnaie électronique.

Les modalités de cette désignation ont été précisées dans le décret n° 2019-490 du 21 mai 2019 [99]. Enfin, l'entrée en relation d'affaires a connu une évolution majeure depuis l'ordonnance n° **2016-1635** du 1er décembre 2016 **renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme** et transposant la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment des capitaux ou du financement du terrorisme [100].

Après de multiples évolutions réglementaires intervenues, dont la plus signifiante est le décret n° 2020-118 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme [101], les modalités propres à une vérification d'identité « *pleine et entière* » figurent à l'art. R.561-5-1 du CMF et prévoient notamment - de manière autosuffisante - le recours à :

- « *un moyen d'identification électronique certifié ou attesté par l'Agence nationale de la sécurité des systèmes d'information conforme au niveau de garantie soit substantiel soit élevé fixé par l'article 8 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, ou*
- *À un moyen d'identification électronique délivré dans le cadre d'un schéma notifié à la Commission européenne par un Etat membre de l'Union européenne dans les conditions prévues au paragraphe 1 de l'article 9 de ce règlement et dont le niveau de garantie correspond au niveau soit substantiel soit élevé fixé par l'article 8 du même règlement ;*

2° En recourant à un moyen d'identification électronique présumé fiable au sens de l'article L. 102 du Code des postes et des communications électroniques ; »

De plus, l'art. R. 561-5-2 du Code monétaire et financier précise les mesures de vigilance complémentaires à apporter pour fiabiliser un procédé d'entrée à relations à distance.

(99) Décret n° 2019-490 du 21 mai 2019 précisant les modalités de désignation du représentant permanent par les personnes mentionnées au 1° quater de l'article L. 561-2 du code monétaire et financier (J.O. 23 mai 2019).

(100) J.O. du 2 décembre 2016.

(101) J.O. du 13 février 2020.

En sus des mesures traditionnellement admises comme l'obtention d'une copie d'une pièce d'identité (ou un autre document), la mise en œuvre de mesures de vérification et de certification de la copie d'un document officiel ou d'un extrait de registre officiel par un tiers indépendant de la personne à identifier, le fait d'exiger que le premier paiement des opérations soit effectué en provenance ou à destination d'un compte ouvert au nom du client auprès d'une personne établie dans un État membre de l'Union européenne ou dans un État partie à l'accord sur l'Espace économique européen ou dans un pays tiers imposant des obligations équivalentes en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, ou l'obtention directe d'une confirmation de l'identité du client de la part d'un tiers remplissant les conditions prévues au 1° ou au 2° du I de l'article L. 561-7 du Code monétaire et financier, l'établissement bancaire pourra recourir comme mesure de vigilance renforcée, à savoir une entrée en relation à distance :

« (…)

5° Recourir à un service certifié conforme par l'Agence nationale de la sécurité des systèmes d'information, ou un organisme de certification que cette agence autorise, au niveau de garantie substantiel des exigences relatives à la preuve et à la vérification d'identité, prévues à l'annexe du règlement d'exécution (UE) 2015/1502 du 8 septembre 2015.

Un arrêté conjoint du Premier ministre et du ministre chargé de l'Économie précise les modalités d'application de ce 5° ;

6° Recueillir une signature électronique avancée ou qualifiée ou un cachet électronique avancé ou qualifié valide reposant sur un certificat qualifié ou avoir recours à un service d'envoi recommandé électronique qualifié comportant l'identité du signataire ou du créateur de cachet et délivré par un prestataire de services de confiance qualifié inscrit sur une liste de confiance nationale en application de l'article 22 du règlement (UE) n° 910/2014 du 23 juillet 2014. »

Ces deux mesures s'appuient directement ou indirectement sur le règlement eIDAS. Si le fait de recourir à un certificat qualifié dans le cadre d'une signature, d'un cachet ou d'un envoi recommandé qualifiés renvoie directement aux dispositions applicables du règlement eIDAS, le moyen d'identification électronique n'a pas à découler d'un schéma d'identification notifié dans le cadre du règlement eIDAS. En effet, la solution doit être certifiée conforme à certaines exigences de l'annexe du règlement d'exécution (UE) 2015/1502 du 8 septembre 2015 relatives à la preuve et à la vérification d'identité.

En outre, le KYC devrait s'appuyer prochainement sur des prestations de vérification d'identité à distance. Un service de vérification d'identité à distance a « *pour objectifs de réaliser l'acquisition et la vérification des données d'identification des utilisateurs afin de les identifier, de constituer le dossier de preuve et de transmettre le résultat de la vérification d'identité à distance au service métier* » [(102)].

(102) Référentiel d'exigences Prestataires de vérification d'identité à distance V.1.1 du 1er mars 2021, § I.3.

Le référentiel PVID a notamment pour vocation à être utilisé dans le cadre de :

- « *la* ***certification au titre du décret n° 2020-118 des services de vérification d'identité à distance (dits « services d'entrée en relation d'affaires à distance*** *») lorsqu'ils sont mis en œuvre par des organismes assujettis à la lutte contre le blanchiment de capitaux et le financement du terrorisme ;*
- ***la qualification*** *au titre du règlement eIDAS des services de confiance lorsque ces derniers recourent à une vérification d'identité à distance ;*
- ***l'évaluation de conformité*** *au titre du règlement eIDAS et la certification au titre de l'article L102 du CPCE des moyens d'identification électronique, pour les niveaux de garantie substantiel et élevé, lorsque ces derniers recourent à une vérification d'identité à distance ; la certification au titre de l'article L102 du CPCE des moyens d'identification électronique présumés fiables lorsque ces derniers recourent à une vérification d'identité à distance.[...]* » .

d.Crypto-monnaies et crypto-actifs

Le paiement électronique a subi une réelle révolution avec l'arrivée du Bitcoin ou d'autres crypto-monnaies (comme Litecoin, Namecoin, Peercoin, Ethereum), fondée sur l'usage d'outils cryptographiques (signature numérique, hachage cryptographique) appliqués sur des données échangées entre utilisateurs (*peer-to-peer*).

La validation d'une transaction en crypto-monnaie passe par la résolution d'un casse-tête numérique. Les établissements bancaires et certains États sont souvent hostiles à ce type de système, autocontrôlé (c'est-à-dire sans contrôle des autorités de régulation en la matière) et public. Pour rappel l'article L. 111-1 du Code monétaire et financier dispose que « *la monnaie de la France est l'euro* ».

Les crypto-actifs ne correspondent pas non plus à la définition de la monnaie électronique énoncée dans l'article L. 315-1 du Code monétaire et financier qui nécessite un agrément.

Ainsi, l'ACPR a adopté le 29 janvier 2014 la Position 2014-P-01 relative aux opérations sur les Bitcoins en France [(103)].

(103) Disponible à l'adresse ; http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Rappelant qu'elle est l'autorité chargée de délivrer les agréments aux prestataires de services de paiement, et donc en première ligne dans cet encadrement réfléchi de l'expansion du Bitcoin et consorts, l'ACPR indique que l'intermédiation dans l'opération d'achat/vente de Bitcoins relève de la fourniture de services de paiement, ce qui implique de disposer d'un agrément délivré par elle quand l'activité est exercée à titre habituel en France.

Si elle n'interdit pas le principe d'une telle conversion, elle rappelle que l'obtention de l'agrément nécessite de disposer d'un dispositif de contrôle interne et de mesure de vigilance en matière de lutte contre le blanchiment et le financement du terrorisme.

Les crypto-monnaies se définissent comme « *2° Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.* » au sens de l'article L. 54-10-1 du Code monétaire et financier [104].

Bien évidemment, cette définition admet les bitcoins [105] mais aussi les ethers, XMR (Monero) ou litecoin, c'est-à-dire tout crypto actif [106] renvoyant à une fonction de paiement.

> Elles restent des moyens d'échange, c'est-à-dire des « *vecteurs monétaires acceptés par des personnes pour s'acquitter contractuellement de leurs dettes d'échange. [Elles] ressemblent aux monnaies légales en ce sens qu'elles n'ont pas de valeur intrinsèque mais elles en diffèrent dans le sens où elles ne sont pas garanties par un émetteur mais surtout du fait qu'elles n'ont pas cours légal.* [107]».

D'ailleurs, certains commerçants dans des pays de plus en plus nombreux acceptent d'être payés en crypto-monnaies.

(104) Selon la Commission d'enrichissement de la langue française (J.O. du 23 mai 2017), par « cybermonnaie », on entend : « Monnaie dont la création et la gestion reposent sur l'utilisation des techniques de l'informatique et des télécommunications. Note : 1. Certaines cybermonnaies sont convertibles en monnaie régalienne via des plateformes d'échanges. 2. La cybermonnaie ne doit pas être confondue avec la monnaie électronique. 3. Le bitcoin est l'une des principales cybermonnaies. ». On ajoutera que sont déconseillés les termes « monnaie virtuelle » et « cryptomonnaie ».

(105) É A. Caprioli, Crypto-monnaies - La nature juridique du Bitcoin enfin précisée ! (T. com. Nanterre 26 février 2020), Comm. Com. Electr. Juin 2020, comm. 52.

(106) Pour une étude globale et précise sur cette question, v. D. Legeais, Blockchain et actifs numériques, Lexisnexis, Actualité, 2019, p.1.

(107) H. de Vauplane, Les nouvelles représentations monétaires : crypto-monnaies, stablecoins et monnaies digitales des banques centrales, RDBF, mai 2020, dossier 15.

Pour autant, la nature juridique du bitcoin n'est pas encore fixée [108], et ce même si la Cour de justice de l'Union européenne [109] a décidé qu'il n'était pas un bien corporel dès lors qu'il n'existe que sous la forme d'un code numérique [110].

Un des reproches fréquents relatif à ces crypto-monnaies a trait à l'absence de sécurité des plateformes d'échanges qui se font pirater les unes après les autres (Flexcoin, Mt.gox, Poloniex) avec des conséquences d'autant plus fortes pour les utilisateurs « *déposants* » qu'ils n'ont pas de garanties autres que purement contractuelles (et très limitées, voire inexistantes en pratique) contrairement aux monnaies « *officielles* » comme l'euro ou la livre sterling.

La loi PACTE a changé ce paradigme et a établi le régime juridique français des ICO [111].

Le Code monétaire et financier (CMF) comporte désormais un chapitre relatif aux « *émetteurs de jetons* » (art. L. 621-7, I ter du CMF nouveau).

Sont ainsi concernées :

+ Les ICO dont les jetons ne sont pas des instruments financiers mais sont « *utilitaires* » donc utilisés pour acquérir un produit ou un service ;
+ Les offres publiques de jetons dont les biens incorporels numériques s'apparentent à des titres financiers qui dépendent de la réglementation des titres financiers et soumis à l'AMF (règlement prospectus [112]). Les émetteurs de jetons dépendent du règlement général de l'AMF.

Le jeton (art. L. 522-2 du CMF) et l'offre au public de jetons (art. L. 552-3 du CMF) sont désormais définis. Ainsi, préalablement à toute offre au public de jetons, les émetteurs qui le souhaitent peuvent solliciter un visa optionnel de l'AMF (art. L. 552-4 et L. 552-5 nouveaux du CMF).

Des mesures de conformité avec les dispositions anti-blanchiment et anti-terrorisme sont ajoutées dans le cadre d'une offre au public de jetons ayant fait l'objet du visa de l'AMF et, sous certaines conditions, les émetteurs de jetons peuvent être assujettis aux obligations LCB-FT (art. L. 561-2, 7° ter nouveau du CMF).

(108) Le BTC interroge sur sa nature juridique : v. M. Roussille, Le bitcoin : objet juridique non identifié : Banque et droit 2015, n 159, p. 27 et s. ; M. Bali, Les cryptomonnaies, une application des blockchain technologies à la monnaie : RD bancaire et fin. 2016, comm. 8. – G. Bourdeaux, Propos sur les « crypto-monnaies » : RD bancaire et fin. 2016, dossier 39 ; T. Bonneau, Analyse critique de la contribution de la CJUE à l'ascension juridique du bitcoin, In Liber Amicorum Blanche Sousi. L'Europe bancaire, financière et monétaire : RB éd., 2016.

(109) CJUE, 22 octobre 2015, aff. C-264/14, Skatteverket c/. David Hedqvist.

(110) V. en ce sens, P. Théry, La propriété monétaire numérique : les bitcoins, JCP G, décembre 2017, dossier 9, p.41.
(111) Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (J.O. 23 mai 2019).

(112) Règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé, et abrogeant la directive 2003/71/CE (J.O.UE 30 juin 2017 n° L. 168/12).

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

L'AMF contrôle alors le respect par les émetteurs de jetons des obligations relatives au dispositif LCB-FT et dispose d'un pouvoir de sanction (art. L. 561-36, I, 2° du CMF nouveau). Un régime relatif aux prestataires de services sur actifs numériques (PSAN) est aussi créé : fourniture à titre de profession habituelle d'un ou plusieurs services sur actifs numériques, possibilité de solliciter un agrément auprès de l'AMF dans des conditions prévues par décret (art. L. 54-10-5, I nouveau du CMF).

L'AMF doit également publier la liste des PSAN agréés en précisant les services pour lesquels ils sont agréés (art. L. 54-10-5, VII nouveau du CMF).

La technologie sous-jacente des crypto-monnaies, la **technologie de la Blockchain**, reste faillible.

Les crypto-monnaies et leur relatif anonymat permettent notamment la commission d'infractions sur le Darkweb [113].

Cette technologie peut se définir comme ***un protocole ouvert*** visant à assurer ***la gestion décentralisée et cohérente de l'historique des transactions*** ou encore en matière de titres financiers et la création d'un dispositif d'enregistrement électronique partagé pour lesquels le droit européen n'impose pas de passer par un dépositaire central de titres (parts de fonds, titres de créances négociables, actions et obligations non côtées) [114].

(113) V. A ce propos Éric A. Caprioli, Une première condamnation aux USA pour la commission d'infractions sur le Dark Web, Comm. com. électr. 2017, comm. 68.

(114) Décret n° 2018-1226 du 24 décembre 2018 relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons (J.O. 26 déc. 2018) et Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

NOTES

Cet espace vous est dédié pour prendre des notes.

Sommaire

fntc

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

1. L'archivage électronique

Il convient de noter que la Proposition de Règlement eIDAS du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique du 3 juin 2021 – COM (2021) 281 final prévoit d'intégrer dans la prochaine version du Règlement eIDAS des dispositions spécifiques au service d'archivage électronique (SAE), qui jusque-là était l'un des grands oubliés du Règlement eIDAS. Ce faisant, le service défini devrait rejoindre les autres services de confiance. En outre, un SAE de niveau « *qualifié* » devrait également être reconnu.

En attendant les évolutions à venir, en droit interne, actuellement, 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* [115]».

Du point de vue juridique, il n'existe pas encore de définition de l'archivage électronique. Au niveau européen, la proposition de Règlement eIDAS entend le définir comme un « *service assurant la réception, le stockage, la suppression et la transmission de données ou documents électroniques afin de garantir leur intégrité, l'exactitude de leur origine et leurs particularités juridiques pendant toute la durée de leur conservation* » (art. 3 § 47 de la proposition).

Pour l'heure, au niveau national, seule une définition légale des archives applicable pour l'essentiel aux 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, y compris les données, 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* ».

En ce qui concerne le droit privé, la notion d'archivage électronique dans les textes juridiques s'attache plus aux exigences qui sont attendues des documents électroniques « *conservés* » qu'à une éventuelle approche descriptive des procédés et modalités à mettre en œuvre.

En conséquence, l'archivage électronique doit prendre en compte différents paramètres et chaque système d'archivage doit tenir compte de 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 [116] à mettre en œuvre en fonction

(115) Définition du Dictionnaire du multimédia, AFNOR, 1995.

(116) Voir en droit public, Politique et Pratiques d'archivage (sphère publique), version du 24 juillet 2006, disponible à l'adresse : http://opendata.girondenumerique.fr/OpenData/Doc_Archivage/ArchivageSecurise-P2A-2006-07-24.pdf. Cette politique est une trame qui doit être adaptée au contexte (exemple : collectivité territoriale, hôpitaux publics, établissements 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.

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…). Les développements qui suivent ne constituent donc que quelques-unes des pistes à intégrer dans le cadre de l'archivage électronique.

a. La nature des documents à archiver

L'archivage va concerner 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, bons de commande, bordereau de livraison, 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**[117].

Certains de ces documents sont spécifiquement traités dans la suite du présent Vade-mecum (voir le point I.D infra).

Les documents signés et les courriers électroniques illustrent toutefois, les problématiques de l'archivage électronique.

En ce qui concerne les **documents signés**, l'archivage d'un contrat signé répond essentiellement à deux finalités juridiques :

+ Prouver le contenu d'un acte juridique (articles 1366 et 1367 du Code civil) voire la constatation d'un fait juridique ;
+ Ou respecter une exigence de forme (article 1174 du Code civil relatif à la validité des actes juridiques conclus sous forme électronique).

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 en cas de litige). 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 1367 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.

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

En ce qui concerne la **gestion et l'archivage des courriers électroniques**, leur archivage doit être une préoccupation centrale de toutes les entités utilisant les courriers électroniques/mails comme moyens de communication, aussi bien en interne (salariés, actionnaires…) que vis-à-vis de l'extérieur (fournisseurs, clients, partenaires…).

En effet, 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 constituer des éléments de preuve, par exemple dans le cas d'un engagement contractuel ou de l'exécution du contrat, ce qui est particulièrement utile en cas de contentieux.

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

Une Politique de gestion et d'archivage des courriers électroniques[118] - 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.

b. Les durées de conservation

Les durées de conservation applicables doivent être appréciées selon la nature des documents concernés et selon la matière juridique dans laquelle ils sont utilisés et conservés. En ce sens, un même document peut être soumis à différentes durées de conservation légales.

Doivent également être prises en compte les durées de prescription des actions judiciaires. Ces dernières peuvent ainsi constituer des paramètres importants à connaître pour déterminer la durée de conservation « *utile* » des documents.

(118) Voir É. Caprioli, Gestion et archivage des mails : une problématique juridique délicate, disponible sur le site www.journaldunet.com - É. 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.

À cet égard, il est précisé que 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 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.

A titre d'illustration, l'article L.213-1 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° 2016-884 du 29 juin 2016 [(119)] **codifié à l'article D.213-1 du Code de la consommation** a ainsi fixé **le montant à 120 euros et le délai de conservation à dix ans à compter de la conclusion du contrat (D. 231-2)**, 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 l'article L.213-1 du Code de la consommation n'est pas applicable aux relations entre professionnels (B to B). Dès lors la durée fixée à l'article D.213-1 du Code de la consommation ne doit pas, de droit, être appliquée à ce type de relations.

Ceci étant précisé, au regard des prescriptions, en matière civile, la loi n° 2008-561 du 17 juin 2008 portant réforme de la prescription en matière civile [(120)] 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 [(121)] mais peut durer jusqu'à 20 ans (délai butoir [(122)]).

(119) Décret n° 2016-884 du 29 juin 2016 relatif à la partie réglementaire du code de la consommation (J.O. 30 juin 2016).

(120) J.O. du 18 juin 2008, p. 9856 et s. V. É. A. Caprioli, Les apports de la loi n° 2008-561 du 17 juin 2008 portant réforme de la prescription en matière civile, Comm. Com. Electr. n°12, Décembre 2008, comm. 141, p. 46 et s, disponible sur le site www.caprioli-avocats.com.

(121) Article 2224 du Code civil.

(122) Article 2232 du Code civil.

Les actions réelles immobilières continuent à se prescrire par 30 ans [123]. Il est à noter également que la loi prévoit la possibilité pour les parties d'aménager la prescription dans certains contrats [124].

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.

(123) Article 2227 du Code civil.

(124) 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. ancien et L. 218-1 nouveau issu de l'ordonnance du 14 mars 2016)) et avec les mutuelles (art. L. 221-12-1 du code de la mutualité) ».

Dès lors, les durées de conservation des documents et les délais de prescription ne se rejoignent pas forcément, comme le démontrent les exemples exposés dans le tableau ci-après.

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. 213-1 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) (exemple : 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 (exemple : 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 (art L.102-B LPF associé à l'article 169 du LPF).*	*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.*

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

TYPE DE DOCUMENTS	DÉLAI DE CONSERVATION	DÉLAI DE PRESCRIPTION
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).*
Relevés 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) (exemple : cf. convention de comptes bancaires).*
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.*	

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

TYPE DE DOCUMENTS	DÉLAI DE CONSERVATION	DÉLAI DE PRESCRIPTION
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 (art. L. 244-3 du Code de la sécurité sociale)* – *5 ans en cas de travail illégal (art. L. 244-11 du Code de la sécurité sociale)* – *2 ans concernant le paiement des majorations de retard (art. L. 244-3 du Code de la sécurité sociale)*	

c. Les modalités de conservation

Les modalités de conservation peuvent être prescrites par un texte qui impose des modalités spécifiques (exemple : comptabilité informatisée, factures électroniques ou EDI, documents liés au droit du travail…). À défaut, il faudra être en mesure de garantir les exigences juridiques de conformité au droit commun, applicables aux écrits électroniques et aux copies numériques, le cas échéant, et plus largement au régime probatoire des documents concernés, selon les règles applicables.

Il conviendra également de s'assurer que les modalités mises en place respectent les règles de protection des données personnelles conformément au RGPD, à la législation nationale, voire à la doctrine de la CNIL [125].

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 [126], 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 2020 précitée ou à la norme NF Z 42-020 relative au coffre-fort numérique [127].

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.

d. Le coffre-fort électronique

L'article L.103 du Code des Postes et des communications électroniques dispose que : *« Un service de coffre-fort numérique est un service qui a pour objet :*

> ***1° La réception**, le stockage, la suppression et la transmission de données ou documents électroniques dans des conditions permettant de justifier de leur intégrité et de l'exactitude de leur origine ;*
>
> ***2° La traçabilité des opérations** réalisées sur ces documents ou données et la disponibilité de cette traçabilité pour l'utilisateur ;*
>
> ***3° L'identification de l'utilisateur** lors de l'accès au service par un moyen d'identification électronique respectant l'article L. 102 ;*
>
> ***4° De garantir l'accès exclusif aux documents électroniques**, données de l'utilisateur ou données associées au fonctionnement du service à cet utilisateur,*
>
> → *suite*

(125) Par ex., à titre indicatif, la CNIL prévoyait que les données archivées soient supprimées ou anonymisées au-delà du délai mentionné dans la déclaration (cf. CNIL, délibération 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, J.O. 23 novembre 2005). V. plus récemment sur le sujet : CNIL, Guide pratique sur les durées de conservation, version juillet 2020, https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf

(126) 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. Ce label est en cours de révision.

(127) Guide FnTC « Vers le Relevé d'Identité du Coffre-fort Numérique », disponible sur le site www.FnTC.org.

→ *suite*

aux tiers autres que le prestataire de service de coffre-fort numérique, explicitement autorisés par l'utilisateur à accéder à ces documents et données et, le cas échéant, au prestataire de service de coffre-fort numérique réalisant un traitement de ces documents ou données au seul bénéfice de l'utilisateur et après avoir recueilli son consentement dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

5° De donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine, dans des conditions définies par décret.

Le service de coffre-fort numérique peut également proposer des services de confiance au sens du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Ce service de coffre-fort numérique peut bénéficier d'une certification établie selon un cahier des charges proposé par l'autorité nationale de la sécurité des systèmes d'information après avis de la Commission nationale de l'informatique et des libertés et approuvé par arrêté du ministre chargé du numérique ».

Le décret n° 2018-418 du 30 mai 2018 [(128)] précise les différentes notions que sont notamment la traçabilité des opérations réalisées sur les documents et données stockés, l'intégrité, la disponibilité et l'exactitude de l'origine des données et documents stockés, l'obligation d'information claire, loyale et transparente sur les modalités de fonctionnement et d'utilisation du service qui incombent au prestataire de coffre-fort numérique. Ces précisions sont codifiées aux articles R. 55-1 s. du Code des postes et des communications électroniques.

Le **Décret n° 2018-853 du 5 octobre 2018** fixe les **conditions de récupération des documents** [(129)] **et données stockés par un service de coffre-fort numérique**. Ces conditions sont codifiées aux articles D. 537 s. du Code des postes et communications électroniques. Le cahier des charges, que doit adopter l'ANSSI afin de connaître les modalités de certification des services de coffre-fort numérique, serait en cours de finalisation.

Ceci étant précisé, les prestataires de service de coffre-fort numérique devraient s'intéresser à la Proposition de modification du règlement eIDAS [(130)] qui fait du service d'archivage électronique défini, un service de confiance, afin de vérifier si leur positionnement juridique, opérationnel et technologique est susceptible, ou non, de relever de cette nouvelle catégorie de service de confiance.

(128) Décret n° 2018-418 du 30 mai 2018 relatif aux modalités de mise en œuvre du service de coffre-fort numérique (J.O. 31 mai 2018).

(129) J.O. 7 octobre 2018.

(130) Proposition de Règlement eIDAS du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique du 3 juin 2021 – COM (2021) 281 final .

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. 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 [131] (signature informatique par la saisie du code PIN dans les opérations avec carte bancaire).

La loi n° 2000-230 du 13 mars 2000 précitée [132] avait entériné la pratique des conventions sur la preuve en introduisant un article 1316-2 dans le Code civil disposant « *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* ».

À contrario, si une convention sur la preuve avait été conclue entre les parties, le juge devait l'appliquer mais encore fallait-il qu'elle soit valable étant précisé que certaines dispositions peuvent être réputées non écrites.

Bien évidemment, ces conventions sur la preuve ne doivent pas porter atteinte à des règles d'ordre public (exemple : 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.

De plus, elles doivent retranscrire la réalité technique d'un process ; une convention de preuve ne peut donc pas être décorrélée de ce qui se passe techniquement.

(131) Cass. civ. 1ère, 8 nov. 1989, n° 86-16.196, Sté Crédicas c/ Cassan : D. 1990, p. 369, note C. Gavalda.
(132) J.O. 14 mars 2000.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

L'ordonnance du 10 février 2016 a non seulement changé la numérotation, puisque les dispositions de l'article 1316-2 figurent désormais à l'article 1368 du Code civil mais le texte a également été modifié. En effet, l'article 1368 du Code civil dispose qu'« *À défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable* ».

On peut regretter la suppression des termes « *quel qu'en soit le support* » qui permettait d'éviter les divergences d'interprétation et posait à nouveau l'équivalence probatoire entre un écrit papier et électronique, l'essentiel résidant pour le juge dans la vraisemblance du titre.

De plus, l'ordonnance du 10 février 2016 est venue consacrer cette pratique tout en posant ses limites, mais qui sont identiques à celles qui existaient dans la jurisprudence.

En effet, le nouvel article 1356 du Code civil dispose que « *Les contrats sur la preuve sont valables lorsqu'ils portent sur des droits dont les parties ont la libre disposition. Néanmoins, ils ne peuvent contredire les présomptions irréfragables établies par la loi, ni modifier la foi attachée à l'aveu ou au serment. Ils ne peuvent davantage établir au profit de l'une des parties une présomption irréfragable.* »

On relèvera cette volonté de clarification du législateur qui a, en outre, intégré un nouvel article 1357 renvoyant directement l'administration judiciaire de la preuve et les contestations qui s'y rapportent aux dispositions du Code de procédure civile portant sur la preuve [133].

(133) On relèvera notamment l'article 287 du Code de procédure civile applicable en cas de dénégation ou de refus de connaissance portant sur un écrit ou une signature électronique : « Si la dénégation ou le refus de reconnaissance porte sur un écrit ou une signature électronique, le juge vérifie si les conditions, mises par les articles 1316-1 et 1316-4 du Code civil à la validité de l'écrit ou de la signature électroniques, sont satisfaites ».

Sommaire

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Actuellement, la digitalisation des documents et des échanges se répand dans tous les domaines juridiques ; les textes législatifs et règlementaires se multiplient comme dans le cadre des procédures civiles [134] et pénales, les jeux de hasard et paris en ligne, la billetterie électronique ou encore dans le droit des sûretés réelles et personnelles [135].

Nous avons pris le parti de ne développer que certains domaines d'application étant donné leur nombre et les changements qui s'opèrent régulièrement.

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 temporaire**, 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 sur la preuve ;

+ 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.

  À titre indicatif, la **signature du contrat** de mission est **d'ordre public**. S'il est établi sous forme électronique, il devrait donc être signé électroniquement. Son omission entraîne, à la demande du salarié, la requalification du contrat de mission en contrat de droit commun à durée indéterminée.

(134) V. notamment les articles 748-1 à 748-9 du CPC, modifiés à plusieurs reprises depuis le décret n°2005-1678 du 28 décembre 2005, comme par ex. le Décret n°2019-402 du 3 mai 2019 ou encore l'arrêté du 20 novembre 2020 relatif à la signature électronique des décisions juridictionnelles rendues en matière civile, J.O. du 22 novembre 2020 (É. A. Caprioli, Comm. com. électr. 2021, comm n°17).

(135) Ord. n° 2021-1192 du 15 septembre 2021 portant réforme du droit des sûretés, J.O. du 16 septembre 2021.

a. Le bulletin de salaire ou de paie

Il se définit comme le « *décompte détaillé des divers éléments de la rémunération du travailleur, obligatoirement délivré par l'employeur lors de la paie* » [136].

Dans sa rédaction issue de la loi n° 2009-526 du 12 mai 2009 [137] et modifiée par la loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels [138], 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.*

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.

Sauf opposition du salarié l'employeur peut procéder à la remise du bulletin de paie sous forme électronique, dans des conditions de nature à garantir ***l'intégrité, la disponibilité*** *pendant une durée fixée par décret et la* ***confidentialité*** *des données ainsi que leur accessibilité dans le cadre du service associé au compte mentionné au 2° du II de l'article L. 5151-6.*

Un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés détermine les modalités de cette accessibilité afin de préserver la confidentialité des données. Les mentions devant figurer sur le bulletin ou y être annexées sont déterminées par décret en Conseil d'État ».

L'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 est donc consacrée par le législateur. Mais elle est enfermée dans le respect de certaines modalités et des questions restent en suspens.

D'abord, le salarié doit être préalablement informé de la remise du bulletin de paie sous forme électronique par son employeur conformément à l'article D. 3243-7 du Code du travail. Ensuite, le salarié peut toujours refuser le recours au bulletin de paie par voie électronique. Toutefois, désormais, il est réputé avoir accepté la remise dématérialisée par défaut, et ce n'est que s'il a notifié son opposition que la remise par voie électronique ne pourra se faire ou devra cesser.

(136) V Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2011. V° Bulletin de paie.

(137) Loi n°2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, J.O. 13 mai 2009, p. 7920 ; É. A. Caprioli, La dématérialisation des bulletins de paie, Cahier de droit de l'entreprise n°4, juillet 2009, prat. 20.

(138) J.O. 9 août 2016.

De plus, 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 qualifiée, horodatage, signature avec un certificat de serveur/cachet électronique, 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 (cachet électronique ou certificat de serveur qui assure le scellement/intégrité du bulletin de paie). De son côté, le salarié n'a pas à signer la pièce.

Par ailleurs, en application de l'article D. 3243-8 du Code du travail, l'employeur doit déterminer les conditions dans lesquelles il garantit la disponibilité du bulletin de paie sous forme électronique pour le salarié, conformément aux durées fixées.

À cet égard, on notera que les conditions d'intégrité, de confidentialité et d'accessibilité posées également à l'article L. 3243-2 du Code du travail devront être garanties pendant cette durée. C'est pourquoi la mise en œuvre de la mise à disposition des bulletins de paie par voie électronique nécessite une analyse des modalités proposées par les prestataires en la matière, afin de s'assurer de la conformité légale de la solution concernée.

b. Le contrat de travail

Qu'il soit à durée déterminée ou indéterminée le contrat de travail est défini notamment 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, dans l'exécution du travail, d'un lien de subordination juridique du travailleur à l'employeur* » (139).

(139) Voir G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2011. V° Contrat de travail.

La dématérialisation de ce type de contrat permet de le transmettre par voie électronique et de l'intégrer directement dans les systèmes de gestion RH des entreprises. Cela entraîne 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. Avec la signature électronique du contrat, il faut faire attention au risque de requalification du CDD en CDI [140].

c. En matière de notes de frais

La loi n° 2018-1203 du 22 décembre 2018 [141] de financement de la sécurité sociale pour 2019 est venue introduire un article L. 243-19 du Code de la sécurité sociale qui oblige les employeurs à conserver, pendant au moins 6 ans à compter de la date à laquelle ils ont été établis ou reçus « *les documents ou pièces justificatives nécessaires à l'établissement de l'assiette ou au contrôle des cotisations et contributions sociales* ».

Le deuxième alinéa dispose que « *Lorsque les documents ou pièces sont établis ou reçus sur support papier, ils peuvent être conservés sur support informatique* ».

L'arrêté du 23 mai 2019 [142] fixant les modalités de numérisation des pièces et documents établis ou reçus sur support papier en application de l'article L. 243-16 du Code de la sécurité sociale impose donc que ces justificatifs soient reproduits à l'identique de la copie originale et sous format PDF ou PDF A/3.

La numérisation des justificatifs des notes de frais doit être sécurisée au moyen :

+ D'un **cachet serveur** fondé sur un certificat conforme, au moins, au référentiel général de sécurité de niveau une étoile ;
+ D'une **empreinte numérique** ;
+ D'une **signature électronique** fondée sur un certificat conforme, au moins, au référentiel général de sécurité de niveau une étoile ;
+ Ou de tout **dispositif sécurisé** équivalent fondé sur un certificat délivré par une autorité de certification figurant sur la liste de confiance française.

(140) V. Plusieurs décisions ont entraîné la requalification d'un CDD en CDI pour défaut d'écrit électronique, l'employeur ne rapportant pas la preuve permettant de justifier que le contrat avait bien été signé électroniquement (Cass. Soc., 14 nov. 2018, n°16-19.038 : JurisData n°2018-020153, Comm. Com. Electr. 2019, comm. 21 É. A. Caprioli. - CA Lyon, ch. Soc A, 25 nov. 2020, n°18/02313 : Comm. Com. Électr. 2021, comm. 25, É. A. Caprioli).

(141) Loi n° 2018-1203 du 22 décembre 2018 de financement de la sécurité sociale pour 2019 (J.O. 23 décembre 2018).

(142) J.O. 29 mai 2019

En définitive, lorsque la législation ne contient pas d'obstacle manifeste à la possibilité de recourir à la dématérialisation de certains documents ou des processus [143], les modalités de cette dématérialisation doivent être appréciées au regard des textes particuliers éventuellement applicables et, à défaut, au regard des principes juridiques généraux applicables soit à des fins de validité, soit à des fins de preuve.

2. La facture électronique dans l'entreprise [144]

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 [145]. Cette dernière a été ensuite transposée en droit français par l'article 17 de la loi de finances rectificative pour 2002 [146].

La directive 2006/112/CE du Conseil du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoutée [147] 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 directive modifiant la directive 2006/112 a été adoptée le 13 juillet 2010 [148].

(143) V. par ex., l'ordonnance n° 2014-699 du 26 juin 2014 portant simplification et adaptation du droit du travail, J.O. 27 juin 2014, qui a notamment permis, dans plusieurs situations spécifiques, une transmission « par tout moyen » de documents par l'employeur à l'inspecteur du travail ou à l'autorité administrative concernée.

(144) Le lecteur est également invité à prendre connaissance du Guide établi par la FnTC « La facture électronique à la portée de tous », publié sur son site en 2019 et accessible en ligne à l'adresse : https://FnTC-numerique.com/upload/file/guides-FnTC/Guide_la_facture_electronique.pdf. Par ailleurs, les aspects relatifs à la facturation électronique dans la sphère publique sont traités dans le II du présent Vade-mecum.

(145) J.O.C.E 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.

(146) Loi n°2002-1576 du 30 décembre 2002, J.O du 31 décembre 2002, p. 22070.

(147) J.O.U.E. L 347 du 11 décembre 2006, p. 1-118.

(148) 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, J.O.U.E L. 189 du 22 juillet 2010, p. 1 et s.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

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 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.

Depuis lors, ces dispositions ont fait l'objet d'une transposition par le biais de la loi de finances rectificative du 29 décembre 2012.

Dans l'intervalle, c'est l'article 17 de la loi de finances rectificative pour 2002 ainsi que le cadre règlementaire associé qui étaient applicables.

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.

De 2002 à 2013, la transmission de la facture électronique sur le territoire français ou entre Etats membres de l'Union européenne pouvait s'effectuer selon deux modalités sécurisées dont les conditions d'utilisation diffèrent :

+ La signature électronique des factures ;
+ L'échange de données informatisé (EDI ou « *Electronic Data Interchange* »).

Par le biais de l'article 62 de la loi de finances rectificative du 29 décembre 2012 [149], la transposition des dispositions de la directive 2010/45/UE [150] a été réalisée, en modifiant notamment l'article 289 du Code général des impôts (CGI) [151].

Ainsi, le V de l'article 289 du CGI a été entièrement modifié et rappelle désormais le principe d'égalité de traitement des factures papiers et électroniques en ce qu'il impose sans spécifier le support que « *L'authenticité de l'origine, l'intégrité du contenu et la lisibilité de la facture doivent être assurées à compter de son émission et jusqu'à la fin de sa période de conservation.* ».

(149) Loi n° 2012-1510 du 29 décembre 2012 de finances rectificative pour 2012, J.O. du 30 décembre 2012.

(150) 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, J.O.U.E L. 189 du 22 juillet 2010, p. 1 et s.

(151) Pour une étude détaillée des modifications issues de la loi de finance rectificative du 29 décembre 2012, voir : É. Caprioli, Les nouvelles règles fiscales applicables en matière de facturation électronique, Comm. Com. électr. n° 3, Mars 2013, comm. 36. É. Caprioli, P. Agosti, Les (r)évolutions juridiques de la facture électronique, Expertises des Systèmes d'information Mai 2013.

Cependant, l'apport essentiel de cette transposition est l'ajout à l'article 289 des VI et VII du CGI.

En effet, le VI dispose que « *Les factures électroniques sont émises et reçues sous une forme électronique quelle qu'elle soit. Elles tiennent lieu de factures d'origine pour l'application de l'article 286 et du présent article. Leur transmission et mise à disposition sont soumises à l'acceptation du destinataire.* ». Cette disposition permet ainsi le recours à d'autres modalités de facturation électronique que la signature électronique et l'EDI.

De plus, le VII est venu établir les règles nécessaires pour satisfaire aux conditions de l'article 289 V du CGI à savoir :

« 1° Soit sous forme électronique en recourant à toute solution technique autre que celles prévues aux 2° et 3°, ou sous forme papier, dès lors que des contrôles documentés et permanents sont mis en place par l'entreprise et permettent d'établir une piste d'audit fiable entre la facture émise ou reçue et la livraison de biens ou prestation de services qui en est le fondement ;

2° Soit en recourant à la procédure de signature électronique avancée définie au a) du 2° de l'article 233 de la directive 2006/112/CE du Conseil du 28 novembre 2006 précitée en ce qui concerne les règles de facturation. Un décret précise les conditions d'émission, de signature et de stockage de ces factures ;

*3° Soit sous la forme d'un message structuré selon une norme convenue entre les parties, permettant une lecture par ordinateur et pouvant être traité automatiquement et de manière univoque, dans des conditions précisées par décre*t ».

4° Une dernière voie de sécurisation a été ajoutée par la loi n°2022-1726 du 30 décembre 2022 : le recours à un cachet électronique qualifié au sens du Règlement eIDAS

Un arrêté du 7 janvier 2016 est venu préciser les modalités de numérisation des documents constitutifs des contrôles documentés et permanents mis en place par une entreprise mentionnés au 1° du VII de l'article 289 précité [152].

(152) Arrêté du 7 janvier 2016 relatif aux modalités de numérisation des documents constitutifs des contrôles documentés et permanents mis en place par une entreprise mentionnés au 1° du VII de l'article 289 du code général des impôts, J.O. du 31 janvier 2016.

Un nouvel article A. 102 B-1 du CGI détermine comment garantir le lien et la fiabilité entre la facture émise et la livraison ou la prestation qui en est le fondement.

Ainsi, le résultat de la numérisation permettant de conserver la facture pendant un délai de six ans doit être la copie conforme à l'original en image et en contenu (les couleurs devant être reproduites à l'identique), le document doit être conservé sous format PDF conforme au référentiel général de sécurité de niveau une étoile et faire apparaître les annotations sur le document papier. De plus, en cas de modification ou correction des données portées sur le document numérisé, seul le document corrigé et numérisé à nouveau est retenu comme pièce constitutive des contrôles précités.

En respectant ces préconisations, l'authenticité de l'origine, l'intégrité du contenu et la lisibilité de la facture (article 289 V du CGI) pourront être garanties. On relèvera donc ici l'importance pour les entreprises de mettre en place un système de conservation des documents à valeur probante satisfaisant à ces différents critères.

De plus, la loi de finances rectificative a modifié les règles relatives au contrôle des factures. A noter que l'article L. 80 FA du CGI permet désormais aux agents de l'administration d'intervenir de manière inopinée dans les locaux professionnels des entreprises émettrices et réceptrices des factures et, s'il y a lieu, dans les locaux professionnels des prestataires de services de télétransmission des factures pour contrôler la conformité du fonctionnement du système de télétransmission des factures et de la procédure de signature électronique.

À sa suite, le décret n°2013-346 du 24 avril 2013 relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et au stockage des factures électroniques [153] est venu modifier l'art. 242 nonies de l'Annexe II au CGI qui prévoit désormais expressément un mandat écrit et préalable en cas de recours à un tiers en charge de l'établissement des factures électroniques lorsque ce dernier est établi dans un pays avec lequel il n'existe pas d'instrument d'assistance administrative ainsi que celle de l'art. R. 102 C-1-I du Livre de procédures fiscales concernant les modalités de stockage des factures électroniques dans un pays non lié à la France par une convention fiscale (soit un droit d'accès en ligne, de téléchargement et d'utilisation des données stockées par l'Administration, soit une assistance mutuelle).

De plus, le décret n° 2013-350 du 25 avril 2013 modifiant les dispositions de l'annexe III au Code général des impôts relatives aux factures transmises par voie électronique en matière de taxe sur la valeur ajoutée [154] a précisé certains points concernant les dispositifs de dématérialisation préexistants, en renforçant les caractéristiques de la signature électronique, qui doit désormais être fondée sur un certificat électronique qualifié et être créée par un dispositif sécurisé de création de signature électronique et en codifiant certaines dispositions relatives à l'EDI.

(153) J.O. 25 avril 2013.
(154) J.O. 26 avril 2013.

D'autres articles précisent les modalités de conservation des factures dont l'authenticité de l'origine, l'intégrité du contenu et la lisibilité sont assurées par des contrôles mis en place par les assujettis et les règles applicables en matière de restitution des factures sous forme papier ou électronique.

L'arrêté du 25 avril 2013 portant modification des dispositions de l'article 41 septies de l'annexe IV au Code général des impôts relatif aux factures transmises par voie électronique [155] a pris en compte les modifications terminologiques issues du décret n° 2013-350 du 25 avril 2013.

Prenant acte de ces modifications et des nouvelles notions qui s'en sont détachées telles que la notion de « *contrôles documentés et permanents* » et de « *piste d'audit fiable* », la Direction générale des finances publiques a entendu apporter, avec la publication au Bulletin officiel des Finances publiques-Impôts du 18 octobre 2013 « *BOFIP* » [156] des précisions et ses recommandations. Cette publication détaille, en effet, l'ensemble du cycle de vie de la facture de son émission à sa conservation en passant par sa restitution en cas de contrôle.

Le BOFIP (BOI-CF-COM-10-10-30-20-20180720) [157] dispose que les entreprises n'auront plus à conserver sous certaines conditions le double original des factures de vente créées sous forme informatique et transmises sur support papier. La facture papier numérisée constitue donc une pièce justificative au même titre que la facture originale, à condition que les exigences de l'article A. 102-B-2 du Livre des procédures fiscales soient respectées.

La loi PACTE a aussi ajoutée des précisions en matière de facturation électronique. Elle modifie l'article L. 224-12 du Code de la consommation [158] concernant les modalités de communication par voie électronique des factures d'électricité et de gaz naturel. Les professionnels de ces deux secteurs peuvent communiquer les factures à leurs clients par voie électronique après avoir vérifié que ce mode de communication est compatible avec la situation du client.

Ces derniers doivent être informés par l'opérateur de la possibilité de se voir communiquer par voie électronique leurs factures.

Ils doivent aussi avoir la possibilité de s'opposer à la facturation électronique et pouvoir demander à tout moment et sans frais que les factures soient reçues sous format papier [159] .

(155) J.O. du 26 avril 2013, p. 7297.

(156) BOFIP, 18 oct. 2013 : BIC – TVA – CF – Transposition de la 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 : http://bofip.impots.gouv.fr/bofip/9113-PGP, voir. : Comm. Com. Electr. n° 4, Avril 2014, comm. 41, note E. A. Caprioli.

(157) La FnTC a édité en 2019 à ce propos le guide « Disparition du double électronique (de la facture) et apparition du double numérique, que faire ? ».

(158) Art. L. 224-12 § 2 du Code de la consommation « Lorsqu'un fournisseur souhaite adresser à un consommateur les factures sur un support durable autre que le papier, ce fournisseur vérifie au préalable que ce mode de communication est adapté à la situation de son client et s'assure que ce dernier est en mesure de prendre connaissance de ces factures sur le support durable envisagé [...] ».

Mais la loi de finances pour 2020 du 28 décembre 2019 [160] a instauré une révolution en matière de facturation électronique. L'article 153 de ladite loi énonce : « *Les factures des transactions entre assujettis à la taxe sur la valeur ajoutée sont émises sous forme électronique et les données y figurant sont transmises à l'administration pour leur exploitation à des fins, notamment, de modernisation de la collecte et des modalités de contrôle de la taxe sur la valeur ajoutée [...]* ». Cet article rend ainsi obligatoire dans les relations entre assujettis à la TVA (par exemple, des entreprises) le recours à un procédé de facturation électronique.

L'Ordonnance n° 2021-1190 [161] du 15 septembre 2021 relative à la généralisation de la facturation électronique dans les transactions entre assujettis à la taxe sur la valeur ajoutée et à la transmission des données de transaction est venue fixer le cadre de cette réforme profonde dans la vie des entreprises. Le texte de l'Ordonnance est périmé et remplacé à l'identique par l'art. 26 de la Loi n° 2022-1157 du 16 août 2022 de finances rectificative pour 2022 [162].

La Loi de Finances Rectificative insère un article 289 bis dans le Code général des impôts qui généralise en I. l'obligation d'émission, de transmission et de réception des factures électroniques pour les seuls **assujettis à la TVA établis en France ou ayant leur résidence habituelle en France**. Elle porte sur les factures de ventes de biens et services « *domestiques* » réalisées entre assujettis (B2B) mais aussi sur les livraisons aux enchères publiques de biens d'occasion, d'œuvres d'art, d'objets de collection ou d'antiquité. L'obligation porte également sur les avoirs et les factures d'acomptes.

Les intéressés pourront choisir entre un portail public de facturation décrit à l'article L. 2192-5 de la Code de la commande publique ou à une plateforme de dématérialisation privée.

(159) Art. L. 224-12 § 2 al. 2 du Code de la consommation : « [...] le fournisseur informe le client de façon claire, précise et compréhensible de la poursuite de l'envoi des factures sur le support durable retenu. Il renouvelle ces vérifications annuellement.
Le fournisseur informe le client du droit de celui-ci de s'opposer à l'utilisation d'un support durable autre que le papier et de demander, par tout moyen, à tout moment et sans frais, à recevoir les factures sur un support papier [...] ».

(160) J.O. du 29 décembre 2019.

(161) J.O. du 16 septembre 2021.

(162) J.O. du 17 août 2022.

Une autre grande nouveauté de la réforme figurant à l'article 289 bis II du CGI a trait à la **communication à l'administration des données relatives aux mentions figurant dans les factures électroniques émises et se rapportant à leurs ventes et achats non concernés par l'obligation de facturation électronique mais taxés à la TVA en France ou réalisés à partir de la France.** Celles-ci seront transmises à l'administration soit par le portail public directement, soit par la plateforme de dématérialisation.

Là encore, un décret en Conseil d'État portant sur les modalités de transmission des données est prévu. Le portail public met à disposition des plateformes de dématérialisation un annuaire central recensant les informations nécessaires à l'adressage des factures électroniques.

Ces dispositions s'appliqueront au plus tôt à compter du 1er juillet 2024 et au plus tard à compter du 1er janvier 2026 selon des modalités qui devraient être précisées d'ici là. Cet article va plus loin puisqu'en sus de la transmission de la facture électronique, il faudrait communiquer les données y figurant de manière individualisée ou autonome.

L'administration fiscale disposerait ainsi d'une parfaite visibilité par rapport à la TVA collectée par les assujettis mais permettrait aussi aux assujettis de disposer d'une version pré-remplie de l'imprimé déclaratif CA3 ou équivalent. **Pour l'heure (30 septembre 2022), les modalités tant nationales qu'européennes ne sont pas fixées.**

3. Les services bancaires électroniques : 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° la fourniture mensuelle 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 [163]).

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

(163) La loi n°2001-1168 du 11 décembre 2001 portant mesures urgentes de réformes à caractère économique et financier, dite loi MURCEF, J.O. du 12 décembre 2001.

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 compte.

À l'issue de cette transposition, il n'y a donc pas eu lieu de modifier la pratique de délivrance par les banques des relevés de compte électroniques, la DSP2 donnant au « *support durable* » la même définition [164]. Le maintien dans la DSP2 de ladite définition confirme l'affirmation précitée en tous points.

4. Les envois électroniques recommandés

Sur le plan juridique, l'envoi recommandé est un instrument utilisé dans les notifications en général et les mises en demeure ainsi que plus spécifiquement chaque fois qu'un texte mentionne - et ils sont très nombreux - l'envoi d'une « *lettre* » recommandé avec ou sans demande d'avis de réception.

Initialement, l'équivalent électronique de la lettre recommandée (papier) a été consacré par l'ordonnance du 16 juin 2005 [165] dans le cadre de la formation et de l'exécution des contrats et était précisé par les décrets n° 2011-144 du 2 février 2011 [166] et n° 2011-434 du 20 avril 2011 [167]. Le régime juridique défini était ainsi réservé aux formalités contractuelles du droit civil.

Avec l'article 93 de la loi pour une République numérique du 7 octobre 2016 [168], la reconnaissance juridique de l'envoi recommandé électronique (ERE) devient transversale et autonome.

(164) V. nos développements I.B.2) relatifs à la reconnaissance juridique des documents électroniques dans le domaine bancaire.

(165) Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique, J.O 17 juin 2005 ; É. A. Caprioli, Les lettres recommandées électroniques, Cahiers de droit de l'entreprise, n° 3, mai 2011, prat. 15.

(166) 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, J.O. 4 févr. 2001 ; v. É A. Caprioli, La lettre recommandée électronique, un nouveau décret pour la « confiance numérique » ; Comm. Com. Electr., n° 4, avril 2011, com. 40 ; L. Grynbaum, Pour une bonne réception de la lettre recommandée électronique, note sous 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, JCP E, n°8, 24 février 2011, Act. 98, p. 9-10 ; Réponse ministérielle publiée au J.O. du 9 juillet 2013, p. 7214.

(167) 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, J.O. 21 avr. 2011 p. 7093 ; v. É. A. Caprioli, Fiabilité du procédé d'horodatage électronique, Comm. Com. Electr., n° 7, juillet 2011, com. 70 ; T. Piette-Coudol, Fiabilité de la date et horodatage de l'article 1369-8 du Code civil, Rev. Lamy Droit de l'Immatériel, n° 72, juin 2011, p. 40-47.

(168) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, J.O. 8 oct. 2016.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

D'une part, il n'est plus question de lettre recommandée, par parallélisme à la terminologie utilisée dans le règlement européen eIDAS [169]. D'autre part, un nouvel instrument est né.

Ainsi, l'article 93 de la loi étend le champ d'application de **l'envoi recommandé électronique qui sort du cadre du Code civil et est désormais régi par l'article L. 100 du Code des Postes et des Communications électroniques** (CPCE).

L'envoi recommandé électronique s'applique ainsi à tous les usages.

L'article L. 100 du CPCE pose deux caractéristiques importantes. D'abord, « *l'envoi recommandé électronique est équivalent à l'envoi par lettre recommandée, dès lors qu'il satisfait aux exigences de l'article 44 du règlement (UE) n° 910/2014* » du 23 juillet 2014 (eIDAS). Le renvoi à l'article 44 n'est pas sans incidence juridique et technique, étant donné qu'il concerne les envois recommandés électroniques qualifiés. En conséquence, seuls les envois recommandés électroniques qualifiés sont équivalents à une lettre recommandée papier.

Toutefois, cette équivalence ne doit pas permettre de remettre en cause le principe de non-discrimination affirmé par le législateur européen à l'art. 43.1 du Règlement eIDAS [170]. Ensuite, « *dans le cas où le destinataire n'est pas un professionnel, celui-ci doit avoir exprimé à l'expéditeur son consentement à recevoir des envois recommandés électroniques* ».

L'article L. 100-I, al. 3 du CPCE prévoit également, à l'instar de ce que faisait l'ancien article 1369-8 du Code civil, la possibilité d'un envoi recommandé hybride, c'est à dire, envoyé par voie électronique, imprimé sur papier et acheminé par la voie postale habituelle.

En ce qui concerne l'article 44 du Règlement eIDAS qui traite des envois recommandés électroniques **qualifiés, il précise** :

(169) Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, J.O.U.E. 28 août 2014 L. 257/73.

(170) Art. 43.1 du Règlement eIDAS « L'effet juridique et la recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique comme preuves en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'envoi recommandé électronique qualifié ».

*« a. Ils sont fournis par un ou plusieurs prestataires de services de confiance **qualifiés** ;*

b. Ils garantissent l'identification de l'expéditeur avec un degré de confiance élevé ;

c. Ils garantissent l'identification du destinataire avant la fourniture des données ;

d. L'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification indétectable des données ;

e. Toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données ;

f. La date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié. ».

Parallèlement, en droit national, les modalités de la LRE ont été précisées par le décret n° 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique [171] qui a créé les articles R. 53-1 à R. 53-4 du CPCE (partie réglementaire). Le pouvoir réglementaire a ainsi déterminé les conditions d'application de l'article L. 100-II du CPCE.

Les exigences requises ont trait à l'identification de l'expéditeur et du destinataire ; à la preuve du dépôt par l'expéditeur et du moment de ce dépôt ; à la preuve de la réception par le destinataire et du moment de cette réception ; à l'intégrité des données transmises ; à la remise de l'envoi recommandé imprimé sur papier (LR hybride).

Sont également précisées les informations que le prestataire d'un envoi recommandé électronique doit porter à la connaissance du destinataire et enfin le montant de l'indemnité forfaitaire due par le prestataire dont la responsabilité est engagée, en cas de retard de la réception, perte, altération ou modification frauduleuse des données transmises dans le cadre de la prestation.

(171) Décret n° 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique, J.O. 12 mai 2018.

Plus précisément, l'article R.53-1 al.1 du CPCE indique que la **vérification initiale de l'identité de l'expéditeur** devra être réalisée selon les modalités de l'article 24 du Règlement eIDAS, à savoir :

> *« a. Par la présence en personne de la personne physique ou du représentant autorisé de la personne morale ; ou*
>
> *b. À distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfont aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie substantiel et élevé ; ou*
>
> *c. Au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b) ; ou*
>
> *d. À l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité* ».

L'alinéa 2 de ce même article traite de la **vérification initiale de l'identité du destinataire** qui s'appuie sur un moyen d'identification électronique relevant d'un niveau de garantie substantiel au sens du chapitre I du Règlement eIDAS.

On fera ici deux remarques.

D'une part, on soulignera que le décret ne traite pas des conditions de manifestation du consentement à la réception des LRE par le destinataire non professionnel (art. L. 100-I al.2 CPCE) [172], ce qui constituait une des interrogations des acteurs du marché. Ce point doit de plus être mis en perspective avec l'application du Règlement Général de Protection des Données qui fait de la gestion du consentement à l'utilisation des données l'alpha et l'oméga de la relation client.

D'autre part, on notera avec intérêt que si la vérification initiale de l'identité de l'expéditeur peut être assurée par le prestataire de services de lettre recommandée lui-même, il n'en va pas de même pour celle du destinataire qui dépend des mesures de vérification d'identité figurant au § 2.1 de l'Annexe du Règlement n° 2015/1502 (préc.).

Cet état des lieux nécessite donc de savoir qui peut fournir une identité aussi fiable aujourd'hui en France. Actuellement, on relèvera que « *L'identité numérique La Poste* » a été reconnue conforme au niveau de sécurité substantiel défini par le règlement eIDAS [173].

(172) Art. L. 100-I al. 2 du CPCE : « Dans le cas où le destinataire n'est pas un professionnel, celui-ci doit avoir exprimé à l'expéditeur son consentement à recevoir des envois recommandés électroniques ».

(173) Voir le Communiqué Presse - La Poste ANSSI - Identité numérique accessible à l'adresse : https://le-groupe-laposte.cdn.prismic.io/le-groupe-laposte/5ee5fddb-5e12-47c6-8b2c-562f95f64b32_CP-La-Poste-Identite-numerique-qualification-ANSSI.pdf (date du 31/01/2020).

En conséquence, ce service devrait pouvoir être valablement utilisé dans le cadre des envois recommandés électroniques, en ce qui concerne l'exigence d'identification d'un niveau « *substantiel* ».

Le texte traite également du contenu de la preuve de dépôt (art. R. 53-2 du CPCE) [174] délivrée à l'expéditeur, du contenu de la preuve de réception par le destinataire (art. R 53-3-II du CPCE) [175] ainsi que du contenu de la preuve de refus (art. R. 53-3-III du CPCE) [176]. Les conditions de conservation et d'accessibilité y sont prévues.

Par ailleurs, l'article R. 53-4 du CPCE indique qu'en cas de retard dans la réception ou en cas de perte des données, la responsabilité du prestataire ne serait engagée que dans les conditions prévues à l'art. R.2-1 du CPCE, à savoir 16 euros.

Enfin, l'article L. 101 du CPCE introduit une nouveauté importante. Ainsi, « *est puni d'une amende de 50.000 euros le fait de proposer ou de fournir un service qui ne remplit pas les exigences fixées à l'article L.100 dans des conditions de nature à induire en erreur l'expéditeur ou le destinataire sur les effets juridiques de l'envoi.* »

Cette disposition revêt une importance particulière, dans la mesure où la LRE est un service de confiance qui entre dans le champ d'application du règlement eIDAS. Par conséquent, les sociétés qui fournissent un tel service sans en remplir les exigences seront sanctionnées.

(174) Article R. 53-2 du CPCE : « Le prestataire de lettre recommandée électronique délivre à l'expéditeur une preuve du dépôt électronique de l'envoi. Le prestataire doit conserver cette preuve de dépôt pour une durée qui ne peut être inférieure à un an.

Cette preuve de dépôt comporte les informations suivantes :

1° Le nom et le prénom ou la raison sociale de l'expéditeur, ainsi que son adresse électronique ;

2° Le nom et le prénom ou la raison sociale du destinataire ainsi que son adresse électronique ;

3° Un numéro d'identification unique de l'envoi attribué par le prestataire ;

4° La date et l'heure du dépôt électronique de l'envoi indiquées par un horodatage électronique qualifié tel que défini par l'article 3 du règlement (UE) n° 910/2014 mentionné ci-dessus ;

5° La signature électronique avancée ou le cachet électronique avancé tels que définis par l'article 3 du règlement (UE) n° 910/2014 mentionné ci-dessus, utilisé par le prestataire de services qualifié lors de l'envoi ».

(175) Article R. 53-3 II. du CPCE : « En cas d'acceptation par le destinataire de la lettre recommandée électronique, le prestataire procède à sa transmission.

Le prestataire conserve une preuve de la réception par le destinataire des données transmises et du moment de la réception, pour une durée qui ne peut être inférieure à un an.

Outre les informations mentionnées aux 1° à 5° de l'article R. 53-2, cette preuve de réception comporte la date et l'heure de réception de l'envoi, indiquées par un horodatage électronique qualifié ».

(176) Article R. 53-3 II du CPCE : « En cas de refus de réception ou de non-réclamation par le destinataire, le prestataire met à disposition de l'expéditeur, au plus tard le lendemain de l'expiration du délai prévu au I, une preuve de ce refus ou de cette non-réclamation. Cette preuve précise la date et l'heure du refus telles qu'indiquées par un horodatage électronique qualifié, et fait mention des informations prévues aux 1° à 5° de l'article R. 53-2.

Le prestataire conserve la preuve de refus ou de non-réclamation du destinataire pour une durée qui ne peut être inférieure à un an ».

D'autant que les envois recommandés électroniques qualifiés selon les modalités du règlement, bénéficieront d'un label européen, représenté par un logo qui pourra figurer sur les supports de communication [177] , de sorte que les utilisateurs soient dûment informés de la qualification ou non du service de confiance proposé.

Reste à voir comment cet article sera appliqué, notamment, si cette sanction sera assortie d'une condamnation à publication sur le site internet de l'entreprise aux pratiques déloyales ou à une publication par voie de presse ou sur certains sites internet.

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* » [178]. 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, mais aussi les décisions de justice et les actes de l'état civil [179].

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'État. Deux décrets ont été adoptés en application de ce texte : il s'agit des décrets n° 2005-972 et 2005-973 du 10 août 2005 [180] qui respectivement modifient le décret n° 56-222 du 29 février 1956 [181] 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.

(177) Exemple : site web ; v. le Label TrustMark : label de confiance pour les services de confiance qualifié - Règlement d'exécution (UE) 2015/806 de la commission du 22 mai 2015, J.O.U.E. du 23 mai 2015, L.128/13.

(178) V. G. Cornu, Vocabulaire juridique, éd. Quadrige PUF, 2011. V° Authentique.

(179) V. pour la dématérialisation de la procédure de recouvrement des petites créances par les huissiers de justice : Décret n°2016-285 du 9 mars 2016 relatif à la procédure simplifiée de recouvrement des petites créances, J.O. 11 mars 2016.

(180) J.O. 11 août 2005.

(181) 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, J.O du 3 mars 1956.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Des conditions sont communes aux actes authentiques des deux professions :

1. Les systèmes d'information des notaires et les huissiers de justice, 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 commissaires de justice - CNCJ - pour les huissiers de justice et commissaires-priseurs) ;
   - 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 notaires et les huissiers de justice 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.
3. Les notaires et les huissiers de justice 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 CNCJ. 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.

Des exigences particulières sont applicables à chaque profession.

L'ordonnance du 10 février 2016 a introduit un article 1369 qui reprend la définition de l'acte authentique et intègre la dispense de mention manuscrite prévue à l'article 1317-1 actuel. Aucun changement substantiel n'est à relever et les modalités décrites dans les décrets applicables aux huissiers de justice et notaires continuent à s'appliquer.

Conformément à l'article 20 du décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par notaires, modifié par le décret n° 2005-973 du 10 août 2005, le système mis en place impose la présence du notaire à côté de son client ou de deux notaires qui communiquent entre eux à distance, mais chacun d'eux étant en présence physique d'un client.

En effet, « *Lorsqu'une partie ou toute autre personne concourant à un acte n'est ni présente ni représentée devant le notaire instrumentaire, son consentement ou sa déclaration est recueilli par un autre notaire* ***devant lequel elle comparaît*** *et qui participe à l'établissement de l'acte.* » Il est à noter que « *le système de traitement et de transmission de l'information agréé par le Conseil supérieur du notariat et garantissant l'intégrité et la confidentialité du contenu de l'acte*. » (article 16 du décret de 1971 modifié).

La perfection de l'acte est parachevée par la signature électronique sécurisée du notaire (art. 17), c'est-à-dire la signature électronique qualifiée établie à l'aide de la clé REAL depuis le règlement eIDAS.

Pendant la période de COVID, « *jusqu'à l'expiration d'un délai d'un mois à compter de la date de cessation de l'état d'urgence sanitaire déclaré dans les conditions de l'article 4 de la loi du 23 mars 2020 susvisée, le notaire instrumentaire peut, par dérogation aux dispositions de l'article 20 du décret du 26 novembre 1971 susvisé, établir un acte notarié sur support électronique lorsqu'une ou toutes les parties ou toute autre personne concourant à l'acte ne sont ni présentes ni représentées.* » (art. 1er du décret du 3 avril 2020) ».

La note d'information du CSN du 4 avril 2020 (182) venait en préciser les contours. « *Si le notaire n'a pu procéder lui-même à la vérification de l'identité de son client [au cours des 10 années précédant le rendez-vous de comparution à distance], il peut déléguer cette procédure grâce à un système agréé ANSSI dans le cadre de la procédure DocuSign.*

(182) Disponible à l'adresse : https://www.cridon-ne.org/wp-content/uploads/2020/04/note_dinformation_du_4_avril_2020.pdf.

Cette procédure prend la forme d'une visio conférence avec les services de DocuSign via sa plateforme IDNOws.

Afin d'éviter une rupture du flux vidéo lors de la réception de l'acte authentique par comparution à distance, il convient de faire réaliser cette vérification au préalable.

Ainsi l'identité du client sera vérifiée et il ne sera plus nécessaire de procéder à une visio entre le client et DocuSign lors de la cérémonie de recueil des consentements.

Pour réaliser cette vérification préalable, le notaire envoie au client, avant la cérémonie de signature de l'acte par comparution à distance, un document (par exemple l'accord du client pour que l'acte soit reçu par le notaire au moyen d'une comparution à distance) à signer via DocuSign avec le mode « signature à distance avec vidéo ».

Le client signe ce document via DocuSign (IDNow vérifie alors l'identité du client via une vidéo chat).

Le client se crée un compte sur la plateforme IDNow afin que son identité soit conservée ». Quai des notaires, legaltech dont la solution a été labellisée par le CSN, a précisé que la solution DocuSign de vérification d'identité à distance continuait l'utilisation de sa solution après quelques difficultés.

Le décret du 3 avril 2020 mettait l'accent sur trois fonctions juridiques et sécurité fondamentales que le processus de communication et de transmission de l'information, toujours agréé par le CSN, devait garantir : l'identification des parties, l'intégrité et la confidentialité du contenu de l'acte.

Le consentement et la déclaration des parties sont recueillis par le notaire instrumentaire en même temps que la signature électronique qualifiée (SEQ) des parties. Cette SEQ répond aux exigences du décret du 28 septembre 2017 ; trois conditions cumulées en application du règlement européen eIDAS (articles 26, 28 et 29) : elle doit être une signature électronique avancée, créée à l'aide d'un dispositif de création de signature électronique qualifié qui repose sur un certificat qualifié de signature électronique.

En d'autres termes, le décret exigeait le niveau le plus élevé de fiabilité de la signature électronique. On peut considérer qu'il était regrettable que le certificat de signature du client ne soit pas délivré par le notariat après son identification et son enregistrement par le notaire instrumentaire et que le système impose le recours à un prestataire de service de confiance, externe à la profession.

Un notaire a demandé en référé au Conseil d'État, la suspension du décret du 3 avril 2020. Il estimait que l'établissement de l'acte à distance, sans la comparution physique des parties, était incompatible avec la notion d'authenticité.

La requête est rejetée le 15 avril 2020.

Le décret ne dérogeait pas aux dispositions législatives et le fait qu'il « *autorise l'établissement de l'acte notarié sur support électronique à distance n'est pas de nature à créer un doute sérieux sur sa légalité, alors qu'il ne résulte d'aucune disposition législative que la mission du notaire instrumentaire ne puisse être accomplie que dans le cas d'une comparution physique des parties* » et que la dérogation au décret du 26 novembre 1971 n'est que temporaire.

La présente dérogation a expiré un mois après la cessation de l'état d'urgence sanitaire (soit au 31 août 2022).

Seule persiste la faculté d'établir des procurations notariées à distance telle que prévue à l'art. 20-1 du Décret du 26 novembre 1971 modifié par le Décret n°2020-1422 du 20 novembre 2020 (J.O. du 21 novembre 2020).

6. Le vote électronique

D'un point de vue général, la délibération n° 2010-371 du 21 octobre 2010 de la CNIL [183] avait adopté une recommandation relative à la sécurité des systèmes de vote électronique qui prenait en compte les évolutions des techniques et de la pratique. La CNIL avait par la suite donné un avis favorable au projet de label « *e-vote* » présenté par la FnTC [184].

La délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet [185] abroge et actualise les recommandations qu'elle avait effectuées en 2010.

Cette délibération identifie trois niveaux de risque associés à des objectifs de sécurité cumulables qui permettent de définir le niveau de sécurité attendu du dispositif.

+ **Le Niveau 1** correspond aux personnes ayant peu de ressources et de motivations, et s'applique pour les scrutins impliquant peu d'électeurs (par exemple : élection d'un représentant de classe), dans un cadre non conflictuel ;

(183) Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, J.O. du 24 novembre 2010.

(184) CNIL, Délibération n° 2016-071 du 17 mars 2016 portant avis sur un projet de label « e-vote » présenté par la Fédération des Tiers de Confiance (FnTC) (n° LB15033885), J.O. du 8 avril 2016.

(185) J.O. 21 juin 2019.

+ **Le Niveau 2** concerne des ressources et des motivations moyennes dont les scrutins impliquent un nombre important d'électeurs (par exemple : élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel), avec un enjeu élevé mais dépourvu de conflictualité particulière ;

+ **Le Niveau 3** vise des ressources importantes et de fortes motivations (par exemple : élections de représentants du personnel au sein d'organisations importantes), dont les scrutins impliquent de nombreux électeurs, avec un enjeu très élevé dans un climat potentiellement conflictuel.

  La CNIL déconseille fortement d'utiliser un dispositif de niveau 3.

La CNIL met à disposition une grille d'analyse simplifiée pour déterminer les objectifs de sécurité que doit atteindre la solution de vote. Dans tous les cas, le niveau de risque choisi doit être évalué par un expert indépendant mandaté, que la solution soit gérée en interne ou fournie par un prestataire.

Ces exigences devront être prises en compte par les organismes sous un délai de douze mois à compter de la publication de la recommandation.

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'État* ». 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'État* ».

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 cinquième alinéa de l'article R. 225-77 du Code de commerce : « *Les formulaires de vote par correspondance reçus par la société comportent : [...] 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 deuxième alinéa de l'article R. 225-79 du Code de commerce quant à la procuration donnée par un actionnaire pour se faire représenter à une assemblée.

Ces modifications ont une incidence pratique importante sur la signature électronique. En effet, l'ancien décret n° 67-236 du 23 mars 1967 sur les sociétés commerciales dans sa dernière version, abrogé par le 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* ».

Dorénavant, une signature électronique « *simple* » suffit (C. civ., art. 1316-4, al. 2, première phrase devenu art. 1367 du Code civil) sans que les sociétés anonymes n'aient à modifier leurs statuts. Il n'est plus nécessaire de disposer d'une signature électronique qualifiée [186].

Ainsi, désormais, l'exigence de signature consiste à utiliser un procédé fiable d'identification de l'actionnaire, garantissant son lien (logique) avec le vote au moyen d'un certificat électronique d'identification.

(186) (188) J.O. du 31 mars 2001, p. 2553. V. É. 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.

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 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 » [187].

La société doit créer un site exclusivement consacré à cette fin [188]. 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. 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* [189] ». 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* » [190].

b. Le vote électronique au sein des ordres professionnels à travers l'exemple des avocats

Le décret n° 2002-1306 du 28 octobre 2002 [191] 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 [192] organisant la profession d'avocat.

(187) 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 (J.O. du 10 novembre 2011 p. 18893), v. É. Caprioli, Les formalités de communication par voie électronique en matière de droit des sociétés, Comm. Com. électr. n° 1, Janvier 2012, comm. 9.

(188) Article R. 225-61 du Code de commerce.

(189) Article R. 225-80 du Code de commerce.

(190) Article R.225-98 du Code de commerce.

(191) J.O. 30 octobre 2002.

(192) J.O. 28 novembre 1991.

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 confidentie*l ».

Malgré sa consécration, la mise en place du vote électronique puis son application au sein de l'Ordre des avocats suscitent encore des contestations [192].

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

La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) a instauré la possibilité de recourir au vote électronique pour les élections des délégués du personnel et des membres du comité d'entreprise. Son article 54 a inséré, en effet, 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 [194], traitant du vote par bulletin-papier, les mots « *ou par vote électronique, dans les conditions et selon les modalités définies par décret en Conseil d'État* ».

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 [195] 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 ;

(193) V. Cass.1er civ., 7 juin 2005, n°05-60.044 : JurisData n°2005-028790, - V. CA, Aix-en-Provence, 17 septembre 2015, n°14/23041 pour un rejet des recours formés par un avocat contre deux délibérations du conseil de l'Ordre introduisant le vote électronique pour les élections au sein du barreau de Marseille.

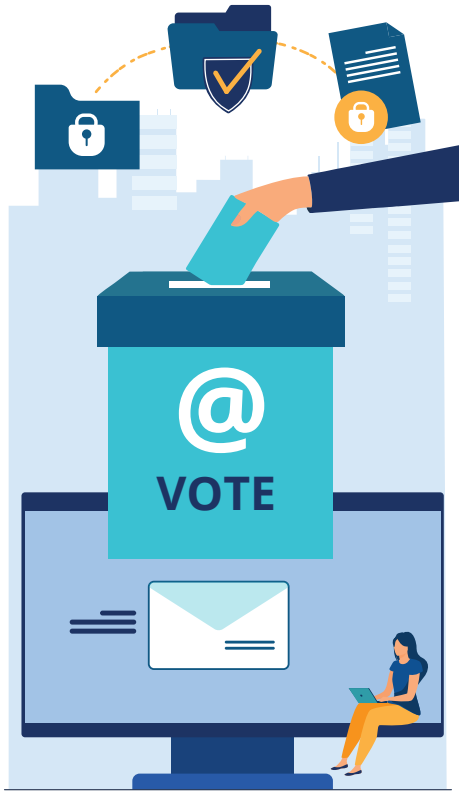
(194) Ordonnance n° 2007-329 du 12 mars 2007 relative au code du travail (partie législative), J.O. 13 mars 2007.

(195) J.O. 27 avril 2007.

+ 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 [196] ;
+ 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 [197].

Notons que le renvoi d'une question prioritaire de constitutionnalité portant sur la conformité des articles L. 2314-21 et L. 2324-19 du Code du travail et donc de l'autorisation du recours au vote électronique à la Constitution, a été rejeté pour défaut de caractère nouveau et sérieux par la Cour de cassation [198].



(196) Sur cette thématique voir : É. A. Caprioli, Annulation d'un vote électronique en l'absence d'une expertise du logiciel conforme, Comm. Com. Electr. n° 10, Octobre 2012, comm. 118, relatif au jugement du TI Brest, 7 juin 2012, n° 11-11-000973.

(197) 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. 27 avril 2007.

(198) Cass. soc., 29 janvier 2015.

7. 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 pré-remplir un formulaire de souscription avant l'envoi postal du dossier contenant les documents justificatifs ainsi que le formulaire signé.

Progressivement, certaines d'entre elles ont mis en place des services de souscription en ligne pour notamment 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 pré-constituer les preuves de l'engagement des clients. Tel est l'apport de l'arrêt de la Cour de cassation du 27 mai 2008 [199] :

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. Ces motivations étaient les suivantes. Tout d'abord, l'absence d'envoi du document est justifiée par le fait que l'assuré vivait aux États-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 par l'assureur ne peut pas avoir d'effet rétroactif au jour de l'accident. À 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.

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

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.

Plus récemment, dans une décision du 6 avril 2016, la Cour de cassation a reconnu la validité de la signature d'une adhésion à une assurance complémentaire, alors que le souscripteur avait dénié sa signature [200].

La fiabilité de la procédure de souscription est donc nécessaire et les sociétés d'assurance, ainsi que les banques mettent aujourd'hui en place des services de souscription en ligne pour leurs contrats, et ont commencé la souscription de prestations plus engageantes comme les contrats d'assurances-vie.

Pour des raisons de sécurité juridique et technique, elles ont en principe recours à des moyens et des prestations de signature électronique (avec des certificats standard ou à la volée).

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

En outre, le décret du 29 décembre 2014 relatif à la résiliation à tout moment de contrats d'assurance et portant application de l'article L. 113-15-2 du Code des assurances [201] a permis une avancée significative dans la gestion par voie électronique des relations entre les Sociétés d'assurance et leurs assurés. En effet, en permettant notamment aux assurés de transmettre pour certains contrats leur demande de résiliation par lettre ou « *tout support durable* », ce décret devrait constituer une incitation à une prise en compte étendue des relations dématérialisées et à la création de moyens internes permettant de les gérer.

De plus, l'ordonnance n° 2017-1433 du 4 octobre 2017 relative à la dématérialisation des relations contractuelles dans le secteur financier consacre le support durable en matière de contrat d'assurance. Elle reconnait aussi l'utilisation du courrier électronique recommandé et de la signature électronique si le choix est laissé au futur assuré. Ce texte permet à ces établissements de prendre le virage numérique comme celui déjà opéré par les établissements de banque et de finance en ligne. [202]

Ainsi, l'article L. 110-10-I dispose notamment que l'établissement qui « *[...] souhaite fournir ou mettre à disposition des informations ou des documents à un assuré sur un support durable autre que le papier, vérifie au préalable que ce mode de communication est adapté à la situation de celui-ci* », après s'être assuré que le client était en mesure de prendre connaissance des informations et documents sur le support durable envisagé.

Le recours à la voie électronique est donc le principe et le recours à la voie papier l'exception.

On notera également l'article L. 111-11 du Code des assurances qui prévoit la mise en place d'un espace personnel sécurisé qui doit comprendre deux fonctions :

+ La communication et la notification des informations et documents auprès de l'assuré par tout moyen à la disposition de la société d'assurance ;
+ La conservation des informations et des documents (précontractuels ou contractuels) dans des conditions de nature à garantir l'accessibilité des informations et documents.

Enfin, le décret n° 2018-229 du 30 mars 2018 relatif à la dématérialisation des relations contractuelles dans le secteur financier [203] et l'arrêté du 27 mars 2018 modifiant le Code des assurances et relatif à la dématérialisation des relations contractuelles dans le secteur financier [204] sont pris en application de l'ordonnance n° 2017-1433 du 4 octobre 2017 relative à la dématérialisation des relations contractuelles dans le secteur financier [205]. Les références à l'écrit papier sont supprimées dans le Code des assurances.

(201) Décret n° 2014-1685 du 29 décembre 2014 relatif à la résiliation à tout moment de contrats d'assurance et portant application de l'article L. 113-15-2 du Code des assurances, J.O. du 31 décembre 2014, p. 23383.

(202) V. à ce sujet : P. Agosti, Le formalisme de l'assurance à l'épreuve des réseaux, l'Usine Digitale, 17 avril 2018.

(203) J.O. 31 mars 2018.

(204) J.O. 30 mars 2018.

(205) J.O. 5 oct. 2017.

8. 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 [206] modifie certaines dispositions du Code de commerce (articles L. 814-2 et L. 814-13 C. Com.) 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'État, 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. [207]»

L'échéance de la mise en service était fixée au plus tard le 1er janvier 2014 et deux décrets d'application de l'article L. 814-13 C. Com. devaient être publiés, à savoir :

+ 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'État pris après avis de la CNIL fixant les modalités d'utilisation du portail électronique par les Administrateurs judiciaires et les Mandataires judiciaires.

(206) J.O. du 29 mars 2011.

(207) Article L.814-2 du code du commerce.

LA DIGITALISATION DANS LA SPHÈRE PRIVÉE (B TO C, B TO B ET C TO C)

Le décret n° 2015-1009 du 18 août 2015 relatif à la mise en œuvre du portail électronique prévu aux articles L. 814-2 et L. 814-13 du Code de commerce ainsi qu'un arrêté du 1er octobre 2015 relatif à la mise en œuvre du portail électronique prévu aux articles L. 814-2 et L. 814-13 du Code de commerce sont ainsi venus préciser les modalités d'application dudit portail.

Ce dernier arrêté précise les garanties auxquelles doivent répondre les envois et les remises des actes lorsqu'ils sont effectués par voie électronique : authentification de l'identification des parties à la communication, signature électronique, protection de l'intégrité et de la confidentialité des actes, horodatage, conservation des actes.

Ce Portail a pour finalité de permettre la transmission électronique :

+ D'actes de procédure dans le cadre des procédures collectives,
+ Des actes relatifs aux créances, à savoir : informations générales par le mandataire judiciaire aux créanciers qui en font la demande (C. com., art. R. 621-19) ; déclaration de créance antérieure (C. com., art. L. 622-24) ; transmission des créances par le débiteur dans la SFA (C. com., art. L. 628-7) ; créances postérieures privilégiées portées par les créanciers concernés à la connaissance du mandataire judiciaire ou du liquidateur (C. com., art. L. 622-17 et L. 641-13) ; discussion entre le mandataire ou le liquidateur et le créancier à propos des créances déclarées (C. com., art. L. 622-27) ; déclaration de créance de dommages et intérêts en cas de résiliation de contrat en cours par l'administrateur (C. com., art. L. 622-13 et L. 641-11-1)
+ Des actes relatifs aux biens qui sont prévus : demande de revendication et de restitution (C. com., art. L. 624-9 et s.) ; acquiescement et contestation par l'administrateur judiciaire ou le liquidateur en matière de revendication et de restitution (C. com., art. L. 624-17 et L. 641-14-1) ;
+ Des actes concernant les contrats en cours comme la mise en demeure adressée à l'administrateur ou au mandataire judiciaire concernant un contrat en cours (C. com., art. L. 622-13 et L. 641-11-1) ; réponse faite à la mise en demeure par ledit mandataire de justice dans le délai prévu (art. préc.).

NOTES

Cet espace vous est dédié pour prendre des notes.

Sommaire

fntc

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

Les enjeux de la dématérialisation dans la sphère publique ont été appréhendés il y a déjà plusieurs décennies en France [208]. Progressivement, les plans [209] et mesures [210] adoptés par les pouvoirs publics successifs ont octroyé une place grandissante à la digitalisation.

Ces dernières années, la transformation numérique des administrations est ainsi devenue l'une des composantes du processus de modernisation des administrations de l'État et plus largement de l'ensemble des personnes publiques. Elle est même annoncée comme une priorité « *notamment pour atteindre l'objectif fixé par le président de la République de 100% de services publics dématérialisés à horizon 2022* » [211].

En 2020, la pandémie et ses conséquences ont renforcé la nécessité de mener à bien cette transformation.

Les téléservices et les téléprocédures connaissent donc des déploiements de plus en plus aboutis au sein des administrations. La digitalisation dans la sphère publique est désormais omniprésente dans les relations entre administrations et usagers (particuliers et professionnels), dans les relations entre administrations (collaboration et/ou contrôle), dans les relations de travail (administration et agents) et dans la commande publique (administrations et fournisseurs).

(208) V. à titre d'illustration, Observatoire des technologies de l'information, Vers une administration sans papier ?, La documentation française, juillet 1996.

(209) V. par exemple le programme d'action gouvernementale pour la société de l'information (PAGSI) lancé en janvier 1998 (v. http://archive.dgmic.culture.gouv.fr/article.php3?id_article=841) et plus récemment le programme « Action publique 2022 » lancé le 13 octobre 2017 (https://www.modernisation.gouv.fr/action-publique-2022/comprendre/lancement-du-programme-action-publique-2022) et le programme TECH.GOUV publié le 10 octobre 2019 qui prévoit un fonds dédié de 700 millions d'euros sur les 5 années à venir pour la transformation du service public par le numérique (Note d'information DGP/SIAF/2019/005 DINUM et DINSIC, réf. DGP/SIAF/2019/005).

(210) V. par exemples l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du Code des relations entre le public et l'administration (J.O. du 25 octobre 2015) qui a notamment intégré les modalités de saisine et d'échanges entre administration et usager par voie électronique ; la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance (J.O. du 11 août 2018) qui s'inscrit dans la « Stratégie nationale d'orientation de l'action publique » établie par le gouvernement le 10 août 2018 et tend vers une « Administration engagée dans la dématérialisation » (chapitre 1er du Titre 2 de la loi) en prévoyant diverses mesures expérimentales ; ou encore plus récemment la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (J.O. du 26 juillet 2019) qui consacre plusieurs dispositions au déploiement du numérique dans le secteur de la santé.

(211) Comme indiqué dans le programme « Action publique 2022 », réf. cit. supra.

Parallèlement, la digitalisation dans la sphère publique s'est accompagnée de son lot d'interrogations quant à la sécurité juridique des échanges électroniques et de la dématérialisation des procédures et des actes administratifs [212]. **A cet égard, il est important de rappeler que le droit public et administratif connaît ses propres principes et règles.**

De plus, **la digitalisation des administrations doit tenir compte d'une multitude de facteurs**, dont notamment la diversité des autorités administratives qui constituent un ensemble hétéroclite (administrations centrales et déconcentrées de l'État, collectivités territoriales comprenant les régions, les départements, les grandes villes comme de très petites communes, établissements publics, autorités administratives indépendantes…).

Il existe également une multitude de procédures (obligatoires ou non, déclaratives ou d'autorisation…), plusieurs catégories juridiques d'actes (consultatifs, administratifs, contractuels) et des domaines de compétence aussi vastes que différents (santé, justice, éducation, police, état civil, urbanisme, aides sociales, finances publiques, fonction publique…). S'ajoutent à ces paramètres, le souci d'un service public de qualité s'adressant à des personnes aguerries aux technologies comme à des « *illectronautes* » [213].

En conséquence, dès lors que les prestataires de services de confiance ont un rôle à jouer dans la sphère publique, l'approche juridique en la matière doit reposer sur l'étude étayée de l'ensemble des éléments à prendre en compte. Chaque projet « *sphère publique* » doit ainsi faire l'objet d'une analyse au cas par cas. Les développements qui suivent ne peuvent dès lors que dresser, partiellement et dans les grandes lignes, les principes juridiques applicables et certaines illustrations y afférents.

(212) V. pour une analyse des principes de droit administratif confrontés aux perspectives de la dématérialisation des actes administratifs : Anne Cantero, La dématérialisation des actes administratifs, Presses Universitaires Aix Marseille, 2001.

(213) V. sur le sujet : Défenseur des droits, Rapport Dématérialisation des services publics : trois ans après, édition 2022, accessible à l'adresse https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/ddd_rapport-dematerialisation-2022_20220207.pdf.

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

Les échanges par voie électronique sont reconnus par principe dans les relations entre les administrations et le public (1). Toutefois, cette reconnaissance juridique est assortie du respect de certaines modalités (2).

La particularité des envois recommandés appelle des remarques spécifiques (3). Enfin, le principe de reconnaissance des échanges par voie électronique peut connaître des exceptions (4).

1. Les principes

L'ordonnance n° 2005-1516 du 8 décembre 2005 (214) a introduit le principe de la reconnaissance juridique des échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives elles-mêmes.

Modifiées à plusieurs reprises (215), les dispositions adoptées sont désormais codifiées aux articles L.112-7 et suivants du Code des relations entre le public et l'administration (CRPA). Sauf dispositions contraires, ces règles s'appliquent, en principe, au sens de l'article L.100-3 du CRPA :

+ Aux administrations, c'est-à-dire « *les administrations de l'État, les collectivités territoriales, leurs établissements publics administratifs et les organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif, y compris les organismes de sécurité sociale* »,
+ Et au public, c'est-à-dire : « *toute personne physique* » et « *toute personne morale de droit privé, à l'exception de celles qui sont chargées d'une mission de service public lorsqu'est en cause l'exercice de cette mission* ».

En pratique, il conviendra donc d'identifier d'une part, les parties concernées par la digitalisation, d'autre part, si lesdites relations sont régies par des textes spécifiques ou si les dispositions « *de droit commun* » posées par le CRPA s'appliquent.

(214) 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 9 décembre 2005, p. 18896 et s.

(215) V. notamment : ordonnance n° 2014-1330 du 6 novembre 2014 relative au droit des usagers de saisir l'administration par voie électronique, J.O. du 7 novembre 2014, p. 18780 ; loi n° 2015-1268 du 14 octobre 2015 d'actualisation du droit des outre-mer, J.O. du 15 octobre 2015 p. 19069 ; ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, J.O. du 25 octobre 2015 p. 19872 ; loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté, J.O. du 28 janvier 2017 ; ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques, J.O. du 5 octobre 2017.

Dans ce dernier cas, trois types d'échange par voie électronique sont prévus.

+ **Premièrement**, en application de l'article L.112-8 du CRPA, le **public se voit reconnaître un droit de saisine de l'administration** [(216)] **et de réponse à l'administration par voie électronique, sous réserve que la personne se soit identifiée préalablement auprès d'une administration**. Cette saisine peut porter sur une demande, une déclaration, un document ou une information. Les modalités d'application de ce droit ont été précisées par décret [(217)] et codifiées à l'**article R.112-9-1 du CRPA**. Lorsque la saisine ou la réponse par voie électronique respecte les conditions posées, l'administration est réputée en être régulièrement saisie. En ce sens, elle doit traiter la demande, la déclaration, le document ou l'information sans demander à la personne concernée la confirmation ou la répétition de son envoi sous une autre forme.

+ **Deuxièmement**, **l'administration peut mettre en place un ou plusieurs téléservices** conformément à l'article L.112-9 du CRPA. Le cas échéant, les usagers pourront saisir l'administration par voie électronique exclusivement en utilisant ledit téléservice. Toutefois, l'administration doit avoir informé le public du téléservice.

  De plus, le Conseil d'État a précisé dans un arrêt du 3 juin 2022 que l'obligation d'avoir recours à un téléservice pour accomplir une démarche administrative auprès d'un service de l'État ne constitue pas en elle-même une atteinte à l'exercice des libertés publiques et aux droits fondamentaux des personnes; néanmoins, l'obligation de recourir au téléservice ne doit ni avoir pour effet de modifier les conditions légales de la demande concernée, ni empêcher l'accès normal des usagers au service public et elle doit permettre de garantir aux personnes concernées l'exercice effectif de leurs droits [(218)].

(216) Cette disposition ne s'applique pas à la saisine par voie électronique des juridictions administratives qui fait l'objet de textes spécifiques (v. nos développements sur la digitalisation des procédures contentieuses administratives infra).

(217) Décret n° 2015-1404 du 5 novembre 2015 relatif au droit des usagers de saisir l'administration par voie électronique (J.O. du 6 novembre 2015) modifié par le décret n° 2016-1411 du 20 octobre 2016 relatif aux modalités de saisine de l'administration par voie électronique, (J.O. du 22 octobre 2016) dont les modalités sont précisées dans la circulaire ARCB1711345C du ministre de l'aménagement du territoire, de la ruralité et des collectivités territoriales et du ministre de l'intérieur à destination des préfets.

(218) Conseil d'État, Section, 3 juin 2022, req. n° 452798, accessible à l'adresse: https://www.legifrance.gouv.fr/ceta/id/CETATEXT000045863484?init=true&page=1&query=452798&searchField=ALL&tab_selection=all. En l'espèce, le décret n° 2021-313 du 24/03/2021 et deux arrêtés subséquents rendaient obligatoire le recours au téléservice mis en place par l'administration pour déposer des demandes de titres de séjour par les étrangers. Prenant en compte les difficultés pour les étrangers d'accéder aux services en ligne et leur maniement, ainsi que l'absence d'accompagnement de ceux-ci prévu par les textes applicables pour accomplir les formalités concernées, le Conseil d'État a annulé les textes concernés dans la mesure où aucune solution de substitution n'était prévue.

A défaut, le public se voit reconnaître le droit de saisir l'administration par tout type d'envoi. En outre, les modalités d'application de l'article L.112-9 du CRPA ont été précisées par décret [219] et codifiées à l'article R.112-9-2 du CRPA. Ainsi, le téléservice doit respecter les dispositions relatives à la protection des données personnelles [220] ainsi que les règles de sécurité, d'interopérabilité et d'accessibilité fixées respectivement dans le Référentiel Général de sécurité (RGS), le Référentiel Général d'Interopérabilité (RGI) et le Référentiel Général d'Amélioration de l'Accessibilité (RGAA) [221].

De plus, la décision de création du téléservice et ses modalités d'utilisation doivent être accessibles depuis ce service. En pratique, les modalités d'utilisation prennent la forme de conditions générales d'utilisation, accessibles à partir du téléservice et du site de l'administration. Ces conditions générales d'utilisation s'imposent de façon unilatérale au public et relèvent de la compétence du juge administratif en cas de contentieux.

+ **Troisièmement**, en application de l'article L.112-14 du CRPA : « ***L'administration peut répondre par voie électronique :***

1° A toute demande d'information qui lui a été adressée par cette voie par une personne ou par une autre administration ;

2° Aux autres envois qui lui sont adressés par cette même voie, sauf refus exprès de l'intéressé. ».

(219) Décret n° 2015-1404 du 5 novembre 2015 relatif au droit des usagers de saisir l'administration par voie électronique, J.O du 6 novembre 2015 modifié par le décret n° 2016-1411 du 20 octobre 2016 relatif aux modalités de saisine de l'administration par voie électronique, J.O. du 22 octobre 2016 dont les modalités sont précisées dans la circulaire ARCB1711345C du ministre de l'aménagement du territoire, de la ruralité et des collectivités territoriales et du ministre de l'intérieur à destination des préfets.

(220) A savoir notamment les dispositions issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données dit RGPD), JOUE du 4 mai 2016 et de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. du 7 janvier 1978 p. 227 modifiée notamment par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, J.O. du 21 juin 2018.

(221) Les RGS, RGI et RGAA servent de référentiels transversaux dans le cadre de la digitalisation des administrations. Ils font l'objet de développements spécifiques infra.

L'administration se voit donc reconnaître un droit de réponse par voie électronique, dès lors que cette voie a été utilisée par l'autre partie pour les demandes d'informations et lorsque ce moyen a été utilisé dans tous les autres cas, sauf si l'interlocuteur s'y est expressément opposé.

Lorsque les échanges par voie électronique entre les administrations et les usagers relèvent de l'un des cas ci-dessus visés, ils doivent en plus respecter un certain nombre d'exigences.

2. Les conditions

Le Code des relations entre le public et les administrations (CRPA) impose différentes exigences aux échanges dématérialisés entre les administrations et le public. Aux conditions exposées ci-dessous s'ajoutent celles tenant au respect des référentiels de sécurité, d'interopérabilité et d'accessibilité qui concernent plus largement l'ensemble des communications des administrations sous forme et par voie électroniques [222].

a. L'identification du public

En application de l'article L.112-8 du CRPA, l'identification d'une personne lors d'échanges par voie électronique avec une administration est imposée. Cette identification doit avoir été faite préalablement auprès d'une administration.

En d'autres termes, il s'agit, concrètement, d'indiquer « *dans son envoi, s'il s'agit d'une entreprise, son numéro d'inscription au répertoire des entreprises et de leurs établissements, s'il s'agit d'une association, son numéro d'inscription au répertoire national des associations et, dans les autres cas, ses nom et prénom et ses adresses postale et électronique*. » (article R.112-9-1 du CPRA).

D'autres alternatives sont reconnues pour les téléservices. Ainsi, l'alinéa 2 de l'article R.112-9-1 du CPRA prévoit : « *Les modalités peuvent également permettre l'utilisation d'un identifiant propre à la personne qui s'adresse à l'administration ou celle d'autres moyens d'identification électronique dès lors que ceux-ci sont acceptés par l'administration* ».

(222) Les RGS, RGI et RGAA sont présentés dans les grandes lignes infra dans la partie « dispositions communes».

Dans le cadre des téléservices, l'administration pourra déterminer quels sont ces moyens (dans les conditions générales d'utilisation notamment, qui, le cas échéant s'imposent aux usagers).

Les moyens d'identification électronique du public peuvent ainsi reposer sur diverses modalités dans la sphère publique. A cet égard, il est important de rappeler que FranceConnect, qui est un service proposé par l'Etat, n'est pas un fournisseur d'identité en tant que tel. En effet, **FranceConnect** agrège les données de fournisseurs d'identité, vérifie les données auprès de l'INSEE et génère un identifiant technique transmis au fournisseur de service auprès duquel la personne entend s'identifier. Initié par l'arrêté du 24 juillet 2015 [(223)] et précisé par l'arrêté du 8 novembre 2018 [(224)] après l'adoption du Règlement eIDAS [(225)], FranceConnect garantit ainsi l'identité d'un usager en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée par un fournisseur d'identité.

Réservé à l'origine exclusivement aux autorités administratives, ce téléservice est désormais ouvert aux acteurs privés proposant « *des services en ligne dont l'usage nécessite, conformément à des dispositions législatives ou règlementaires, la vérification de l'identité de leurs utilisateurs ou de celle de certains de leurs attributs et uniquement pour les services qui nécessitent cette vérification* » [(226)].

La Direction du Numérique (DINUM) qui est en charge de ce téléservice a précisé dans des documents spécifiques les exigences et engagements attendus d'une part, des partenaires « *fournisseurs d'identité* », d'autre part, des partenaires « *fournisseurs de services* ».

En outre, dans le cadre de la régulation du marché communautaire et pour son bon développement, **le Règlement eIDAS [(227)] contraint les Etats membres à la reconnaissance transfrontalière des moyens d'identification électronique permettant de s'identifier aux services publics lorsque ceux-ci ont été notifiés à la Commission européenne conformément aux modalités posées**.

(223) Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », J.O. du 6 août 2015 p. 13487.

(224) Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'État, J.O. du 15 novembre 2018.

(225) Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, J.O.UE du 28 aout 2014.

(226) En application de l'article 4 de l'arrêté du 8 novembre 2018. Un arrêté du 11 mai 2020 a prévu à titre expérimental d'étendre à d'autres personnes morales relevant de secteurs d'activité strictement énumérés le recours à FranceConnect. Cette expérimentation s'est terminée en principe le 12 mai 2021 et la CNIL aurait dû rendre un rapport 6 mois après cette date.

(227) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (dit Règlement eIDAS) ; v. les considérants 12, 13, 14 et 15 ainsi que les dispositions du chapitre II Identification électronique, et notamment les exigences d'interopérabilité des schémas (articles 6 et 12).

Dans ce cadre, FranceConnect constitue également le « *nœud eIDAS* » permettant au public « *d'accéder à des téléservices d'autres Etats membres en respectant les dispositions prévues par le règlement e-IDAS* » relatives notamment au niveau de garantie requis par le téléservice concerné (art. 2, 4° de l'arrêté).

b. L'identification de l'administration et de l'agent

L'article L.111-2 du CRPA reconnaît à toute personne « *le droit de connaître le prénom, le nom, la qualité et l'adresse administratives de l'agent chargé d'instruire sa demande ou de traiter l'affaire qui la concerne ; ces éléments figurent sur les correspondances qui lui sont adressées. Si des motifs intéressant la sécurité publique ou la sécurité des personnes le justifient, l'anonymat de l'agent est respecté* ».

Ces principes s'appliquent quel que soit le support utilisé.

Concrètement, par exemple, le mail à l'instar de la lettre, devra indiquer qui est chargé de la demande et du suivi du dossier (administration, service et nom de l'agent).

Cette identification de contact administratif doit être distinguée de la qualité juridique de la personne qui prend, le cas échéant, une décision administrative. En effet, les règles relatives à la compétence juridique des personnes pouvant adopter des décisions administratives demeurent.

Dès lors, les dispositions relatives à l'identification du représentant de l'administration en tant qu'autorité décisionnaire, signataire de l'acte, doivent être distinguées des dispositions relatives à l'identification de l'administration et de l'agent en tant que personne chargée de la gestion et du suivi du dossier.

Dans ce cas, sont dispensés de signature :

+ *« 1° Les décisions administratives qui sont notifiées au public par l'intermédiaire d'un téléservice conforme à l'article L. 112-9 et aux articles 9 à 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 ainsi que les actes préparatoires à ces décisions ;*

+ *2° Les décisions administratives relatives à la gestion de leurs agents produites par les administrations sous forme électronique dans le cadre de systèmes d'information relatifs à la gestion ou à la dématérialisation de processus de gestion des ressources humaines conforme aux articles 9, 11 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 précitée, quelles que soient les modalités de notification aux intéressés, y compris par l'intermédiaire d'un téléservice mentionné au 1° ;*

+ *3° Quelles que soient les modalités selon lesquelles ils sont portés à la connaissance des intéressés, les saisies administratives à tiers détenteur, adressées tant au tiers saisi qu'au redevable, les lettres de relance relatives à l'assiette ou au recouvrement, les avis de mise en recouvrement, les mises en demeure de souscrire une déclaration ou d'effectuer un paiement, les décisions d'admission totale ou partielle d'une réclamation et les demandes de documents et de renseignements pouvant être obtenus par la mise en œuvre du droit de communication prévu au chapitre II du titre II de la première partie du livre des procédures fiscales ;*

+ *4° Les visas délivrés aux étrangers. ».*

c. L'accusé d'enregistrement et/ou de réception électroniques

En application de l'article L.112-11 du CRPA, tout échange par voie électronique (par téléservices ou autre) ainsi que tout paiement par téléprocédure doivent faire l'objet d'un accusé de réception [228].

Si ce dernier ne peut pas être instantanément produit (par exemple dans le cas où - avant d'accuser réception de la demande - il faut l'analyser afin de générer un avis de réception contenant les mentions obligatoires informant le demandeur des délais applicables le cas échéant), un accusé d'enregistrement électronique doit être émis.

(228) Sauf en cas d'abus ou de risque pour la sécurité du système d'information de l'administration en application de l'article L.112-11, al. 3 et 4 du CRPA.

Les articles R.112-11-1 à R.112-11-4 du CRPA précisent les mentions et modalités d'émission et d'envoi.

L'obligation de générer un accusé de réception ou d'enregistrement doit être respectée de façon très large puisque tout usager doit en bénéficier quel que soit son lieu de résidence. Indirectement, cette précision implique qu'aucun filtrage quant à l'envoi desdits accusés ne saurait être fait selon l'identification du lieu d'émission de la saisine [229].

Ceci est particulièrement louable dans la mesure où la dématérialisation de l'administration s'avère notamment intéressante pour les personnes résidant à l'étranger afin de lever certains obstacles de communication éventuellement liés au décalage horaire.

- **S'agissant de l'accusé de réception électronique, les mentions obligatoires qu'il doit contenir sont :**

> *« 1° La date de réception de l'envoi électronique effectué par la personne ;*
>
> *2° La désignation du service chargé du dossier, ainsi que son adresse électronique ou postale et son numéro de téléphone.*
>
> *S'il s'agit d'une demande, l'accusé de réception indique en outre si la demande est susceptible de donner lieu à une décision implicite d'acceptation ou à une décision implicite de rejet ainsi que la date à laquelle, à défaut d'une décision expresse, et sous réserve que la demande soit complète, celle-ci sera réputée acceptée ou rejetée.*
>
> *Dans le premier cas, l'accusé de réception mentionne la possibilité offerte au demandeur de recevoir l'attestation prévue à l'article L. 232-3. Dans le second cas, il mentionne les délais et les voies de recours à l'encontre de la décision »* [230].

- **Si c'est un accusé d'enregistrement qui est émis, en application de l'article R. 112-11-2 du CRPA, il doit notamment mentionner la date de réception de l'envoi.**

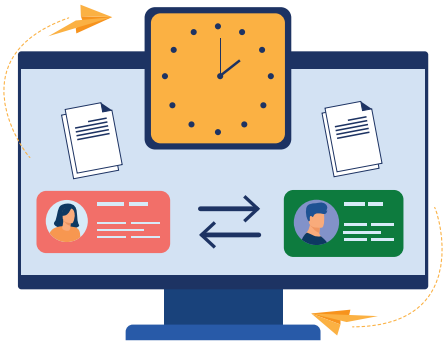
(229) L'article L.112-11 du CPRA, alinéa 2, dispose ainsi : « L'administration est également tenue de respecter l'obligation prévue au premier alinéa du présent article pour les envois par voie électronique effectués par tout usager résidant en France ou à l'étranger ou par toute autorité administrative étrangère lorsque celle-ci agit pour le compte d'un Français établi à l'étranger ». Article R.112-11-1 du CRPA (version issue du décret n 2016-1411 du 20 octobre 2016).

(230) Cette question doit également être appréhendée au regard de l'article L.112-12 du CRPA.

On relèvera que les accusés de réception et d'enregistrement doivent être émis conformément au Référentiel Général de Sécurité en application de l'article L.112-11 du CRPA.

À cet égard, les politiques d'horodatage définies par l'Agence nationale de la sécurité des systèmes d'information constituent des références essentielles.

Compte tenu des calculs de délai éventuellement applicables dans le cadre de recours administratifs, gracieux ou contentieux, contre des décisions expresses ou implicites reçues par voie électronique, l'importance accordée à la fiabilité des procédés utilisés prend tout son sens [231].



Ces formalités de réception doivent être distinguées de l'envoi recommandé.

3. Le cas particulier des envois recommandés

En application de l'article L.112-15 alinéa 1 du CRPA, **lorsqu'une personne doit adresser un document à l'administration en envoi recommandé**, elle dispose de trois possibilités pour le faire par voie électronique :

+ Soit elle utilise un téléservice au sens du CRPA (ce qui suppose que l'administration en ait mis un en place et qu'il permette des envois) ;
+ Soit elle utilise un envoi recommandé au sens de l'article L.100 du Code des postes et communications électroniques [232] ;
+ Soit elle utilise « *un procédé électronique, accepté par cette administration, permettant de désigner l'expéditeur et d'établir si le document lui a été remis* ».

En application de l'article L.112-15 alinéa 2 du CRPA, **lorsqu'une administration doit notifier un document à une personne**, elle dispose de deux possibilités pour le faire par voie électronique, et ce, **sous réserve que la personne intéressée (personne physique comme personne morale) ait préalablement donné son accord exprès** :

+ Soit elle utilise un envoi recommandé au sens de l'article L.100 du Code des postes et communications électroniques [233] ;
+ Soit elle utilise « *un procédé électronique permettant de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si le document lui a été remis* ».

(231) Cette question doit également être appréhendée au regard de l'article L.112-12 du CRPA.
(232) Sur ce service de confiance, voir nos développements dans la partie « Sphère privée » du présent Vade-Mecum.
(233) Sur ce service de confiance, voir nos développements dans la partie « Sphère privée » du présent Vade-Mecum.

Les modalités d'application de ces dispositions ont été précisées par décrets [234].

À titre principal, l'administration doit informer les usagers du procédé qu'elle accepte en dehors des téléservices et de l'article L.100 du code des postes et communications électroniques et de ses caractéristiques (articles R.112-16 et suivants du CRPA). Ce procédé doit être conforme aux RGS et RGI .

Concrètement, les administrations ont la possibilité de recourir à des solutions d'« *espace personnel*» ou de services de coffre-fort numérique, dans le respect des exigences juridiques posées et, le cas échéant, des procédures d'achat de la commande publique. L'administration doit adresser à la personne « *un avis l'informant qu'un document est mis à sa disposition et qu'elle a la possibilité d'en prendre connaissance par le procédé » ; étant noté que cet avis doit mentionner « la date de mise à disposition du document, les coordonnées du service expéditeur et le délai prévu à l'article R. 112-20. » (article R.112-19 du CRPA).*

L'article R.112-20 précise quant à lui : « Le document notifié est réputé avoir été reçu par son destinataire à la date de sa première consultation. Cette date peut être consignée dans un accusé de réception adressé à l'administration par le procédé prévu au deuxième alinéa de l'article L. 112-15. À défaut de consultation du document par son destinataire dans un délai de quinze jours, le document est réputé lui avoir été notifié à la date de mise à disposition. ».

4. Les possibles exceptions au principe de reconnaissance des échanges électroniques

L'article L.112-10 du CRPA donne la possibilité au pouvoir réglementaire d'écarter par décret en Conseil d'État certaines démarches administratives de la saisine par voie électronique pour des « *motifs d'ordre public, de défense et de sécurité nationale, de bonne administration, ou lorsque la présence personnelle du demandeur apparaît nécessaire*. ».

En application de cette disposition, on citera à titre d'exemple le décret n° 2016-1491 du 4 novembre 2016 [236] concernant les démarches effectuées auprès des collectivités territoriales, de leurs établissements publics ou des établissements publics de coopération intercommunale dressant dans son annexe 1 la liste des exceptions à titre définitif et dans son annexe 2 la liste des exceptions à titre transitoire jusqu'au 31 décembre 2021.

(234) V. les articles R.112-16 à R.112-18 du CRPA créés par le décret n° 2017-1728 du 21 décembre 2017 relatif au procédé électronique prévu à l'article L. 112-15 du CRPA.

(235) Sur le RGS et le RGID v. nos commentaires infra.

(236) Décret n°2016-1491 du 4 novembre 2016 modifié par le décret n° 2018-954 du 5 novembre 2018 modifiant le décret n° 2016-1491 du 4 novembre 2016 relatif aux exceptions à l'application du droit des usagers de saisir l'administration par voie électronique concernant les démarches effectuées auprès des collectivités territoriales, de leurs établissements publics ou des établissements publics de coopération intercommunale.

NOTES

Cet espace vous est dédié pour prendre des notes.

Sommaire

fntc

B. LES ÉCHANGES ÉLECTRONIQUES ENTRE ADMINISTRATIONS

Afin d'alléger les démarches des administrés et d'éviter la redondance des informations demandées aux usagers, certaines demandes ou informations transmises à une administration peuvent être obtenues auprès d'une autre administration.

Le régime juridique de cette facilité résulte de la combinaison des articles L.113-12, L.113-13, L.114-8 et L.114-9 du Code des relations entre le public et l'administration (CRPA). Mais ce pouvoir est limité et encadré. Ainsi, l'article L.114-8 du CRPA limite ces échanges à ***« toutes les informations ou données strictement nécessaires pour traiter une demande présentée par le public ou une déclaration transmise par celui-ci en application d'un texte législatif ou réglementaire ».***

De plus, les administrations sont notamment tenues d'en informer les personnes concernées. Les articles R.114-9-1 et suivants du CRPA désignent également les administrations auprès desquelles la demande de communication doit être adressée compte tenu du type d'informations ou de données concernées [(237)].

En pratique, plusieurs projets sont nés sur le fondement de ces textes.

Par exemple, au niveau national, la Direction du numérique propose le guichet « *Dites-le nous une fois* » via des API spécifiques à destination des administrations centrales, décentralisées et territoriales [(238)]. L'objectif affiché est d'accompagner les administrations dans la circulation et l'exploitation des données des usagers afin d'optimiser le service public rendu.

Au niveau local, certaines administrations territoriales ont mis en place leur propre plateforme d'échanges de données entre différentes structures publiques dans la mesure où un suivi commun est juridiquement justifié (départements et communes dans le cadre de subvention d'associations, communes et CCAS…).

Ce type de démarche ne manque toutefois pas de soulever un certain nombre de problématiques juridiques. Il en a été ainsi, par exemple, des modalités juridiques des échanges de données de santé entre les maisons départementales des personnes handicapées et les départements sous la tutelle desquelles elles sont placées et de l'hébergement desdites données par ces derniers.

(237) Le décret n° 2021-464 du 16 avril 2021 a récemment complété ces dispositions créées par le décret n° 2019-31 du 18 janvier 2019 relatif aux échanges d'informations et de données entre administrations dans le cadre des démarches administratives et à l'expérimentation prévue par l'article 40 de la loi n° 2018-727 du 10 août 2018 pour un Etat au service d'une société de confiance, J.O. du 20 janvier 2019.

(238) Pour une présentation, v. https://www.numerique.gouv.fr/services/guichet-dites-le-nous-une-fois/.

À toutes fins utiles, il est précisé qu'en cas de manquement aux principes juridiques applicables, la décision finale pourrait être entachée d'un vice de forme et encourir, le cas échéant, son annulation, nonobstant la mise en cause de la responsabilité de l'administration concernée.

Les échanges par voie électronique entre administrations peuvent également résulter de dispositions législatives et réglementaires relatives aux contrôles dont une administration est chargée à l'égard d'une autre autorité administrative. Tel est le cas par exemple du contrôle des dépenses publiques locales (ordonnateur/comptable [239]) ou encore du contrôle de la légalité des actes des collectivités territoriales [240].

Les modalités de ces échanges électroniques sont régies par des textes spécifiques et des contions de mise en œuvre dédiées. Ces échanges reposent notamment sur des plateformes d'opérateurs de transmission homologuées pour le système d'échange.

C. LES ÉCHANGES ÉLECTRONIQUES ENTRE LES ADMINISTRATIONS ET LEURS AGENTS

La digitalisation des administrations a également un impact sur les agents, qu'ils soient fonctionnaires ou contractuels.

Toutes les phases peuvent être concernées, du recrutement à la fin de carrière (ou de contrat pour les agents contractuels). Il appartient à l'administration de s'assurer que les modalités mises en œuvre respectent les dispositions légales et réglementaires applicables.

(239) V. sur le sujet : https://www.collectivites-locales.gouv.fr/finances-locales/dematerialisation-de-la-chaine-comptable-et-financiere.

(240) En matière de contrôle de légalité, la dématérialisation repose sur le téléservices @CTES initié en mars 2004 et dont l'ensemble de la documentation a été mis à jour en 2019 après l'évolution successive des textes en la matière. V. pour plus d'infos : https://www.collectivites-locales.gouv.fr/institutions/ctes-dematerialisation-de-la-transmission-des-actes.

Bien évidemment, la digitalisation ne doit pas remettre en cause les principes posés en la matière (règles de recrutement, publication de certains actes, respect des indices, règles de mutation, détachement, mise en disponibilité…).

Ceci étant précisé, la dématérialisation des échanges avec les agents peut être appréhendée selon deux angles :

+ Vis-à-vis des usagers et de tiers (autres administrations ou autres fournisseurs de services). Dans ce cadre, l'administration doit mettre en place des modalités d'identification de ses agents afin de s'assurer qu'il s'agit bien de la personne identifiée en tant qu'agent, et qu'il dispose des habilitations pour agir. À cet égard, l'État « *plateforme* » a notamment mis en place FranceConnect Agent. Mais d'autres solutions restent bien évidemment envisageables, et ce, notamment pour les administrations territoriales.

+ Vis-à-vis de l'agent lui-même. Dans ce cadre, il s'agit d'envisager la création d'un espace numérique personnel réservé à chaque agent et aux documents relatifs à sa « *carrière* ».

  Tel est par exemple l'objet de l'Espace numérique sécurisé des agents publics de l'État (Ensap) qui permet à chaque agent concerné de consulter ses bulletins de paie, ses bulletins de pension, ses attestations fiscales et décomptes de rappel éventuels et son compte individuel de retraite. (241)

  Les autres administrations peuvent également mettre à disposition de leurs agents des espaces numérisés reposant sur d'autres solutions et intégrant, par exemple, leurs actes de nomination, d'avancement…

(241) Pour plus d'informations, v. le décret n° 2016-1073 du 3 août 2016, la délibération n° 2016-282 du 20 septembre 2016 de la CNIL et l'arrêté du 23 décembre 2016 portant création d'un traitement automatisé de données à caractère personnel dénommé Espace numérique sécurisé des agents publics (ENSAP) ainsi que les mentions légales du site ENSAP : https://ensap.gouv.fr/web/information/mentionslegales.

Sommaire

fntc

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

En France, le principe de la dématérialisation des marchés publics a été introduit dans le Code des marchés publics dès 2001 (242). Un seul article (article 56) était spécialement dédié à la transmission par voie électronique d'informations et le 4°) admettait par principe que les références à des écrits dans le code ne faisaient pas obstacle au remplacement de ceux-ci par un support ou un échange électronique (243). Les bases de la dématérialisation étaient ainsi posées.

Après de nombreuses modifications, tant au niveau communautaire (244) qu'en droit interne (245), **aujourd'hui, le régime applicable en matière de marchés publics et de contrats de concession résulte du Code de la commande publique dont les dispositions sont à titre principal issues de l'ordonnance n° 2018-1074 du 26 novembre 2018 portant partie législative du Code de la commande publique (246), du décret n° 2018-1075 du 3 décembre 2018 portant partie réglementaire du Code de la commande publique (247) et des arrêtés du 22 mars 2019 (248)**. La voie électronique y occupe une place prépondérante, sans remettre en cause les principes fondamentaux qui régissent les marchés publics et les contrats de concession.

(242) En application du décret n° 2001-210 du 7 mars 2001 portant code des marchés publics, J.O. du 8 mars 2001.

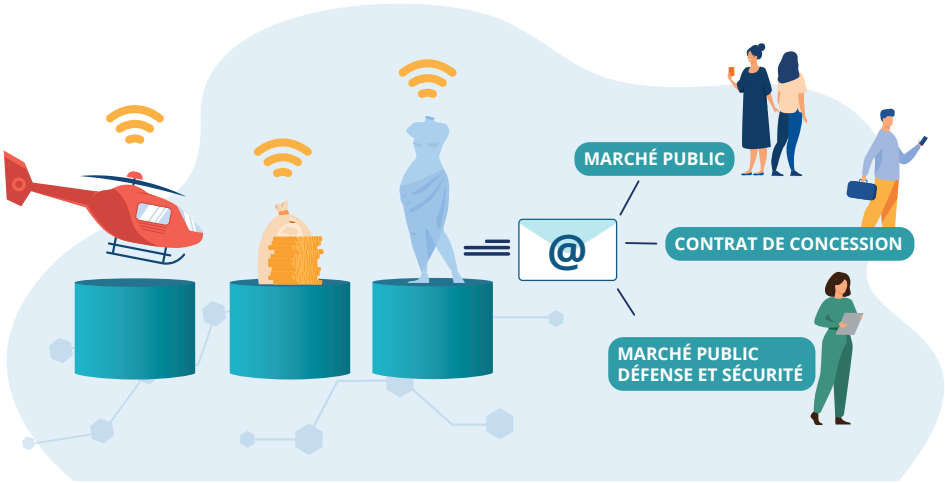
(243) Deux textes réglementaires en posaient les modalités : Décret n° 2001-846 du 18 septembre 2001 pris en application du 3° de l'article 56 du code des marchés publics et relatif aux enchères électroniques et Décret n° 2002-692 du 30 avril 2002 pris en application du 1° et du 2° de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics. Sur les avantages de la dématérialisation des marchés publics, v. E. Caprioli et A. Cantero, L'entreprise face à la dématérialisation des marchés publics, La Semaine juridique, éd. E, (LexisNexis), 3 novembre 2005, pp.1887-1891.

(244) Les textes les plus récents étant la Directive 2014/24/UE du parlement européen et du conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE, J.O.U.E. n° L 94 du 28/03/2014, p. 243 et s. ; la Directive 2014/23/UE du parlement européen et du conseil du 26 février 2014 sur l'attribution de contrats de concession, J.O.U.E. n° L 94 du 28/03/2014, p. 1 et s. ; le Règlement d'exécution (UE) 2016/7 du 5 janvier 2016 établissant le formulaire type pour le document unique de marché européen, J.O.U.E. n° L 3 du 06/01/2016, p. 16 et s.

(245) V. notamment le décret n° 2006-975 du 1er août 2006 portant code des marchés publics, J.O. du 4 août 2006, p. 11627 ; le décret n° 2014-1097 du 26 septembre 2014 portant mesures de simplification applicables aux marchés publics, J.O. n°0225 du 28 septembre 2014 p. 15782 ; l'ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics, J.O. du 24 juillet 2015 p. 12602 ; le décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics, J.O. du 27 mars 2016 ; le décret n° 2016-361 du 25 mars 2016 relatif aux marchés publics de défense ou de sécurité, J.O. du 27 mars 2016 ; l'arrêté du 14 avril 2017 relatif aux fonctionnalités et exigences minimales des profils d'acheteurs, J.O. du 27 avril 2017 ; l'ordonnance n° 2016-65 du 29 janvier 2016 relative aux contrats de concession, J.O. du 30 janvier 2016 ; le décret n° 2016-86 du 1er février 2016 relatif aux contrats de concession, J.O. du 2 février 2016.

Au fil des évolutions textuelles, le support et la forme électroniques sont devenus obligatoires, sous réserve du respect de certaines modalités et sauf exceptions .

Les développements qui suivent ne traitent que des aspects relatifs à la voie électronique pour les marchés publics (1), pour les marchés publics de défense et de sécurité (2) et pour les contrats de concession (3). Les procédures exclusivement réalisables par voie électronique sont ensuite traitées (4). Enfin, la facturation dans la commande publique mérite une attention particulière (5).



(246) J.O. du 5 décembre 2018.

(247) Décret n° 2018-1075 du 3 décembre 2018 portant partie réglementaire du Code de la commande publique, J.O. du 5 décembre 2018.

(248) V. partie Annexe préliminaire du Code de la commande publique créée par l'Arrêté du 22 mars 2019 (J.O. du 31 mars 2019) qui dresse la liste des différents avis et arrêtés constituant les annexes du Code de la commande publique parmi lesquels, dans le cadre de la dématérialisation, on notera l'annexe 6 (Arrêté du 22 mars 2019 fixant les modalités de mise à disposition des documents de la consultation et de la copie de sauvegarde), l'annexe 7 (Arrêté du 22 mars 2019 relatif aux fonctionnalités et exigences minimales des profils d'acheteurs), l'annexe 8 (Arrêté du 22 mars 2019 relatif aux exigences minimales des moyens de communication électronique utilisés dans la commande publique), l'annexe 12 (Arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique) et l'annexe 15 (Arrêté du 22 mars 2019 relatif aux données essentielles dans la commande publique).

1. La digitalisation des marchés publics

a. Obligation de principe et exceptions

Alors que les anciennes directives permettaient que les échanges d'information s'effectuent au choix de l'acheteur par courrier, télécopieur, par moyen électronique voire par téléphone, les articles 40 de la directive 2014/25/UE et 22 de la directive 2014/24/UE ont imposé que :

« *Les États membres veillent à ce que toutes les communications et tous les échanges d'informations effectués en vertu de la présente directive, et notamment la soumission électronique des offres, soient réalisés par des moyens de communication électroniques, conformément aux exigences du présent article.* ».

Pour les marchés publics, cette obligation a été transposée en droit interne à l'article L.2132-2 [(249)] **du Code de la commande publique** qui dispose : « *Les communications et les échanges d'informations effectués dans le cadre de la procédure de passation d'un marché sont réalisés par voie électronique, selon des modalités et sous réserve des exceptions prévues par voie réglementaire.* ».

L'article R.2132-7 [(250)] du Code de la commande publique précise : « *les communications et les échanges d'informations lors de la passation d'un marché en application du présent livre ont lieu par voie électronique*. » ; étant noté que son alinéa 2 prend soin de définir ce qu'il convient d'entendre par moyen de communication électronique, à savoir : « *un équipement électronique de traitement, y compris la compression numérique, et de stockage de données diffusées, acheminées et reçues par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques* ».

En application de ces dispositions, la voie électronique devient donc obligatoire pour la communication et les échanges d'informations dans le cadre des marchés publics [(251)].

Cette obligation connaît **un nombre limité d'exceptions posées**, notamment, à l'article R.2132-12 du Code de la commande publique. Ainsi, les moyens de communication électronique peuvent ne pas être utilisés dans le cadre des marchés publics : pour les marchés d'un montant inférieur à 25 000 euros (1°) ; pour les marchés de services sociaux et autres spécifiques mentionnés au 3° de l'article R.2123-1 et à l'article R.2123-2 du code (2°) ; lorsque la

(249) Issu dans sa dernière version de l'ordonnance n° 2018-1074 du 26 novembre 2018, réf. cit. supra.

(250) Issu du décret n° 2018-1075 du 3 décembre 2018, réf. cit. supra.

(251) Le lecteur est vivement invité à prendre connaissance des versions 4.0 des deux « Guides très « pratiques » de la dématérialisation des marchés publics » rédigés par la Direction des Affaires Juridiques (DAJ), sous l'égide du ministère de l'économie et des finances (mises à jour du 22/04/2019 : accessibles à l'adresse https : //www.economie.gouv.fr/daj/dematerialisation-commande-publique). Publiés en avril 2019, ces deux documents s'adressent respectivement aux acheteurs et aux opérateurs économiques (comprendre les candidats/soumissionnaires). Ils s'inscrivent dans la logique du Plan de Transformation Numérique de la Commande Publique et présentent sous forme de FAQ les aspects essentiels et pratiques de la dématérialisation de la commande publique.

voie électronique « *en raison de la nature particulière du marché* » nécessiterait de recourir à des moyens (outils, dispositifs, formats de fichiers, applications) « *pas communément disponibles* » (3°) ; si les applications prenant en charge les formats de fichiers sont trop spécifiques (4°) ; si un équipement de bureau spécialisé « pas communément utilisé » par l'acheteur s'avérait nécessaire (5°) ; lorsque les documents de consultation exigent la présentation de biens (maquettes, modèles réduits…) (6°) ; et enfin lorsque des raisons de sécurité ou de confidentialité le justifient (7°). Mais, la communication par voie électronique dans le cadre des marchés publics doit répondre à un certain nombre d'exigences.

b. La mise en place d'un « *profil acheteur* »

Parmi les exigences posées, la mise en place du « *profil acheteur* » est essentielle (article R.2132-3 du Code de la commande publique).

Dans son Guide « *très pratique* » de la dématérialisation des marchés publics à l'attention des acheteurs [252], la Direction des affaires juridiques indique que la Plateforme des Achats de l'État (PLACE) est la plateforme de dématérialisation des procédures de marchés de l'État. Les administrations de l'État [253] doivent utiliser PLACE, gérée par la direction des Achats de l'État (DAE).

Pour les autres acheteurs (à savoir les collectivités locales, établissements publics locaux, personnes morales de droit privé soumises à la commande publique…), ils disposent de trois options :

+ soit ils développent la plateforme en interne,
+ soit ils recourent à une plateforme mutualisée,
+ soit ils recourent à un « éditeur ». Le cas échéant, un marché public devra être passé [254].

Quelle que soit la solution retenue, l'arrêté du 22 mars 2019 [255] est applicable. Il précise les actions pouvant être effectuées par les acheteurs sur la plateforme et par les opérateurs économiques. Il apparaît clairement que le « *profil d'acheteur* » constitue l'outil central voire exclusif pour les mises à dispositions et les échanges dans le cadre des marchés publics. Tout prestataire qui souhaiterait proposer une solution en la matière devra donc se conformer aux exigences posées.

Au demeurant, la plateforme doit respecter les exigences du Référentiel Général de Sécurité (RGS), du Référentiel Général d'Interopérabilité (RGI) et du Référentiel Général d'Amélio-

(252) DAJ, « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les acheteurs », point A5, réf. citées supra.

(253) A priori, les établissements publics nationaux seraient également soumis à cette obligation même si le tableau du Guide « très pratique » (réf. citées supra) peut ne pas sembler très clair à cet égard.

(254) A cet égard, il est intéressant de se reporter aux points A8 et suivants du Guide « très pratique » version 4.0 de la dématérialisation des marchés publics pour les acheteurs, réf. citées supra.

(255) Arrêté du 22 mars 2019 relatif aux fonctionnalités et exigences minimales des profils acheteurs (constitutif de l'annexe 7 du code de la commande publique), réf. citées supra.

ration de l'Accessibilité (RGAA) en application de l'article 2.I de l'arrêté du 22 mars 2019 sus visé [256]. Plus avant, l'article 2.II précise que les fonctionnalités du « *profil acheteur* » géré par la plateforme doivent répondre « *aux exigences techniques, de sécurité et d'accessibilité suivantes :*

1° Le profil d'acheteur accepte les fichiers communément disponibles et notamment les fichiers aux formats .XML et .JSON ;

2° La taille et les formats des documents et avis d'appel à la concurrence sont indiqués ;

3° L'horodatage est qualifié conformément aux dispositions du règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 susvisé ;

4° Le profil d'acheteur assure l'intégrité des données ;

5° Le profil d'acheteur permet une visualisation adaptée au média utilisé ;

6° Le profil d'acheteur garantit la confidentialité des candidatures, des offres et des demandes de participation jusqu'à l'expiration du délai prévu pour leur présentation. Les documents sont inaccessibles avant cette date. À l'expiration de ce délai, ils ne sont accessibles qu'aux personnes autorisées. Le profil d'acheteur recourt à des moyens de cryptologie ou à un outil de gestion des droits d'accès et des privilèges ou à une technique équivalente ;

7° Le profil d'acheteur est interopérable avec les autres outils et dispositifs de communication électronique et d'échanges d'informations utilisés dans le cadre de la commande publique. ».

Le profil d'acheteur doit également envoyer immédiatement un accusé de réception automatique pour tout dépôt de documents par l'opérateur économique sur le profil d'acheteur. Cet accusé de réception doit contenir les mentions suivantes (article 2.III de l'arrêté du 22 mars 2019 sus visé) :

+ « *L'identification de l'opérateur économique auteur du dépôt ;*
+ *Le nom de l'acheteur public ;*
+ *L'intitulé et l'objet de la consultation concernée ;*
+ *La date et l'heure de réception des documents ;*
+ *La liste détaillée des documents transmis* ».

(256) Ces référentiels sont traités par ailleurs dans le présent Vade-Mecum.

Enfin, **les modalités d'identification des profils d'acheteurs sont définies à l'article 4 de l'arrêté du 22 mars 2019** comme suit :

+ « ***I. Le profil d'acheteur figure sur une liste publiée sur le portail unique interministériel destiné à rassembler et à mettre à disposition librement l'ensemble des informations publiques.***
+ ***II. Chaque profil d'acheteur est identifié par :***
+ *Le SIRET de l'acheteur ;*
+ *L'adresse URL du profil d'acheteur ;*
+ *L'adresse URL du DCAT prévue à l'article 8 de l'arrêté du 22 mars 2019 relatif aux données essentielles dans la commande publique précité.*
+ *Les coordonnées du ou des acheteurs concernés.* » .

On notera que **les moyens de communication électronique et leurs caractéristiques techniques ne doivent pas être discriminatoires et restreindre l'accès des opérateurs économiques aux marchés publics (article R.2132-8 du Code de la commande publique).**

Ils doivent être communément disponibles et compatibles avec les technologies de l'information et de la communication généralement utilisées.

Les garanties en termes de confidentialité, d'intégrité et de sécurité des échanges sont à la charge de l'acheteur [257] (article R.2132-9 du Code de la commande publique).

Enfin, les moyens de communication devront remplir les conditions posées à l'arrêté du 22 mars 2019 relatif aux exigences minimales des moyens de communication électronique utilisés dans la commande publique et constitutif de l'annexe 8 du code de la commande publique. Y sont notamment traitées les exigences d'horodatage, de coffre-fort numérique et de lettres recommandées électroniques.

Ces conditions générales précisées, lorsque la voie électronique est obligatoire, les modalités posées par le pouvoir réglementaire doivent être respectées à chacune des phases concernées.

(257) V. pour une illustration d'application de cette disposition : Conseil d'Etat, 23 septembre 2021, Sté Alstom-Aptis c/RATP, req. n°449250, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000044097089.

c. La voie électronique et l'engagement de la procédure de passation

La mise à disposition électronique des documents de la consultation est régie par les articles R.2132-1 à R.2132-6 du Code de la commande publique. La voie électronique ne remet pas en cause les règles de fond applicables quant à la nature et au contenu de l'information et que l'acheteur doit respecter.

Les informations relatives à la consultation doivent intégralement être publiées sur le profil de l'acheteur, sauf exceptions expressément prévues par le Code de la commande publique. En fonction des procédures concernées, les informations seront également publiées par voie électronique dans le Bulletin officiel des annonces des marchés publics et/ou au journal officiel de l'Union européenne.

L'arrêté du 22 mars 2019 fixant les modalités de mise à disposition des documents de la consultation et de la copie de sauvegarde [259] **précise également que l'accès aux documents de consultation doit être « *gratuit, complet, direct et sans restriction* » (article 1er).** Le cas où les documents seraient trop volumineux pour être téléchargés y est traité.

On notera qu'auparavant, les décisions rendues par les juridictions administratives divergeaient quant à la portée de l'information d'un candidat par courriel portant sur des documents complémentaires relatifs à la consultation [259]. Désormais, l'alinéa 2 de l'article 1er de l'arrêté du 22 mars 2019 fixant les modalités de mise à disposition des documents de la consultation et de la copie de sauvegarde détermine que les opérateurs économiques peuvent indiquer à l'acheteur une adresse électronique « *afin que puissent lui être communiquées les modifications et les précisions apportées aux documents de la consultation* ».

En conséquence, la communication d'informations complémentaires par courriel est juridiquement admise sous réserve que l'opérateur ait communiqué une adresse électronique et que ladite information soit communiquée sur celle-ci. Il appartiendra à l'acheteur de prouver un tel envoi ; ce qui sera facilité selon le niveau de sécurité des fonctionnalités garanti par le profil acheteur (la plateforme) utilisé.

(258) Entré en vigueur le 1er avril 2019, cet arrêté constitue l'annexe 6 du Code de la commande publique.

(259) Ord. Réf. TA Toulouse, du 29 mars 2010, n°1001105 : en l'espèce, le candidat avait été prévenu par courriel de documents complémentaires et les juges avaient considéré que ledit courriel ne présentait aucun élément de nature à attirer l'attention de son destinataire. A contrario, d'autres juridictions ayant considéré que l'obligation d'information avait été remplie par l'émission d'un courrier électronique : v. par ex. Ord. Ref. TA Poitiers, du 3 janvier 2012, n°112784, E. Caprioli, Courrier électronique et preuve, Comm. Com. électr. n° 5, Mai 2012, comm. 59.

d. La voie électronique et les phases de candidatures et d'offres

Les exigences relatives aux candidatures et aux offres électroniques sont traitées dans la partie réglementaire du Code de la commande publique. Là encore, il n'est plus fait aucune référence spécifique à la **voie électronique dans la mesure où elle constitue désormais la voie obligatoirement utilisée**.

En application de l'article R.2143-4 du Code de la commande publique, l'acheteur « *accepte que le candidat présente sa candidature sous la forme d'un document unique de marché européen et constituant un échange de données structurées, établi conformément au modèle fixé par le règlement de la Commission européenne établissant le formulaire type pour le document unique de marché européen, en lieu et place de la déclaration sur l'honneur et des renseignements mentionnés à l'article R. 2143-3.* ». **Ceci implique que le profil acheteur (la plateforme de dématérialisation) des marchés publics soit en mesure de recevoir ce type de document**.

En outre, en application de l'article R.2142-1 du Code de la commande publique, il appartient à l'acheteur d'indiquer les conditions de participation à la procédure de passation relatives aux capacités du candidat « *ainsi que les moyens de preuve acceptables* ».

L'information relative aux conditions de candidature doit être donnée dans l'avis d'appel à concurrence ou dans l'invitation à confirmer l'intérêt ou, si un tel avis ou une telle invitation n'existe pas, dans les documents de consultation. À cet égard, **les articles R.2143-13 et R.2143-14 du Code de la commande publique déterminent les documents justificatifs et moyens de preuve que les candidats ne sont pas tenus de fournir car l'acheteur peut soit les obtenir directement soit par un autre biais électronique officiel (article R.2143-13, 1° et 2°)** [260].

Au demeurant, le pouvoir réglementaire tend à alléger la transmission des documents justificatifs pour prouver la capacité juridique du candidat en menant des expérimentations, qui à terme pourraient devenir la règle [261].

(260) V. sur ce point les réponses concrètes apportées par la DAJ, dans son « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les acheteurs », points A51, A52 et A53, notamment en ce qui concerne l'utilisation d'un coffre-fort électronique ainsi que le principe du « Dites-le nous une fois », réf. cit. supra.

(261) Cf. nos développements dans la partie relative à la rationalisation des pièces justificatives dans le présent Vade-Mecum.

Par ailleurs, en ce qui concerne les candidatures comme les offres, les règles de fond et de forme sont strictement posées. A cet égard, le respect des délais impartis est essentiel. **C'est pourquoi l'horodatage du profil acheteur doit être qualifié comme l'impose l'annexe 7 du Code de la commande publique.**

En ce qui concerne l'utilisation d'une signature électronique dans le cadre des candidatures et des offres, il convient de relever que l'actuel Code de la commande publique n'impose pas une telle formalité à ces stades. Pour autant, l'acheteur public semble avoir la possibilité de proposer ou d'imposer aux candidats et soumissionnaires la signature électronique des documents transmis (262). Le cas échéant, il devra en informer dûment les candidats et soumissionnaires.

(262) V. en ce sens, DAJ, « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les opérateurs économiques », points E71 et E72, réf. cit. supra.

En tout état de cause, **l'acheteur public devrait intégrer dans ses documents pré-contractuels une «** *convention de preuves* **». Ces dispositions juridiques lui permettront d'établir les moyens de preuve des modalités d'échanges (formats, formes, support, datation électronique…) acceptables dans la phase de candidature et dans la phase des offres.**

On notera ici que le pouvoir réglementaire n'utilise pas le terme de preuve « *recevable* » dans la mesure où en droit administratif, la preuve est libre. Il s'agit là d'une différence majeure avec le droit civil et le droit de la preuve des actes sous seing privé ; **étant noté que le candidat qui souhaitera répondre à un marché public n'aura de toute façon pas d'autre choix que d'accepter la convention de preuve définie par l'acheteur. Pour autant, le moyen de preuve devra être suffisamment fiable pour emporter la conviction du juge.**

On notera également que le candidat ou le soumissionnaire a la possibilité de faire parvenir **une copie de sauvegarde de sa candidature et de son offre** en application de l'article R.2132-11 du Code de la commande publique. Cette copie doit être remise dans les délais impartis dans la procédure. De plus, elle doit respecter les dispositions posées désormais par l'arrêté du 22 mars 2019 fixant les modalités de mise à disposition des documents de la consultation et de la copie de sauvegarde et constitutif de l'annexe 6 du Code de la commande publique.

e. La voie électronique et l'achèvement de la procédure

L'achèvement de la procédure par voie électronique doit intégrer six fonctionnalités : l'information des candidats évincés, la signature électronique du contrat, sa notification, la gestion des avis d'attribution et la conservation des informations.

f. L'information des candidats évincés

En application de l'article R.2181-1 du Code de la commande publique, toute personne évincée d'un marché public doit être informée de la décision du rejet de sa candidature ou de son offre par l'acheteur. Concrètement, la plateforme utilisée (« *profil d'acheteur* ») doit donc gérer ce type d'information afin que l'acheteur soit en mesure de prouver la réalité de ce type d'information et sa réalisation « *sans délai* ».

g. La signature électronique du marché

En ce qui concerne la signature du contrat, l'article R.2182-3 du Code de la commande publique précise que le marché peut être signé électroniquement.

À cet égard, plusieurs remarques méritent une attention particulière.

Premièrement, **la signature électronique des marchés semble être une possibilité** (263). Néanmoins, à terme, il est fort probable que la signature électronique des marchés devienne une formalité obligatoire. C'est pourquoi les acheteurs publics sont incités à y recourir. Dès lors, l'acheteur peut l'imposer. Le cas échéant, il doit obligatoirement l'indiquer dans les documents de consultation adéquats. On notera à cet égard que la Direction des Affaires Juridiques considère, dans son « *Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les opérateurs économiques* » précité, que si l'attributaire d'un marché est dans l'incapacité de signer électroniquement le contrat dans le délai requis, deux cas de figure sont envisageables :

+ *« Si l'obligation de signer l'offre finale de manière électronique figurait parmi les exigences formulées dans les documents de la consultation. Il appartient donc à l'acheteur de demander au candidat retenu de régulariser son offre. Si cette régularisation n'est pas possible, il convient alors d'attribuer le marché au candidat dont l'offre est arrivée en seconde position.*

(263) La DAJ apporte à cet égard un certain nombre de précisions à titre d'avertissement : « La mise en place de la signature électronique suppose un certain nombre de préalables. Les acheteurs et les entreprises doivent avoir acquis les certificats de signature. Surtout, les entreprises doivent avoir précisé l'organisation interne de leur entité et désigné, en leur sein, les personnes qui seront habilitées à signer au nom de l'entité. Cette organisation nécessite un délai. C'est la raison pour laquelle les textes n'ont pas mentionné l'usage de la signature électronique au titre des obligations prévues pour octobre 2018. L'absence d'obligation de recours à la signature électronique n'interdit pas pour autant d'y recourir. Si l'acheteur et l'attributaire du marché sont capables de signer électroniquement le marché, rien ne doit les retenir de le faire. » in DAJ, « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les acheteurs », page 28. On notera que la DAJ réserve d'ailleurs des développements spécifiques à la signature électronique, voir notamment les points E72 et suivants :https://www.economie.gouv.fr/files/files/directions_services/daj/marches_publics/dematerialisation/20180601_Guide-MP-dematerialisation-2018-OE.pdf.

+ *Si une telle obligation n'a pas été mentionnée dans les documents de la consultation, l'offre non signée ne peut être considérée comme irrégulière. Il ne peut donc être demandé à l'attributaire retenu de régulariser son offre, pas plus que l'acheteur ne peut attribuer le marché au candidat dont l'offre est arrivée en seconde position.*

  L'entreprise doit donc imprimer le marché et le signer de manière manuscrite, le transmettre, après l'avoir scanné, par voie électronique à l'acheteur (c'est une copie seulement), l'original signé par elle étant transmis par voie papier après la notification du marché, notification qui met fin à l'obligation des échanges dématérialisés. [264]» .

Deuxièmement, si le marché est signé électroniquement (volontairement ou obligatoirement de par la volonté de l'acheteur), alors la signature électronique du contrat doit respecter les modalités posées par l'arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique (constitutif de l'annexe 12 du Code de la commande publique).

À titre principal, l'article 2 de l'arrêté indique qu'il s'agit d'une signature électronique avancée reposant sur un certificat qualifié au sens du Règlement européen n°910/2014 dit Règlement eIDAS [265]. Sans rentrer plus avant dans le détail de ce texte [266], il convient toutefois de relever que :

+ *« II. - Le certificat de signature électronique qualifié entre au moins dans l'une des catégories suivantes :*
+ *1° Un certificat qualifié délivré par un prestataire de service de confiance qualifié répondant aux exigences du règlement susvisé ;*
+ *2° Un certificat délivré par une autorité de certification, française ou étrangère, qui répond aux exigences équivalentes à l'annexe I du règlement susvisé. ».*

En outre, sont précisés les formats de signature électronique acceptés (article 3), le libre choix du signataire quant au dispositif de création de signature électronique utilisé (article 4) et les modalités de vérification de la signature (articles 5 et 6). La possibilité d'utiliser un parapheur électronique est également posée (article 7).

Troisièmement, la Direction des Affaires Juridiques a indiqué **que le mandat de signature électronique établi par les opérateurs économiques au bénéfice d'un mandataire pour qu'il appose sa signature électronique en leur nom et pour leur compte est juridiquement admis.**

(264) DAJ, « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les acheteurs », point E73, réf. cit. supra.

(265) Règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/C, J.O.UE L.257 du 28 août 2014 p.73 s., disponible sous le lien : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.FRA.

(266) Il est renvoyé à cet égard aux développements relatifs aux signatures électroniques avancées reposant sur un certificat qualifié traitées par ailleurs dans le présent Vade-Mecum.

Toutefois, le mandat doit expressément prévoir une telle signature électronique (signature électronique dans le cadre de la commande publique) et mentionner clairement que c'est le mandant (l'opérateur économique) qui est engagé par le contrat signé électroniquement et non le mandataire [267]. Les contrats proposés par les Prestataires de services de confiance devront prévoir de tel mandat le cas échéant.

h. La notification du marché

En ce qui concerne la notification du marché, on notera l'importance des dates, et par voie de conséquence de la fiabilité des procédés d'horodatage utilisé dans le cadre des notifications par voie électronique (article R.2182-4 et R.2182-5 du Code de la commande publique notamment).

Il sera en effet essentiel d'être en mesure de rapporter la preuve du respect des délais en la matière et par là même la preuve de la fiabilité du procédé de datation électronique mis en œuvre. **C'est pourquoi l'horodatage du profil acheteur doit être qualifié comme l'impose l'annexe 7 du Code de la commande publique**.

i. Les avis d'attribution du marché

En ce qui concerne les avis d'attribution, la voie électronique devra respecter les dispositions des articles R.2183-1 à R.2183-7 du Code de la commande publique.

j. Les modalités de conservation des informations

Enfin, **en ce qui concerne les modalités de conservation des informations [268], aucun arrêté n'a été adopté spécifiquement pour l'archivage électronique des documents et contrats dans le cadre de la commande publique**.

Il convient donc d'appliquer les règles communément admises en matière d'archivage électronique pour les personnes publiques [270]. En conséquence, la conservation des documents devra garantir l'intégrité des informations dans le temps ainsi que leur accessibilité et leur intelligibilité.

(267) V. DAJ, « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les opérateurs économiques », avril 2019, point A73, réf. cit. supra.

(269) Les durées de conservation sont respectivement posées à l'article R.2184-12 du Code de la commande publique pour les candidatures, les offres et les documents relatifs à la procédure de passation (minimum 5 ans à compter de la date de signature du marché) et à l'article R.2184-13 du Code de la commande publique pour les pièces constitutives du marché (minimum 5 ans pour les marchés de fournitures ou de services et minimum 10 ans pour les marchés de travaux, de maîtrise d'œuvre ou de contrôle technique à compter de la fin de l'exécution du marché).

(268) A cet égard, on pourra regretter que la DAJ reste évasive, cf. « Guide très pratique version 4.0 de la dématérialisation des marchés publics pour les opérateurs économiques », avril 2019, points A83 et A84, réf. cit. supra

k. Les données essentielles

Dans le cadre des informations relatives à l'achat, l'article L. 2196-2 du Code de la commande publique prévoit que « ***l'acheteur rend accessibles, sous un format ouvert et librement réutilisable, les données essentielles du marché*** ». Cette obligation doit se faire dans le respect des dispositions réglementaires posées par l'**arrêté du 22 mars 2019 relatif aux données essentielles dans la commande publique (constitutif de l'annexe 15 du Code de la commande publique**) qui fixe la liste des données concernées et les modalités de leur accessibilité.

À titre dérogatoire, les données essentielles peuvent ne pas être communiquées par l'acheteur si la divulgation des informations violait le secret des affaires ou nuisait à une concurrence loyale entre les opérateurs économiques.

En outre, il est prévu que les opérateurs économiques puissent, à la demande de l'acheteur, consentir à la divulgation de certaines informations confidentielles précisément désignées. De plus, des mesures supplémentaires pour protéger les informations communiquées peuvent être imposées par l'acheteur à l'opérateur afin de protéger leur confidentialité.

L'obligation de communiquer les données essentielles est enfin exclue si la divulgation desdites informations est contraire à l'ordre public.

2. La digitalisation des marchés de défense ou de sécurité

À la différence des autres marchés, les communications et les échanges d'informations dans le cadre des marchés de défense ou de sécurité ne doivent pas être obligatoirement réalisés par voie électronique.

En application de l'article L. 2332-2 du Code de la commande publique, la voie électronique est donc une simple possibilité. Il appartiendra à l'acheteur d'en apprécier la pertinence, et le cas échéant, d'être en mesure de la démontrer eu égard à l'objet du marché. De plus, lorsque la voie électronique sera retenue par l'acheteur public, elle ne sera légale que dans les limites suivantes :

+ **La confidentialité des informations concernées par le marché**, tant celles qui émanent de l'opérateur économique que de l'acheteur public, justifie un régime de communication et d'échanges particulier. Tel est l'objet de l'article L. 2332-1 du Code de la commande publique. À cet égard, des exigences spécifiques visant à protéger la confidentialité des informations communiquées peuvent notamment être imposées par l'acheteur. Le cas échéant, les candidats ou soumissionnaires devront en être informés préalablement dans les documents d'information adéquats.

+ Si les échanges et les communications peuvent être réalisés par voie électronique en application de l'article L. 2332-2 du Code de la commande publique, **aucune disposition ne traite des candidatures ou des offres par voie électronique**.

  On notera toutefois que l'article R. 2343-7 du Code de la commande publique renvoie à l'article R.2143-5 pour les documents justificatifs et autres moyens de preuve, et l'article R. 2343-9 aux articles 2143-7 à R. 2143-9 du Code de la commande publique pour les documents justificatifs et autres moyens de preuve de l'absence de motifs d'exclusion. Enfin, les articles R. 2343-14 et R. 2343-15 du Code de la commande publique laissent une certaine latitude aux acheteurs qui peuvent, ou non, permettre aux candidats de ne pas fournir un certain nombre de justificatif alors qu'il s'agit d'une obligation de recevabilité dans le cadre des marchés classiques (sur la base des articles R. 2143-13 et suivants).

+ **En ce qui concerne la signature électronique**, l'article R.2382-3 du Code de la commande publique renvoie à l'article R. 2182-3 applicable aux marchés « *classiques* ». Nous renvoyons donc à nos développements à cet égard (voir supra point II.B.1.d et g).

+ **La facturation électronique est une faculté et non une obligation pour les marchés de défense conclus avec l'État ou ses établissements publics en application des articles L. 2392-1 à L. 2392-4 du Code de la commande publique**.

Cette exception s'explique par un besoin de confidentialité renforcé dans certains cas.

On notera que le texte ne vise pas les marchés de sécurité conclus par les collectivités territoriales [269]. Il s'ensuit qu'a priori de tels marchés doivent faire l'objet d'une facturation électronique dans les conditions posées aux articles applicables aux marchés « *classiques* » [270]. En revanche, lorsque des factures « sous forme électronique » sont émises pour des marchés de défense et de sécurité de l'État, elles sont régies par les articles L. 2392-5 à L. 2392-7 du Code de la commande publique qui permettent d'exclure cette catégorie de marchés à la facturation électronique.

3. La digitalisation des contrats de concession

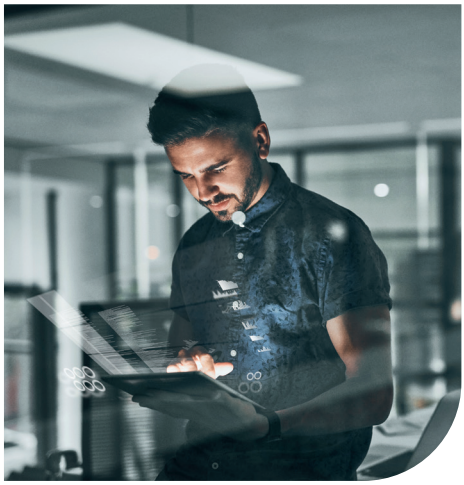
a. Principes généraux

À la différence des marchés publics, l'article L. 3122-5 du Code de la commande publique indique que les communications et les échanges d'informations réalisés dans le cadre de la procédure de passation des contrats de concession **peuvent** être réalisés par voie électronique.

Il s'agit donc d'une possibilité, qui est toutefois strictement encadrée. Ainsi, dès lors que la voie électronique est applicable, on retrouve pour l'essentiel, la logique juridique attachée aux « *moyens de communication et d'échanges* » adoptés dans le cadre des marchés publics.

Il s'ensuit que les **dispositions de l'arrêté du 22 mars 2019 relatif aux exigences minimales des moyens de communication électronique utilisés dans la commande publique s'appliquent aux contrats de concession. Il en va de même des dispositions de l'arrêté du 22 mars 2019 fixant les modalités de mise à disposition des documents de la consultation et de la copie de sauvegarde auquel renvoient les articles R. 3122-15 et R. 3122-17 du Code de la commande publique pour les concessions**.

Sur ces points, il est renvoyé à nos commentaires relatifs aux marchés publics supra.



(269) Étant noté que les marchés de défense sont de droit exclusivement de la compétence de l'État.

(270 Il est donc renvoyé en cet endroit à nos développements supra.

En ce qui concerne l'arrêté du 22 mars 2019 relatif aux fonctionnalités et exigences minimales des profils d'acheteurs, certaines nuances doivent être apportées.

L'article R. 3122-9 du Code de la commande publique impose que les documents de la consultation soient mis à disposition par voie électronique « ***sur un profil d'acheteur*** » tel que défini par l'article R. 3122-10 du Code de la commande publique. Cette définition rejoint celle donnée à l'article R.2132-3 du Code de la commande publique pour les marchés.

Ce faisant, les modalités posées aux articles R. 3122-13 à R. 3122-18 du Code de la commande publique reprennent la logique des modalités fixées pour les moyens de communication et des échanges d'information pour les marchés, et l'on retrouve peu ou prou **les conditions posées pour le profil d'acheteur** dans les contrats de concession.

Pour l'essentiel les développements faits pour les marchés publics se retrouvent donc ici, sous réserve des principales différences ci-après :

+ **Les dérogations à l'obligation de mise à disposition des documents par voie électronique sont expressément et strictement entendues** (en application de l'article R. 3122-11 du Code de la commande publique). Comme l'indiquent les termes « *circonstances dûment justifiées* », « *raisons de sécurité exceptionnelles* », « *caractère particulièrement sensible d'informations* », « *niveau de protection très élevé* », le fait de transmettre les documents informatifs par un autre moyen que la voie électronique doit revêtir un caractère exceptionnel et strictement justifié.

+ L'article 3 de l'arrêté du 22 mars 2019 fixant les fonctionnalités et exigences minimales des profils d'acheteurs (constitutif de l'annexe 7 du Code de la commande publique) détermine les actions que le profil d'acheteur permet d'effectuer pour les autorités concédantes et pour les opérateurs économiques.

  Il convient de relever que le **profil d'acheteur offre moins de fonctionnalités dans le cadre des contrats de concession que pour les marchés publics**. Les profils d'acheteur (plateformes) proposés aux « *acheteurs*» doivent en tenir compte.

En ce qui concerne les autres exigences, elles sont déclinées ci-après selon les différentes phases concernées.

b. La voie électronique et l'engagement de la procédure de passation

L'article L. 3122-4 du Code de la commande publique pose pour principe que l'autorité concédante doit offrir, « *par voie électronique, un accès gratuit, libre, direct et complet aux documents de la consultation, dans les conditions et sous réserve des exceptions prévues par voie réglementaire*. ».

Les articles R. 3122-2 à R. 3122-3 du Code de la commande publique déterminent les supports de publication de l'avis de concession et l'arrêté du 22 mars 2019 fixe le modèle d'avis pour la passation des contrats de concession (annexe 21 du Code de la commande publique). On notera à cet égard que notamment le journal officiel de l'Union européenne (JOUE) comme le bulletin officiel des marchés publics (BOAMP) qui en font partie sont diffusés sous forme électronique. D'ailleurs, l'article R. 3122-4 du Code de la commande publique précise que les avis destinés à être publiés au JOUE sont transmis par **voie électronique** à l'organisme européen compétent.

Il est également intéressant de noter que le Code de la commande publique (article R. 3122-6) indique que **l'autorité concédante « *doit être en mesure de faire la preuve de la date d'envoi des avis de concession* »**.

L'utilisation d'un horodatage qualifié conformément à l'article 5 de l'arrêté du 22 mars 2019 relatif aux exigences minimales des moyens de communication électronique utilisés dans la commande publique permettra de répondre à cette exigence.

c. La voie électronique dans les phases de candidature et d'offre

De même que pour les dispositions relatives aux marchés publics, **le basculement vers la voie électronique n'a pas remis en cause les principes fondamentaux régissant les contrats de concession**. Sur le fond, la voie électronique n'a donc pas engendré de véritables changements. Ceci étant, elle a permis une évolution des modalités de transmission des documents, en ce compris pour certaines pièces justificatives dans le cadre des marchés publics.

En ce qui concerne les contrats de concession, les textes sont moins souples et l'allégement des pièces justificatives ainsi que l'optimisation de leur communication apparaissent plus timides.

À titre d'illustration, on notera qu'il résulte de l'arrêté du 22 mars 2019 relatif aux fonctionnalités et exigences minimales des profils d'acheteurs que :

+ Pour les marchés publics, le profil d'acheteur permet à l'acheteur d'accéder à un service de courrier électronique (article 1er.I.7°) et de répondre à des questions soumises par les entreprises (article 1er.I.9°). Ces fonctionnalités ne se retrouvent pas pour les contrats de concession.

+ Pour les marchés publics, la plateforme « *profil acheteur* » permet aux acheteurs d' « *Obtenir les documents justificatifs et moyens de preuve lorsque ceux-ci peuvent être directement obtenus auprès d'autres administrations* » (article 1er.I.10°) et aux opérateurs économiques ; alors que pour les contrats de concession une telle action n'est pas prévue étant noté que le profil acheteur doit toutefois permettre d'importer les données essentielles prévues par l'arrêté du 22 mars 2019 (annexe 15 du Code de la commande publique) lorsqu'elles sont disponibles dans un autre système d'information (article 3.I.5°).

+ Pour les marchés publics, il est expressément indiqué que le profil d'acheteur doit permettre à l'opérateur économique de déposer ses candidatures et offres y compris les offres signées électroniquement (article 1er.II.8°) ; à la différence des contrats de concession où il est seulement question du dépôt des offres sans plus de précision.

d. La voie électronique et l'achèvement de la procédure

En ce qui concerne l'information des candidats et soumissionnaires évincés, les articles R. 3125-1 à R. 3125-4 du Code de la commande publique ne font pas obstacle à la voie électronique reconnue dans son principe à l'article L. 3122-5 du Code de la commande publique.

En ce qui concerne la signature du contrat de concession, elle est admise dans son principe à l'article R. 3125-5 du Code de la commande publique. Les modalités en sont fixées par l'arrêté du 19 mars 2019 relatif à la signature électronique des contrats de la commande publique (annexe 12 du Code de la commande publique). Elles sont identiques à celles posées pour les marchés publics. **En conséquence, le procédé de signature électronique conforme auxdites modalités pourra être utilisé pour signer les contrats aussi bien dans le cadre des marchés publics que des concessions.**

Pour rappel, à titre principal, l'article 2 de l'arrêté indique qu'il s'agit d'une **signature électronique avancée reposant sur un certificat qualifié au sens du Règlement européen n°910/2014 dit Règlement eIDAS** (271).

(271) Règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/C, J.O.UE L.257 du 28 août 2014 p.73 s., disponible sous le lien : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.FRA. Il est renvoyé à cet égard aux développements relatifs aux signatures électroniques avancées reposant sur un certificat qualifié traitées par ailleurs dans le présent Vade-Mecum.

En outre, sont précisés **les formats de signature électronique acceptés (article 3), le libre choix du signataire quant au dispositif de création de signature électronique utilisé (article 4) et les modalités de vérification de la signature (articles 5 et 6). La possibilité d'utiliser un parapheur électronique est également posée (article 7).**

L'article R. 3125-7 du Code de la commande publique pose quant à lui les modalités de la publicité de l'avis d'attribution.

e. Les données essentielles et les contrats de concession

En application de l'article L. 3131-1 du Code de la commande publique, « ***l'autorité concédante rend accessibles, sous un format ouvert et librement réutilisable, les données essentielles du contrat de concession*** ».

Cette obligation doit se faire dans le respect des dispositions réglementaires posées par **l'arrêté du 22 mars 2019 relatif aux données essentielles dans la commande publique** (constitutif de l'annexe 15 du Code de la commande publique) qui fixe la liste des données concernées et les modalités de leur accessibilité.

De plus, l'autorité concédante peut ne pas communiquer les données essentielles si les conditions posées à l'article L. 3122-3 du Code de la commande publique sont remplies. Il en est notamment ainsi si la divulgation des informations violait le secret des affaires ou nuisait à une concurrence loyale entre les opérateurs économiques.

En outre, il est prévu que les opérateurs économiques puissent, à la demande des autorités concédantes, consentir à la divulgation de certaines informations confidentielles précisément désignées. De plus, **des mesures supplémentaires pour protéger les informations communiquées peuvent être imposées par l'autorité concédante à l'opérateur afin de protéger leur confidentialité**.

L'obligation de communiquer les données essentielles est enfin exclue si la divulgation desdites informations est contraire à l'ordre public (article L. 3131-1 du Code de la commande publique).

4. Les procédures électroniques spécifiques

Dès 2006, le Code des marchés publics admettait en son article L. 2125-1 certaines procédures exclusivement et spécifiquement réalisables par voie électronique. L'Ordonnance n° 2018-1074 du 26 novembre 2018 portant partie législative du Code de la commande publique [272] a entériné ces techniques d'achat qui consistent en :

+ Des systèmes d'acquisition dynamique ;
+ Des catalogues électroniques ;
+ Des enchères électroniques.

Toutes ces techniques d'achat doivent être réalisées dans le respect des exigences de sécurité minimales posées par l'arrêté du 22 mars 2019 relatif aux exigences minimales des moyens de communication électronique utilisés dans la commande publique (annexe 8 du Code de la commande publique). Seuls les aspects relatifs au caractère électronique de ces techniques d'achat sont brièvement exposés [273].

a. Système d'acquisition dynamique

L'article L. 2125-1, 4° du Code de la commande publique définit le système d'acquisition dynamique, comme une technique d'achat « *qui permet de présélectionner un ou plusieurs opérateurs économiques, pour des achats d'usage courant,* ***selon un processus ouvert et entièrement électronique*** ».

Les modalités d'utilisation propres aux systèmes d'acquisition dynamique sont prévues aux articles R. 2162-37 et suivants du Code de la commande publique ; étant noté que cette technique d'achat n'est pas visée pour les marchés de la défense ou de la sécurité (article L. 2325-1 du Code de la commande publique).

A titre principal, il est intéressant de relever qu'en application de l'article R. 2162-39 du Code de la commande publique, pour mettre en place un système d'acquisition dynamique, l'acheteur doit publier un avis d'appel à la concurrence, lequel devra notamment indiquer la période de validité du système.

De plus, si la valeur du besoin est égale ou supérieure aux seuils de la procédure formalisée, la notification à la Commission européenne de tout changement de la durée de validité du système d'acquisition est obligatoire conformément aux formulaires types établis (article R. 2162-40 du Code de la commande publique).

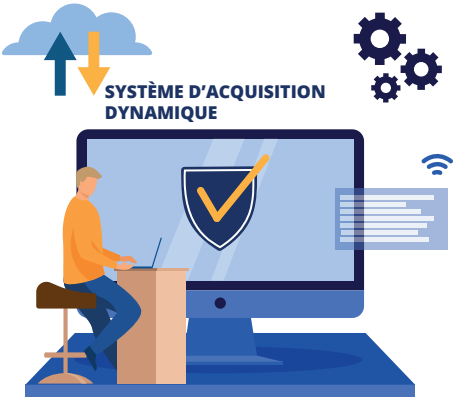
(272) Réf. cit. supra.

(273) La présentation qui suit se focalise donc sur les aspects juridiques des échanges électroniques dans le cadre de ces procédures ; les règles et critères permettant de déterminer si lesdites procédures sont ou non applicables à l'achat concerné ne sont en revanche pas traitées.

Lorsque l'acheteur utilise cette technique d'achat, les documents de la consultation doivent être librement, directement et complètement accessibles par voie électronique, et ce, pendant toute la durée de validité du système (article R. 2162-41 du Code de la commande publique).

En application de l'article R. 2162-42 du Code de la commande publique, les documents doivent contenir des informations sur les achats envisagés (nature et quantité) et sur le système d'acquisition dynamique, à savoir, toutes les informations nécessaires dont les modalités de fonctionnement du système, l'équipement électronique utilisé, et les arrangements et spécifications techniques de connexion, voire, le cas échéant, s'il y a une subdivision en catégories de produits, de services ou de travaux objets de l'achat.

En ce qui concerne les candidatures, l'article R. 2162-43 du Code de la commande publique précise que « *Tout opérateur économique peut demander à participer au système d'acquisition dynamique pendant sa durée de validité.* ».



Les articles R. 2162-44 et suivants du Code de la commande publique déterminent les règles de forme et de délai imposées. L'article R. 2162-49 du Code de la commande publique fixe les conditions dans lesquelles les candidats doivent être invités à présenter une offre. La combinaison du système d'acquisition dynamique avec la présentation des offres sous la forme d'un catalogue électronique est envisagée à l'article R. 2162-56 du Code de la commande publique.

Dans la phase d'achèvement de la procédure, les modalités de conservation des informations sont posées aux articles R. 2184-1 et suivants du Code de la commande publique.

b. Catalogue électronique

L'article L.2125-1, 5° du Code de la commande publique définit le catalogue électronique comme la technique d'achat « *qui permet la présentation d'offres ou d'un de leurs éléments de manière électronique et sous forme structurée* ». En application de l'article L. 2325-1 du Code de la commande publique, le catalogue électronique peut être utilisé pour passer un marché de défense ou de sécurité.

Les modalités d'utilisation des catalogues électroniques sont détaillées aux articles R. 2162-52 et suivants du Code de la commande publique.

À titre principal, on notera que **le catalogue électronique peut être exigé par l'acheteur ou simplement autorisé**.

Dans tous les cas, l'acheteur doit indiquer dans les documents de la consultation « *toutes les informations requises en ce qui concerne le format, l'équipement électronique utilisé ainsi que les modalités de connexion et les spécifications techniques du catalogue* » (article R. 2162-53, alinéa 2 du Code de la commande publique) ; étant précisé que : « *Les catalogues électroniques sont établis par les candidats ou les soumissionnaires conformément aux spécifications techniques et au format prévus par l'acheteur* » (article R. 2162-54 du Code de la commande publique).

Les informations relatives aux caractéristiques du catalogue électronique doivent être communiquées conformément aux règles définies pour la communication des documents de consultation par voie électronique telles qu'exposées supra pour les marchés. Il y est ici renvoyé.

En outre, le catalogue doit pouvoir être actualisé dans certaines procédures.

c. Enchères électroniques

L'article L. 2125-1, 6° du Code de la commande publique détermine que les enchères électroniques « ***ont pour but de sélectionner par voie électronique, pour un marché de fournitures d'un montant égal ou supérieur aux seuils de la procédure formalisée, des offres en permettant aux candidats de réviser leurs prix à la baisse ou de modifier la valeur de certains autres éléments quantifiables de leurs offres*** »[(274)]. Il s'agit donc d'enchères inversées.

En application de l'article L. 2325-1 du Code de la commande publique, les enchères électroniques peuvent être utilisées pour passer un marché de défense ou de sécurité. Cette technique d'achat est néanmoins **réservée aux marchés de fournitures (les marchés de services et de travaux en sont donc exclus) d'un montant égal ou supérieur aux seuils de la procédure formalisée**.

Les modalités d'utilisation des enchères électroniques sont fixées aux articles R. 2162-57 et s. du Code de la commande publique. L'article R. 2162-59 du Code de la commande publique impose notamment que les documents de la consultation de l'enchère électronique comprennent : « *5°) Les informations pertinentes sur le dispositif électronique utilisé et sur les modalités et spécifications techniques de connexion*. ».

(274) V. Sur le sujet : Anne Cantero, Prix et enchères électroniques, Contrats publics, n°199, juin 2019, p.61 et s.

Le classement des offres doit se faire sur la base d'un traitement automatisé (article R. 2162-60 du Code de la commande publique). À cet égard, les invitations à présenter les offres sont strictement encadrées afin que l'égalité des candidats et le principe de transparence dans la commande publique soient respectés (articles R. 2162-61 et suivants du Code de la commande publique).

L'article R. 2162-62 du Code de la commande publique exige notamment que l'invitation « *adressée à chaque soumissionnaire est accompagnée du résultat de l'évaluation complète de son offre réalisée* » (alinéa 1), étant précisé que ladite invitation doit également mentionner « *la formule mathématique qui déterminera, lors de l'enchère électronique, les reclassements automatiques en fonction des nouveaux prix ou des nouvelles valeurs présentés. Cette formule intègre la pondération de tous les critères fixés pour déterminer l'offre économiquement la plus avantageuse, telle qu'indiquée dans l'avis de marché ou dans un autre document de la consultation. Le cas échéant, les fourchettes sont réduites à une valeur déterminée* ».

De plus, « *Lorsque des variantes sont autorisées, une formule distincte est fournie pour chaque variante* ».

L'article R. 2162-64 du Code de la commande publique implique **une exigence d'instantanéité des informations à communiquer par l'acheteur aux soumissionnaires, l'identité de ces derniers devant en revanche rester secrète pendant tout le déroulement de la procédure**.

En application de ces textes réglementaires, **les modalités de déroulement et de clôture des enchères nécessitent des garanties technologiques afin que les obligations juridiques soient respectées et que la preuve du respect de ces exigences puisse être rapportée.**

À **défaut, la légalité du marché attribué risquerait de ne pouvoir être établie…**

5. La facturation électronique dans la commande publique

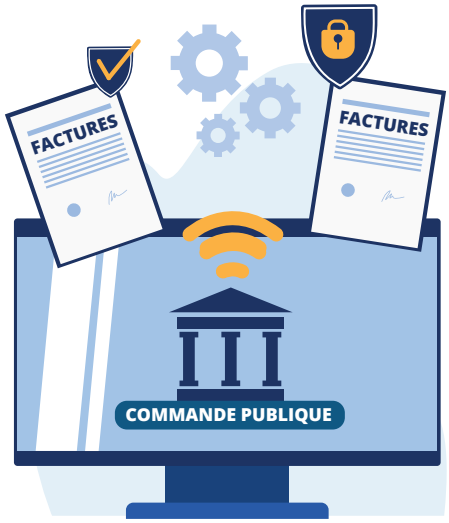
La loi n° 2014-1 du 2 janvier 2014 habilitant le Gouvernement à simplifier et sécuriser la vie des entreprises [275] a autorisé le gouvernement à prendre par ordonnance toutes mesures relevant du domaine de la loi afin « ***2° De permettre le développement de la facturation électronique dans les relations de l'État, des collectivités territoriales et de leurs établissements publics avec leurs fournisseurs, par l'institution d'une obligation, applicable aux contrats en cours, de transmission dématérialisée des factures****, entrant en vigueur de façon progressive pour tenir compte de la taille des entreprises concernées et de leur capacité à remplir cette obligation* ».

C'est sur ce fondement qu'avait été adoptée l'ordonnance du 26 juin 2014 [276]. Cette ordonnance imposait notamment aux titulaires de marchés et aux sous-traitants « *admis au paiement direct de contrats conclus par l'État, les collectivités territoriales et les établissements publics* » de transmettre leurs factures sous forme électronique.

En contrepartie, l'État, les collectivités territoriales et les établissements publics devaient accepter les factures sous forme électronique si elles étaient transmises par le biais du « ***portail de facturation*** » mis à disposition par l'État.

Toutefois, il était prévu que **la mise en œuvre de l'obligation de facturation électronique dans le cadre de la commande publique (marché public et contrat de concession) se fasse progressivement**. Imposée aux grandes entreprises et personnes publiques à partir du 1er janvier 2017, la facturation électronique est devenue obligatoire au 1er janvier 2018 pour les entreprises de taille intermédiaire, et au 1er janvier 2019 pour les petites et moyennes entreprises.

Depuis le 1er janvier 2020, les microentreprises sont également tenues de transmettre leurs factures selon l'une des modalités électroniques admises par la loi.



(275) J.O. du 3 janvier 2014, p. 50.

(276) Ordonnance n° 2014-697 du 26 juin 2014 relative au développement de la facturation électronique, J.O. du 27 juin 2014, p. 10622. Cette ordonnance a depuis été abrogée par la loi n° 2019-186 du 22 mai 2019 relative à la croissance et à la transformation des entreprises, dite loi PACTE (J.O. du 23 mai 2019) et dont l'article 193 a modifié le code de la commande publique.

Désormais, **les articles L. 2192-1 à L. 2192-7 du Code de la commande publique** [277] **ne font plus de distinction selon la taille du co-contractant et tous les titulaires des marchés publics conclus avec l'État, les collectivités territoriales et les établissements publics doivent transmettre leurs factures sous forme électronique aux acheteurs publics**. Il en va de même pour les contrats de concession conclus avec l'État, les collectivités territoriales et les établissements publics [278] en application des articles L. 3133-1 et L. 3133-2 du Code de la commande publique [279].

Les personnes publiques sont quant à elles tenues de les réceptionner. Seules les factures générées en application de contrats de marché public ou de concession dans le domaine de la défense ou de la sécurité peuvent encore échapper à ces dispositions [280].

Le décret n°2019-748 du 18 juillet 2019 [281] a posé les modalités de la facturation électronique dans le cadre de la commande publique ; étant noté que la liste dressée par la Direction Générale des Finances Publiques (DGFiP) relatives aux factures et autres documents soumis à l'obligation de facturation électronique demeure d'application [282]. En application des dispositions réglementaires, les normes de facturation électronique et les mentions obligatoires des factures sous forme électronique sont décrites [283].

De plus, **l'utilisation du portail mutualisé « *Chorus Pro* » s'impose aux facturés (personnes publiques) comme aux factureurs (fournisseurs)** [284]**. Cette plateforme est ainsi devenue le point d'entrée unique** [285] **et gratuit pour la facturation électronique dans le cadre de la commande publique** [286].

(277) V. notamment l'article 193 de la loi n° 2019-186 du 22 mai 2019 relative à la croissance et à la transformation des entreprises, dite loi PACTE (J.O. du 23 mai 2019) modifiant le Code de la commande publique.

(278) En application de l'article L. 2192-2 du Code de la commande publique, cette obligation concerne aussi bien les factures des titulaires de marchés que celles de leurs sous-traitants lorsqu'ils sont admis au paiement direct dans le cadre des marchés publics.

(279) Créés par l'article 193 de la loi n° 2019-186 du 22 mai 2019 relative à la croissance et à la transformation des entreprises, dite loi PACTE (J.O. 23 mai 2019) modifiant le Code de la commande publique.

(280) Ces exceptions peuvent s'appliquer aux marchés de défense ou de sécurité conclus avec l'État ou ses établissements publics (mais pas avec les collectivités territoriales) en application de l'article L.2392-1 du Code de la commande publique. De même, échappent à cette obligation, les contrats de concession de défense ou de sécurité conclus avec l'État, les collectivités territoriales et les établissements publics en application de l'article L. 3133-1 al. 2 et L. 3134-4 du Code de la commande publique.

(281) Décret n° 2019-748 du 18 juillet 2019 relatif à la facturation électronique dans la commande publique modifié (J.O. 21 juillet 2019).

(282) Note d'instruction de la DGFIP relative au développement de la facturation électronique en date du 22 février 2017, BOFIP-GCP-17-0006 du 07/03/2017.

(283) Aux articles D. 2192-1 et D. 2192-2 du Code de la commande publique pour les marchés publics et aux articles D. 3133-1 et D. 3133-2 du Code de la commande publique pour les contrats de concession.

(284) Dès 2012, le portail Chorus Factures avait été élaboré pour l'État afin de lui permettre d'émettre et de recevoir les factures de ses fournisseurs en application du décret n° 2011-1937 du 22 décembre 2011 relatif aux conditions d'acceptation par l'État des factures émises par ses fournisseurs sous forme dématérialisée. Cette solution avait ensuite été reprise et étendue à d'autres acheteurs publics en application du décret n° 2016-1478 du 2 novembre 2016 relatif au développement de la facturation électronique (J.O. du 4 novembre 2016) et de l'arrêté du 9 décembre 2016 subséquent relatif au développement de la facturation électronique (J.O. du 15 décembre 2016) modifié. Le décret du 18 juillet 2019 (réf. cit. supra) a codifié lesdites dispositions en les modifiant.

(285) En application de l'article R.2192-3, alinéa 2 du Code de la commande publique pour les marchés publics, et de l'article R.3133-3 alinéa 2 du Code la commande publique pour les contrats de concession.

Ce qui a des conséquences tant pour les personnes publiques (qui doivent notamment informer le factureur du rejet de la facture adressée par une autre voie et l'inviter à régulariser l'envoi de la facture concernée) que pour le créancier (quant au délai de paiement en cas de rejet de sa facture pour non-respect des modalités notamment).

En application du décret du 18 juillet 2019, un arrêté doit prévoir « *les modalités techniques selon lesquelles le dépôt, la transmission et la réception des factures sont effectués sur le portail public de facturation* ». À défaut d'un texte plus récent, ce sont les dispositions de l'arrêté du 9 décembre 2016 [287] qui continuent à s'appliquer.

Sont ainsi prévus trois modes de transmission : le mode « *flux* » (EDI), le mode « *portail* » et le mode « *service* » (API). Quel que soit le mode utilisé, le décret impose que les modalités mises en œuvre « *garantissent la réception immédiate et intégrale des factures et assurent la fiabilité de l'identification de l'émetteur, l'intégrité des données, la sécurité, la confidentialité et la traçabilité des échanges* » [288].

Dans cette logique, les conditions générales d'utilisation du portail Chorus Pro s'attachent à présenter les caractéristiques techniques mises en œuvre ainsi que les effets probatoires des documents traités via Chorus Pro (convention de preuve) [289]. Concrètement, Chorus Pro est géré par l'Agence pour l'informatique financière de l'État (AIFE).

Signalons enfin que l'ordonnance n° 2021-1190 du 15 septembre 2021 relative à la généralisation de la facturation électronique dans les transactions entre assujettis à la taxe sur la valeur ajoutée et à la transmission des données de transaction [290] rend également obligatoire la facturation électronique entre entreprises (BtoB) selon l'échéance fixée [291]. À terme, il conviendra de voir quelles solutions seront retenues en application de ces nouvelles dispositions.

(286) Sauf pour la Caisse des dépôts et consignation, la RATP et la SNCF qui disposent déjà d'une plateforme de facturation électronique propre.

(287) Réf. cit. supra. V. sur le sujet et le régime juridique actuellement applicable : A. Cantero & P. Agosti, Les modalités de transmission et de réception des factures électroniques dans la commande publique, Contrats publics, n°202, oct. 2019, p. 24 et s.

(288) Article R.2192-3 du Code de la commande publique pour les marchés publics, article R.2392-3 du Code de la commande publique et article R3133-3 du Code de la commande publique pour les contrats de concession.

(289) Dossier de spécifications externes Chorus Pro accessible à partir du site www.communauté.chorus-pro.gouv.fr.

(290) J.O. 16 septembre 2021.

(291) Pour plus de détails sur cette évolution, voir nos développements relatifs à la facturation électronique dans la partie « Sphère privée » du présent Vade-mecum.

NOTES

Cet espace vous est dédié pour prendre des notes.

Sommaire

E. Exigences communes et transversales

fntc

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

1. Le respect des référentiels généraux : RGS, RGI et RGAA

Trois référentiels généraux ont été adoptés pour l'administration électronique. Ils constituent un état de l'art dont le respect devient contraignant dès lors qu'une disposition législative ou réglementaire y renvoie.

a. Le Référentiel Général de Sécurité (RGS)

Le Référentiel Général de Sécurité (RGS) a été introduit par l'ordonnance n° 2005-1516 du 8 décembre 2005 et ses modalités d'élaboration, d'approbation, de modification et de publication ont été fixées par décret [292].

Le RGS « *fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage* » (article 9.I de l'ordonnance du 8 décembre 2005).

Il appartient à l'administration de déterminer les fonctions de sécurité nécessaires pour protéger le système d'information qu'elle met en place. Lorsque le RGS traite lesdites fonctions, l'administration doit choisir le niveau de sécurité adapté parmi ceux proposés dans le RGS et se conformer, le cas échéant, aux règles correspondant (article 9.II de l'ordonnance du 8 décembre 2005).

Les prestataires de service de confiance (PSCo) et les produits de sécurité peuvent être qualifiés s'ils sont conformes au RGS (article 9.III du 8 décembre 2005). Cette qualification est appréciée selon chaque niveau du RGS.

(292) V. notamment 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 (J.O. du 18 mai 2010, p.9152), abrogé et remplacé par l'Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (J.O. du 24 juin 2014, p. 10361) ; l'Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (J.O. du 24 juin 2014).

Actuellement, le RGS est publié dans sa version 2.0 [293]. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui est chargée de son élaboration a ainsi posé les jalons quant aux politiques type en matière de signature électronique, de certificats et d'horodatage.

Ce faisant, **l'ANSSI a défini des règles et recommandations pour la sécurité des systèmes d'information qui constituent un « *état de l'art* » en matière de sécurité [294] , état de l'art qui s'impose dans le cadre de la digitalisation des administrations.** Ainsi, le RGS comporte de nombreuses annexes qui déclinent selon le service de confiance concerné différentes politiques type (politique type de certification, politique type d'horodatage…), donnent des recommandations et précisent les référentiels pour la certification des offres des prestataires de service de confiance qui souhaiteraient obtenir l'attestation de conformité imposée dans certains cas aux téléservices et procédés mis en place par les administrations. Les prestataires de service de confiance (PSCo) ont donc tout intérêt à se conformer aux dispositions du RGS selon le niveau de sécurité visé s'ils entendent cibler le marché des administrations. [295]

On notera notamment que l'arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance [296], complète le dispositif prévu dans le cadre de l'ordonnance du 8 décembre 2005, ainsi que dans le décret n° 2070-172 du 2 février 2010.

Cet arrêté établit une procédure de référencement (validité de 3 ans renouvelable selon l'article 10) relativement proche de la procédure de qualification en matière de signature électronique telle que prévue en droit civil.

Cela étant, l'ANSSI indique que la v.2.0 du RGS est « *un référentiel de transition entre une première version liée à la mise en œuvre de l'administration électronique et une troisième version qui se fondera sur la réglementation européenne en cours d'évolution* » [297]. L'ANSSI devrait adopter sous peu une nouvelle version prenant en compte le règlement européen eIDAS [298].

(293) La version actuelle du RGS (RGS 2.0) a été mise en ligne à la suite de la publication de l'Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (J.O. du 24 juin 2014). Les mesures de transition ont été étendues par arrêté du 1er ministre du 10 juin 2015 prorogeant les délais de mise en œuvre du RGS. Pour plus d'informations, v. : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.

(294) Liste des documents constitutifs du RGS v.2.0 disponibles sous le lien : http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

(295) Arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance, J.O. du 21 février 2012, modifié par l'Arrêté du 25 juillet 2013 modifiant l'arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance J.O. 3 août 2013 et le décret n° 2015-1165 du 21 septembre 2015 relatif au secrétariat général pour la modernisation de l'action publique, J.O. du 22 septembre 2015.

(296) V. en ce qui concerne l'application du RGS en matière de signature électronique des décisions administratives, le point infra II.E.3 consacré à cette question.

(297) Sur ce point voir le lien suivant : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

b. Le Référentiel Général d'Interopérabilité (RGI)

Le Référentiel Général d'Interopérabilité (RGI) a été défini par 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 [(299)]. Son article 11 précise : le « *RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret* ».

Son objectif consiste ainsi à déterminer un ensemble de règles dont le respect s'impose aux administrations pour faciliter les échanges par voie électronique et rendre cohérents les systèmes d'information des services publics, 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. Plusieurs textes réglementaires se sont succédés [(300)]. Actuellement, la version 2.0 du RGI résulte de l'arrêté du 20 avril 2016 [(301)].

On notera que dans le cadre des téléservices qu'elles mettent en place, les administrations (en ce compris les administrations territoriales) sont tenues de respecter le RGI en application de l'article L.112-9 du CRPA.

c. Le Référentiel Général d'Amélioration de l'Accessibilité (RGAA)

Les administrations doivent s'assurer de l'accessibilité des téléservices et téléprocédures par tous les citoyens, y compris les personnes en situation de handicap.

(298) Règlement (UE) n° 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, J.O.U.E n° L. 257 du 28 août 2014, p. 73.

(299) Réf. cit. supra.

(300) V. notamment 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 (J.O. du 3 mars 2007) ; Arrêté du 9 novembre 2009 portant approbation du référentiel général d'interopérabilité (J.O. du 11 novembre 2009) ; décret n° 2011-193 du 21 février 2011 portant création d'une direction interministérielle des systèmes d'information et de communication de l'État (J.O. du 22 février 2011).

(301) Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité, J.O. 22 avril 2016 ; v. sur le sujet : http://references.modernisation.gouv.fr/interoperabilite.

À 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 modifiée [302], le législateur a prévu un référentiel général d'accessibilité pour les administrations (RGA). Depuis 2009, date de la première version du RGA [303], plusieurs versions se sont succédées [304]. La dernière version en date est issue du décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne [305]. Désormais dénommé le Référentiel Général d'Amélioration de l'Accessibilité (RGAA), ce référentiel dresse la liste des différents critères que doivent remplir les sites publics afin d'être accessibles à tous.

Pour les administrations d'État, la Charte internet de l'État définit en sus un ensemble de règles ergonomiques communes aux interfaces des sites Internet publics [306]. La dématérialisation des services publics (en ce compris les téléservices) doit intégrer, le cas échéant, ces modalités d'accessibilité voire d'ergonomie pour les administrations d'État.

À la différence des principes d'accessibilité, cette harmonisation ergonomique ne s'impose pas aux collectivités territoriales qui jouissent de la liberté d'administration en la matière.

2. Le respect de la réglementation relative à la protection des données personnelles

D'une façon générale, les personnes publiques sont soumises à la réglementation relative à la protection des données personnelles, même si certaines règles spécifiques leur sont applicables.

(302) L'article 47 de ladite loi (Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées, J.O. du 12 février 2005) a notamment été modifié par l'article 80 de la loi n° 2018-771 du 5 septembre 2018 pour la liberté de choisir son avenir professionnel, J.O. du 6 septembre 2018.

(303) 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, J.O. 29 octobre 2009.

(304) Dont la version RGA3 qui a connu les modifications les plus significatives en application de l'Arrêté du 29 avril 2015 relatif au référentiel général d'accessibilité pour les administrations, J.O. du 2 mai 2015 p. 7562.

(305) La dernière version mise à jour au 21 octobre 2019 (RGAA4) est accessible à l'adresse : https://www.numerique.gouv.fr/publications/rgaa-accessibilite/.

En ce qui concerne leurs relations avec des PSCo, on notera plus particulièrement que, dans le cadre des marchés publics, l'article R. 2112-2 du Code de la commande publique précise que les cahiers des clauses administratives générales (CCAG) « *fixent les stipulations de nature administrative applicables à une catégorie de marchés* ».

L'application des CCAG n'est pas obligatoire et il appartient à l'acheteur public d'y faire référence, s'il le souhaite, et de choisir, le cas échéant, le CCAG le mieux adapté au marché envisagé. Ceci étant précisé, les CCAG définissent des bonnes pratiques souvent suivies par les acheteurs publics. À cet égard, six arrêtés du 31 mars 2021 ont approuvé les nouveaux CCAG des marchés publics de différentes natures.

Afin d'accompagner les acteurs de la commande publique dans la mise en œuvre de ces nouveaux CCAG, la direction des affaires juridiques (DAJ) a publié un guide sous forme de fiches le 19 novembre 2021.

Compte tenu de la problématique transversale des données personnelles, la DAJ a rédigé une fiche spécifique dédiée au Règlement général sur la protection des données (RGPD) dans les marchés publics (Fiche 3 [307]).

La démarche proposée invite les acheteurs :

+ Premièrement, à déterminer si le marché implique un traitement de données personnelles ou non,
+ Deuxièmement, dans l'affirmative,, à s'interroger sur les rôles de chaque intervenant au regard des qualifications juridiques « *RGPD* » (responsable de traitement/co-responsable de traitement/ sous-traitant),
+ Troisièmement à rédiger des clauses « *RGPD* » spécifiquement adaptées à la situation identifiée en phase 2.

Il est ainsi recommandé d'exclure des clauses « *RGPD* » type, qui seraient intégrées systématiquement.

Compte tenu de ces éléments, les acheteurs publics et les PSCO devraient s'attacher à ce que les CCAG soient adaptés à la réalité juridique de chaque marché [308].

(306) Cette charte a remplacé la Charte ergonomique initialement définie en 2008. V. sur le sujet : circulaire du Premier ministre relative à l'Internet de l'État n°5574 du 16 février 2012, dont le but affirmé est d'améliorer la qualité générale de l'internet de l'Etat (http://references.modernisation.gouv.fr/charte-internet-de-letat).

(307) V. DAJ, Le Règlement général sur la protection des données (RGPD) dans les marchés publics.

(308) Voir également sur ce point la partie « Données personnelles » traitées dans le présent Vade-Mecum.

3. La reconnaissance juridique des signatures électroniques des décisions administratives

Seules les décisions administratives (exprès) doivent comporter la signature de leur auteur. Cette signature doit obligatoirement être assortie de la mention, en caractères lisibles, du prénom, du nom et de la qualité du signataire (article L. 212-1 du CRPA).

Ces obligations formelles trouvent notamment leur fondement dans les règles de légalité des actes administratifs qui font de la compétence juridique du signataire (autorité qui prend la décision) une condition de légalité de la décision.

Dans la logique de la reconnaissance des échanges par voie électronique et de la digitalisation de l'administration, la signature électronique a ainsi fait son apparition dans le Code des relations entre le public et l'administration, en son article L. 212-3 (309).

Désormais, par principe, les décisions de l'administration peuvent faire l'objet d'une signature électronique.

Toutefois, celle-ci « *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 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, qui permette l'identification du signataire, garantisse le lien de la signature avec la décision à laquelle elle s'attache et assure l'intégrité de cette décision* ».

(309) Codifié par l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du Code des relations entre le public et l'administration, J.O. du 25 octobre 2015.

On notera qu'à la différence de la définition donnée dans le Code civil (article 1367), les exigences relatives au procédé utilisé sont posées à des fins de validité (légalité) de la signature.

On se situe donc sur le terrain juridique des formalités (*acte ad validitatem*) et non des preuves (*acte ad probationem*). Cette différence s'explique notamment par le régime probatoire en droit administratif qui repose sur la liberté de la preuve pour les actes administratifs [(310)].

Ceci étant précisé, **dès lors que la décision doit être signée pour être légale, alors le procédé de signature électronique utilisé devra remplir les conditions posées, à savoir être conforme au Référentiel général de sécurité** (RGS [(311)]).

Ce faisant, ledit procédé permettra l'identification du signataire, garantira le lien entre la signature et l'acte auquel elle est attachée et assurera l'intégrité de ladite décision.

À cet égard, le RGS définit plusieurs niveaux de sécurité aux exigences croissantes (*, **, éventuellement***) [(312)]. **Il appartient aux administrations de choisir parmi ceux-ci, celui qui convient à leurs besoins.**

De plus, les Prestataires de service de certification électronique (devenus les Prestataires de services de confiance [(313)]) peuvent demander à ce que leur(s) offre(s) soient certifiée(s) conforme(s) au(x) niveau(x) visé(s) conformément aux procédures définies en la matière [(314)].

Il appartient à l'administration concernée de recourir à l'offre déclarée conforme au RGS selon le niveau de signature choisi.

(310) Sur une présentation des principes, v. Anne Cantero, Des actes unilatéraux des communes dans le contexte électronique – Vers la dématérialisation des actes administratifs ?, Presses Universitaires d'Aix Marseille, 2002, p.147 et s..

(311) V. notre présentation générale du RGS au point II.C.1 du présent Vade-Mecum. La signature électronique ne constitue en effet que l'un des aspects couverts par le RGS. Pour plus d'informations, il est également renvoyé à l'adresse https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/. Plus spécifiquement en ce qui concerne les signatures électroniques, v. Politique de certification type « certificats électroniques de personne », version 3.0 du 27 février 2014, annexe RGS_A2.

(312) V. Politique de certification type « certificats électroniques de personne », version 3.0 du 27 février 2014, annexe RGS_A2.

(313) Depuis le Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, J.O.UE L.257 du 28 août 2014 p.73 s., disponible sous le lien : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.FRA. .

(314) Ces modalités ont été définies par le 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 (dit décret RGS), modifié à plusieurs reprises dont récemment par le décret n° 2019-1139 du 7 novembre 2019 modifiant le décret n° 97-1184 du 19 décembre 1997 pris pour l'application au Premier ministre du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles.

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

Le législateur a posé **plusieurs exceptions** faisant échapper un certain nombre d'actes à l'obligation de signature électronique. Ainsi, en application de l'article L.212-2 du CRPA [315] :

« *Sont dispensés de la signature de leur auteur, dès lors qu'ils comportent ses prénom, nom et qualité ainsi que la mention du service auquel celui-ci appartient, les actes suivants :*

+ ***1° Les décisions administratives qui sont notifiées au public par l'intermédiaire d'un téléservice conforme à l'article L. 112-9 du CRPA et aux RGS et RGI incluant l'utilisation de produits référencés selon le niveau de sécurité requis ainsi que les actes préparatoires à ces décisions ;***

+ *2° Les décisions administratives relatives à la gestion de leurs agents produites par les administrations sous forme électronique dans le cadre de systèmes d'information relatifs à la gestion ou à la dématérialisation de processus de gestion des ressources humaines conforme aux articles 9, 11 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 précitée, quelles que soient les modalités de notification aux intéressés, y compris par l'intermédiaire d'un téléservice mentionné au 1° ;*

+ *3° Quelles que soient les modalités selon lesquelles ils sont portés à la connaissance des intéressés, les saisies administratives à tiers détenteur, adressées tant au tiers saisi qu'au redevable, les lettres de relance relatives à l'assiette ou au recouvrement, les avis de mise en recouvrement, les mises en demeure de souscrire une déclaration ou d'effectuer un paiement, les décisions d'admission totale ou partielle d'une réclamation et les demandes de documents et de renseignements pouvant être obtenus par la mise en œuvre du droit de communication prévu au chapitre II du titre II de la première partie du livre des procédures fiscales ;*

+ *4° Les visas délivrés aux étrangers* ».

L'exception posée au 1°) de cet article L.212-2 du CRPA marque l'importance de la mise en œuvre de téléservices sécurisés dans lesquelles les PSCo ont un rôle à jouer.

(315) Introduit par la loi n° 2014-1545 du 20 décembre 2014 relative à la simplification de la vie des entreprises et portant diverses dispositions de simplification et de clarification du droit et des procédures administratives, J.O. du 21 décembre 2014, p. 21647. Codifié depuis l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, J.O. du 25 octobre 2015 p. 19872 puis modifié par loi n° 2016-1918 du 29 décembre 2016 de finances rectificative pour 2016, loi n° 2017-1775 du 28 décembre 2017 de finances rectificative pour 2017, J.O. 29 décembre 2017, la loi n° 2018-727 du 10 août 2018 pour un Etat au service d'une société de confiance, J.O. du 11 août 2018, et la loi n° 2018-778 du 10 septembre 2018 pour une immigration maîtrisée, un droit d'asile effectif et une intégration réussie, J.O. du 11 septembre 2018.

4. L'archivage

Dans la sphère publique, le régime juridique de l'archivage doit être appréhendé au regard de plusieurs législations révélatrices des enjeux en cause.

Ainsi, les dispositions du Code du patrimoine, du Code des relations entre le public et l'administration, du Code général des collectivités territoriales et celles relatives à la protection des données à caractère personnel (RGPD [316]) doivent cohabiter. Les développements qui suivent tentent d'apporter une certaine visibilité quant aux grands principes à prendre en compte en la matière [317].

a. La définition des archives publiques

L'article L.211-1 du Code du patrimoine dispose : « *Les archives sont l'ensemble des documents, y compris les données, 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* » [318].

En application de l'article L.211-4 du Code du patrimoine, les archives publiques sont :

> *« 1° Les documents qui procèdent de l'activité de l'État, des collectivités territoriales, des établissements publics et des autres personnes morales de droit 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 ;*
>
> *2° Les documents qui procèdent de la gestion d'un service public ou de l'exercice d'une mission de service public par des personnes de droit privé ;*
>
> *3° Les minutes et répertoires des officiers publics ou ministériels et les registres de conventions notariées de pacte civil de solidarité.* ».

(316) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, (RGPD), J.O.UE du 4 mai 2016 et de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, J.O. du 21 juin 2018.

(317) Cette rédaction est issue de la loi n° 2016-925 du 7 juillet 2016 relative à la liberté de la création, à l'architecture et au patrimoine, J.O. du 8 juillet 2016.

(318) V. pour une vision globale des archives publiques le site du Portail national des archives FranceArchives à l'adresse : https://francearchives.fr/fr/gerer.

La nature, le support et/ou la forme électroniques du document ou de la donnée, objet de l'archivage, ne lui ôtent donc pas la qualité d'archive publique. Les travaux du Service Interministériel des Archives de France (SIAF) contribuent à clarifier l'application des dispositions juridiques applicables à ce type d'archives. (319)

b. Les finalités de l'archivage public

L'archivage public a essentiellement deux finalités : une finalité informationnelle, historique, statistique ou une finalité juridique (320).

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).

Dans une finalité juridique, 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 (323). Par ailleurs, 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.

c. Les durées d'utilité des archives et les délais de conservation

En application des articles R. 212-10 à R. 212-12 du Code du patrimoine, on distingue trois phases d'utilisation des archives publiques. Ces périodes dépendent de la durée d'utilité administrative (D.U.A.) du document conservé. La durée d'utilité administrative dépend de l'utilisation du document et de la nature du droit auquel il se rapporte.

(319) V. l'article L.211-2 du Code du patrimoine qui dispose : « La conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche ».

(320) 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.

Il peut s'agir de très courtes durées ou de durées infinies. Ainsi, on distingue :

+ **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 : 1° ont cessé d'être considérés comme archives courantes ; 2° 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.* ».

Les administrations doivent donc réaliser un travail en amont afin de déterminer les catégories de documents et données entrant dans les archives courantes, les archives intermédiaires ou les archives définitives. Chaque phase implique des opérations de tri, sélection et élimination qui sont juridiquement encadrées (article L. 212-2 du Code du patrimoine).

La durée de conservation d'un document doit être déterminée au regard des textes applicables selon la nature du document concerné et la finalité dans laquelle il est reçu ou produit et conservé (par exemple des autorisations administratives, des pièces comptables,...)

d. Les délais et contraintes de communication

L'article L. 213-1 du Code du patrimoine pose pour principe la communicabilité de plein droit des archives publiques. Toutefois, l'application de ce principe doit respecter un enchevêtrement de dispositions qui le limitent.

Premièrement, ce principe ne remet pas en cause les articles L. 311-1 à L. 311-8 du Code des relations entre le public et l'administration (CRPA) relatifs au droit d'accès aux documents administratifs, dès lors que lesdites archives entrent dans la définition des documents administratifs au sens de la loi. Il convient donc de s'assurer que les accès aux archives publiques (courantes, intermédiaires ou définitives) respectent bien ces dispositions et les modalités d'accès aux documents administratifs tels que définies dans le CRPA.

Deuxièmement, le principe de communicabilité de plein droit est limité par l'article L. 213-2 du Code du patrimoine qui pose des délais dérogatoires allant de 25 ans à 100 ans selon le contenu du document (par exemple en cas d'atteinte au secret des affaires, au secret médical, à la sécurité nationale).

Troisièmement, le principe de la communicabilité de plein droit des archives publiques est restreint par l'application des mesures législatives et réglementaires protégeant les données à caractère personnel. D'abord, il est important de rappeler que les principes de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée doivent être respectés en la matière [320] .

(320) V. sur le sujet, l'analyse et les recommandations de la CNIL et du SIAF dans le guide qu'ils ont élaboré en collaboration : CNIL et SIAF, Guide pratique sur les données de conservation, version de juillet 2020, accessible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf.

D'autre part, l'article L.212-3 du Code du patrimoine dispose : « *Lorsque les archives publiques comportent des données à caractère personnel collectées dans le cadre de traitement* » régis par la loi du 6 janvier 1978, « *ces données font l'objet, à l'expiration de la durée prévue au 5° de l'article 4 de ladite loi, d'une sélection pour déterminer les données destinées à être conservées et celles, dépourvues d'utilité administrative ou d'intérêt scientifique, statistique ou historique, destinées à être éliminées.*

Les catégories de données destinées à l'élimination ainsi que les conditions de cette élimination sont fixées par accord entre l'autorité qui a produit ou reçu ces données et l'administration des archives ».

En pratique, l'articulation de ces différents textes peut s'avérer délicate et les propriétaires d'archives publiques, comme les PSCo souhaitant proposer leurs services d'archivage à cette catégorie d'utilisateurs, devront vérifier l'adéquation de l'archivage envisagé avec ces différentes dispositions.

Par exemple, le service d'archivage peut permettre de retrouver de manière rapide et efficace tous les documents faisant l'objet d'une demande de consultation ou de communication. Cette fonctionnalité peut alors impliquer le traitement de données à caractère personnel (métadonnées notamment). Il conviendra alors de s'assurer que les dispositions relatives à la protection des données à caractère personnel sont respectées par le service envisagé. Les préconisations de la Direction des affaires juridiques en matière de marché public et de la qualification des prestataires au regard de la législation sur la protection des données à caractère personnel prend également tout son sens en la matière. (321)

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 ; étant noté que lorsque l'archivage est à des fins juridiques, les conditions de cet archivage devront permettre de rapporter la preuve qu'à la date d'adoption de l'acte, les formalités exigées ont été respectées et que les modalités d'archivage garantissent que ces exigences ont été maintenues dans le temps.

(321) Sur ces questions, v. notamment les travaux de France archives (https://francearchives.fr).

L'archivage et a fortiori l'archivage des documents électroniques nécessitent ainsi un savoir-faire certain et une expertise adaptée aux besoins des personnes publiques et privées soumises aux règles spécifiques de l'archivage publique.

e. Service public d'archives, mutualisation et externalisation

Lorsque les archives publiques ont fait l'objet de la sélection prévue aux articles L. 212-2 et L. 212-3 du Code du patrimoine et sont devenues des archives définitives, elles doivent être versées dans un service public d'archives (article L. 212-4 §I du Code du patrimoine). Les modalités de ces versements ont été déterminées par décrets et sont désormais régies par les articles R. 212-18 et s. du Code du patrimoine [(332)].

Pour la conservation d'archives définitives et intermédiaires, l'article R. 212-18-1 du Code du patrimoine prévoit une possible mutualisation entre les services publics d'archives compétents. Cette possibilité a été étendue à tous les acteurs publics, dont les collectivités territoriales en application de l'article 202 de la loi n°2022-217 du 21 février 2022 relative à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de l'action publique locale. [(323)]

Cette mutualisation doit faire l'objet d'une convention dont l'objet et les clauses attendues sont précisés à l'article R. 212-18-1, §II du Code du patrimoine. De plus, l'article R. 212-18-2 du Code du patrimoine indique que la conservation mutualisée doit répondre aux normes conformes à l'état de l'art, au regard des différents critères énumérés.

Par ailleurs, lorsque les documents constitutifs des archives n'ont pas encore fait l'objet de la sélection prévue aux articles L. 212-2 et L 212-3 du Code du patrimoine (c'est-à-dire qu'elles sont encore courantes ou intermédiaires), les personnes publiques et privées qui gèrent des archives publiques au sens de l'article L. 211-4 du Code du patrimoine ont la possibilité de les déposer auprès d'un tiers (personnes physiques ou morales) sous réserve d'avoir préalablement déclaré à l'administration des archives cette démarche et que le tiers concerné soit agréé par l'administration compétente.

Cette externalisation est régie par l'article L. 212-4 §II du Code du patrimoine et les articles R. 212-19 à R. 212-31 du Code du patrimoine. Le dépôt doit notamment faire l'objet **d'un contrat écrit strictement encadré** [(324)].

(322) V. sur ce point nos développements dans la partie II.E.2. du présent Vade-Mecum.

(323) Loi n°2022-217 du 21 février 2022 relative à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de l'action publique locale (dite loi 3DS), J.O. 22 février 2022.

(324) V. pour une illustration contentieuse de résiliation de contrat : CAA Douai, 3e ch., 8 juillet 2021, 19DA02481 accessible à partir de l'adresse : https://juricaf.org/arret/FRANCE-COURADMINISTRATIVEDAPPELDEDOUAI-20210708-19DA02481.

Enfin, il est important de noter que les données de santé relèvent d'un régime spécifique qui implique notamment, dans le cadre des archives publiques, de respecter les dispositions de l'article 1111-8 du Code de la santé publique.

Le 7 avril 2022, le SIAF a publié une note d'information relative au cadre légal et réglementaire de l'externalisation de la conservation des archives publiques. Des précisions importantes sur les modalités de mise en œuvre des dispositions applicables en matière d'externalisation de l'archivage ont ainsi été apportées [325].

L'externalisation de l'hébergement est notamment distinguée de l'externalisation de la conservation des archives. L'hébergement consiste dans le stockage physique des archives et le maintien en condition opérationnelle des infrastructures et des outils logiciels.

La conservation des archives, quant à elle, est un processus qui, en plus de l'hébergement, implique la définition et la mise en œuvre des procédures archivistiques. Cette distinction a des implications directes sur le régime de l'externalisation.

L'externalisation du seul hébergement est en effet juridiquement plus souple. Ainsi, à titre principal, le tiers hébergeur peut ne pas être agréé (sauf lorsque l'hébergement porte sur des données de santé et relève du régime juridique spécifique fixé à l'article 1111-8 du Code de la santé publique).

En ce qui concerne l'externalisation de la conservation des archives, les modalités suivantes doivent en revanche être respectées :

(325) V. SIAF, Note d'information relative au cadre légal et réglementaire de l'externalisation de la conservation des archives publiques, 7 avril 2022, accessible à partir de l'adresse: https://francearchives.fr/fr/circulaire/DGPA_SIAF_2022_01.

+ Le recours à un PSCo tiers archiveur n'est possible que pour les archives courantes ou **intermédiaires**, ce qui exclut les archives définitives.

+ Le tiers archiveur doit au **préalable être agréé par l'administration des archives par arrêté préfectoral**. 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 (et non de cinq ans comme c'est le cas pour une conservation sur support papier). Par ailleurs, la certification pour l'archivage numérique (NF 461) se fait sur la base de la norme NF Z42-013 dans sa version d'octobre 2020 pour la délivrance de l'agrément.

+ La collectivité doit procéder à une déclaration auprès de l'administration des archives et doit **conclure avec la société privée un contrat de dépôt dont les clauses minimales sont imposées par les dispositions réglementaires** (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). La personne chargée du contrôle scientifique et technique de l'État sur les archives est destinatrice, de droit, d'un exemplaire du contrat signé.

  L'article R. 212-21 du Code du patrimoine précise en outre que ce contrat est nécessairement conclu par écrit 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. »

Compte tenu de la différence de régime juridique entre l'externalisation de l'hébergement des archives et l'externalisation de la conservation des archives, les PSCo comme les personnes ayant recours à leurs services d'archivage doivent ainsi s'assurer de l'exacte qualification juridique de la prestation concernée. S'ajoute à cette recommandation juridique, le respect des procédures de marché public bien évidemment.

f. Un service d'archivage électronique sécurisé

En tout état de cause, qu'il soit interne, mutualisé ou externalisé, pour être considéré comme sécurisé [326], le système d'archivage doit garantir l'intégrité, l'intelligibilité, la durabilité et l'accessibilité du document archivé, et ce, a fortiori s'il a une finalité juridique. Toutes les archives et les opérations y afférentes doivent nécessairement être tracées et la disponibilité du service ainsi que l'interopérabilité entre les différents systèmes d'archivage (collectivités, archives de France, etc.) doivent être assurées. Les référentiels généraux de sécurité et d'interopérabilité (RGS et RGI) peuvent à cet égard être utiles.

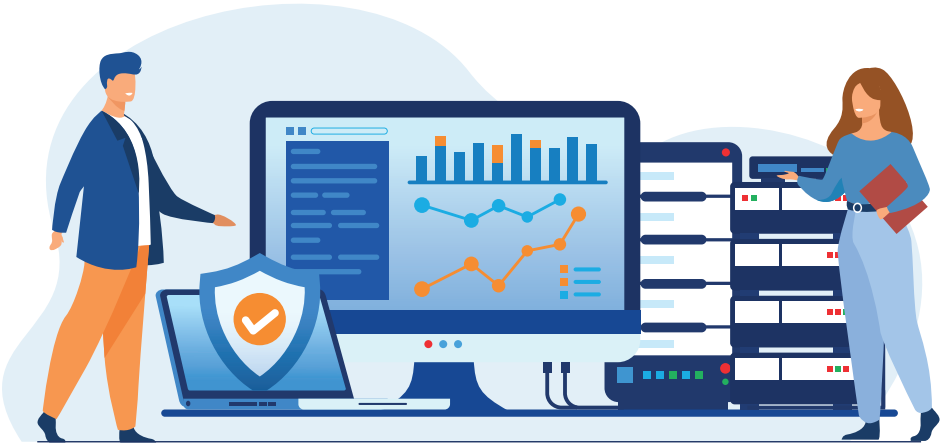
Dans cette optique, la mise en place d'un archivage électronique sécurisé doit reposer sur l'adoption d'un certain nombre de documents importants (politique d'archivage, déclaration des pratiques d'archivage, cahier des charges, grilles d'audit). Concrètement, les recommandations

(326) A titre informatif, en 2006, la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI qui est devenue l'ANSSI) avait publié une étude relative à l'archivage électronique sécurisé dans la sphère publique (https://telechargement.girondenumerique.fr/InnerData/Doc_Archivage/ArchivageSecurise-EtatDeLArt-2006-11-29.pdf). Elle traitait 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 et de la société Oppida.

de la Direction générale des patrimoines dans ce domaine seront à prendre en compte.

De même, le standard d'échange applicable également dans les entreprises, élaboré par l'ancienne Direction des Archives de France avec la Direction Générale de la Modernisation de l'État du Minefi pourra servir de référence [327]. À noter qu'outre la norme AFNOR NF Z 42-013, de nombreux documents tendent également à poser les bases essentielles à tout système d'archivage.

On citera ainsi la norme MEDONA [328] ou le Référentiel général de gestion des archives [329] ou encore le programme Vitam lancé par les ministères des Affaires Étrangères, de la Culture et de la Défense et dont l'objectif est de développer un socle d'archivage électronique réutilisable par (toutes) les administrations [330] dont la V2 a été publiée en février 2019 [331].



(327) Version 0.2 disponible à l'adresse : http://www.archivesdefrance.culture.gouv.fr/seda/f.

(328) MEDONA - Modélisation des échanges de données pour l'archivage, NF Z44-022 Janvier 2014, disponible sous le lien : http://www.boutique.afnor.org/norme/nf-z44-022/medona-modelisation-des-echanges-de-donnees-pour-l-archivage/article/814057/fa179927.

(329) Disponible sous le lien : http://www.gouvernement.fr/sites/default/files/contenu/piece-J.O.inte/2014/07/r2ga_document_complet_201310.pdf.

(330) Vitam : vers un socle d'archivage électronique commun à toute l'administration, détails disponibles sous le lien : http://www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration

(331) http://www.programmevitam.fr/

5. La mise à disposition des données publiques et leur réutilisation

Suite à l'évolution des directives européennes en la matière [332], le régime juridique de la mise à disposition et de la réutilisation des informations du secteur public a subi de nombreuses modifications. Désormais, il repose à titre principal sur les articles L. 321-1 à L. 330-1 du CPRA ; étant noté que la parfaite application de ces dispositions implique de prendre en compte la définition des « *données publiques* » (qui est loin d'être claire), l'analyse des différentes dispositions relatives au droit d'accès aux documents administratifs (articles L. 311-5 et L. 311-6 CPRA notamment), ou encore celles applicables aux informations publiques comportant des données à caractère personnel dont la réutilisation est soumise à un régime juridique précis (sachant que les conditions posées ne sont pas sans ambiguïté et ce, *a fortiori* dans leur mise en œuvre).

Le guide pratique établi par la Commission Nationale Informatique et Libertés (CNIL), la Commission d'Accès aux Documents Administratifs (CADA) en association avec ETALAB confirme la complexité du sujet [333].

En outre, le régime général devra être écarté en cas d'existence d'un texte spécifique établissant un régime dérogatoire.

À titre d'illustration, dans le domaine juridique, l'article 33 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice [334] a posé les nouvelles modalités de la publicité et de la mise à disposition des décisions de justice au public. Ce texte tente de concilier le droit à l'information des personnes, le nouveau credo de l'ouverture des données publiques et de leur réutilisation par des tiers et la protection de la vie privée des personnes voire des magistrats.

Le décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives est venu préciser ces modalités, ainsi que l'arrêté du 28 avril 2021 pris en application de l'article 9 du décret n° 2020-797 du 29 juin 2020 et, enfin, le décret n° 2021-1276 du 30 septembre 2021 relatif aux traitements automatisés de données à caractère personnel dénommés « *Décisions de la justice administrative* » et « *Judilibre* ».

Enfin, il convient de noter que l'adoption du

(332) Dont récemment, la directive 2019/1024 du parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, JOUE du 26 juin 2019, L 172/56 et s.

(333) CNIL, CADA, ETALAB « Guide pratique de la publication en ligne et de la réutilisation des données publiques (« Open Data ») » 17 octobre 2019, accessible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/guide-open-data.pdf.

(334) Cette loi a respectivement modifié les articles L.10 et L.10-1 du Code de justice administrative pour les juridictions de l'ordre administratif (à savoir les tribunaux administratifs, les cours d'appel administratives et le Conseil d'État) et les articles L.111-13 et L.111-14 du Code de l'organisation judiciaire pour les juridictions de l'ordre judiciaire (dont les juridictions civiles et pénales, de première instance et d'appel ainsi que la Cour de cassation).

Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données [335] va avoir des incidences sur les régimes juridiques mis en place par les différents Etats membres en matière de mise à disposition et de réutilisation des données du secteur public. Ce règlement sera applicable de plein droit à compter du 24 septembre 2023.

Cet espace vous est dédié pour prendre des notes.

(335) Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), JOUE du 3 juin 2022, L 152/1.

Sommaire

fntc

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

Aujourd'hui, la digitalisation concerne toutes les autorités administratives (au sens du Code des relations entre le public et l'administration (CRPA) et 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), que ce soit de façon contrainte ou volontaire, de la petite collectivité aux administrations de l'État.

La mise en œuvre de la dématérialisation dans la sphère publique est toutefois confrontée à la complexité et à la disparité juridiques des administrations. Les télé-services et télé-procédures présentés ci-dessous ne constituent donc que des illustrations parmi tant d'autres.

1. Procédure électronique et état civil

Le décret du 10 février 2011 (336) a autorisé les administrations et organismes compétents pour requérir des actes d'état civil à demander directement, par voie électronique, aux officiers de l'état civil dépositaires des actes, la vérification des données déclarées par les usagers. Le décret du 6 mai 2017 (337) a complété le régime juridique défini en précisant plusieurs points.

D'abord, les demandes et les réponses de vérification échangées par voie électronique « *sont réalisées dans des conditions qui garantissent l'intégrité des informations échangées, la sécurité et la confidentialité de la transmission, l'identité et la fonction de l'expéditeur et celles du destinataire* ».

Dans ce cadre, l'utilisation d'une « *plate-forme sécurisée de routage* » est imposée (art. 43 du décret n° 2017-890). Cet outil de transmission gratuit pour les administrations est exploité par l'agence nationale des titres sécurisés (ANTS).

De plus, lorsque l'officier d'état civil atteste de la conformité des informations vérifiées, il peut le faire en apposant sa signature électronique sécurisée sur l'échange concerné. En application de l'alinéa 3 de l'article 43 du décret du 6 mai 2017, les certificats électroniques qualifiés sont également fournis gratuitement aux communes par l'agence nationale des titres sécurisés.

(336) 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, J.O. du 12 février 2011 et modifiant le Décret n° 62-921 du 3 août 1962 modifiant certaines règles relatives aux actes de l'état civil, J.O. du 9 août 1962.

(337) Décret n° 2017-890 du 6 mai 2017 relatif à l'état civil, J.O. du 10 mai 2017 pris en application de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XX^ème^ siècle, J.O. du 19 novembre 2016. V. plus spécialement les articles 43 à 45 du décret n° 2017-890.

Le principe de l'équivalence entre la signature manuscrite et la signature électronique sécurisée est en outre affirmé.

Concrètement, les caractéristiques techniques de la procédure de communication électronique des données de l'état civil sont définies par arrêté [338]. À défaut de nouveau texte réglementaire, l'arrêté du 19 janvier 2016 [339] demeure applicable. Sont définis les éléments techniques relatifs à la mise en œuvre de la vérification par voie électronique des actes d'état civil et de la plateforme de routage (COMEDEC [340]) ainsi que les éléments relatifs au dispositif sécurisé de création de la signature électronique fourni aux collectivités territoriales [341], l'ensemble de ces éléments devant être conforme au RGS [342].

L'État s'est engagé à verser annuellement une aide aux communes qui utilisent cette plateforme dans le cadre des vérifications [343].

Dans la logique de cette avancée digitale, la dématérialisation des actes de l'état civil a également été envisagée à titre expérimental. L'ordonnance n° 2019-724 du 10 juillet 2019 [344] fixe ainsi les conditions de l'expérimentation de la dématérialisation des actes de l'état civil établis par le ministère des affaires étrangères. Il est notamment prévu que ces actes soient signés par l'officier de l'état civil au moyen d'un procédé de signature électronique sécurisée (article 4).

Pour le déclarant, les actes sont signés soit « *au moyen d'un procédé permettant l'apposition sur l'acte, visible à l'écran, de l'image de leur signature manuscrite* » (article 4 dernier alinéa), soit, en cas de déclaration par téléservice d'une naissance ou d'un décès, le déclarant est dispensé de signature, mais l'acte établi par l'officier de l'état civil doit alors mentionner cette dispense (article 5, dernier alinéa).

(338) Article 43 du décret n° 2017-890 du 6 mai 2017 relatif à l'état civil, J.O. du 10 mai 2017.

(339) Arrêté du 19 janvier 2016 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil, J.O. du 28 janvier 2016. Ce texte a abrogé l'arrêté du 23 décembre 2011 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil, J.O. du 29 décembre 2011.

(340) 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 devenus les articles 2 à 8 de l'arrêté du 19 janvier 2016 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil. Pour les chiffres relatifs à l'utilisation de COMEDEC en décembre 2021, v. : http://www.justice.gouv.fr/comedec-12589/comedec-en-chiffres-12794/.

(341) 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 devenus les articles 9 à 13 de l'arrêté du 19 janvier 2016 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil.

(342) V. article 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 devenus les articles 10 et 11 de l'arrêté du 19 janvier 2016 relatif aux échanges par voie électronique des données à caractère personnel contenues dans les actes d'état civil.

(343) En application de l'article 45 du décret n°2017-890, réf. cit. supra ; cette aide devrait exister jusqu'en 2023.

(344) Ordonnance n° 2019-724 du 10 juillet 2019 relative à l'expérimentation de la dématérialisation des actes de l'état civil établis par le ministère des affaires étrangères. Ordonnance prise en application de l'article 46 de la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance, J.O. du 11 août 2018.

Les mentions marginales, les pièces justificatives, les copies et le registre électronique des actes d'état civil font également l'objet de dispositions spécifiques.

Le décret en Conseil d'État n°2019-993 du 26 septembre 2019 pris en application de cette ordonnance en précise un certain nombre de modalités. L'expérimentation menée est prévue pour une durée de 3 ans.

Passée cette période, il sera intéressant de voir les suites données à cette expérimentation tant pour les PSCo que pour les administrations compétentes.

2. Procédure fiscale et tiers de confiance

L'article 170 ter du Code général des impôts [345] prévoit un dispositif de « *tiers de confiance* ». Ce dispositif a pour objet d'autoriser les contribuables assujettis à l'obligation de dépôt d'une déclaration annuelle de revenus qui sollicitent le bénéfice de déductions de leur revenu global, de réductions ou de crédits d'impôts, à remettre les pièces justificatives des charges correspondants à un tiers de confiance. Peuvent prétendre à cette qualité les professionnels de l'expertise comptable, les avocats et les notaires.

La mission de ce tiers de confiance [346] consiste, sur la base d'un contrat conclu avec son client, à réceptionner la ou les pièce(s) justificative(s) déposée(s) et présentée(s) par le contribuable à l'appui de chacune des déductions du revenu global, réductions ou crédits d'impôts, à établir la liste de ces pièces ainsi que des montants y figurant, à attester de l'exécution de ces opérations, à conserver la ou les pièces jusqu'à l'extinction du délai de reprise de l'administration fiscale et à la ou les transmettre à cette dernière sur sa demande.

(345) V. art. 151-2 du décret n°2011-1997 du 28 décembre 2011 (J.O. du 29 décembre 2011) modifié par le décret n°2019-1193 du 19 novembre 2019.

(346) Les disposions relatives aux tiers de confiance visés à l'article 170 ter du Code général des impôts sont fixées aux articles 95 ZA à 95 ZN du Code général des impôts. V. également sur le sujet : instruction Bofip, Dispositions juridiques communes – Tiers de confiance, BOI du 14 décembre 2017, BOI-DJC-TDC.

Ce dispositif est mis en œuvre par une série d'instruments contractuels où les acteurs organisent les modalités de la dématérialisation entre eux.

On notera à cet égard que le pouvoir réglementaire impose également au client d'autoriser dans la lettre de mission, outre les autres engagements déterminés, le tiers de confiance à procéder « *à la télétransmission de sa déclaration annuelle d'impôt sur le revenu et de ses annexes (…)* ».

Un arrêté du 1er mars 2012 fixe les modèles des conventions nationales prévues à l'article 95 ZF de l'annexe II du Code général des impôts et qui doivent être conclues entre les organismes représentant au niveau national les membres des professions réglementées d'avocat, de notaire et de l'expertise comptable et la direction générale des finances publiques.

Cet arrêté fixe également les modèles des conventions individuelles prévues à l'article 95 ZG de l'annexe II du même code, et devant être conclues entre un membre de ces trois professions réglementées et la direction départementale ou régionale des finances publiques ou le délégataire du directeur général des finances publiques (347). L'architecture contractuelle applicable doit respecter ces dispositions réglementaires.

La digitalisation des professions d'expert-comptable, d'avocat et de notaire doit ainsi également tenir compte du rôle de confiance qu'ils occupent déjà juridiquement du fait de leur statut réglementé.

À cet égard, le niveau de sécurité des procédés utilisés et les garanties y étant attachées apparaissent essentiels. Les Prestataires de services de confiance doivent ainsi trouver leur place pour accompagner ces professions dont le métier initial est loin des préoccupations technologiques.

(347) Cet arrêté (J.O. du 9 mars 2012, p. 4398) était toujours d'actualité au 12 janvier 2022.

3. La dématérialisation des procédures douanières

En matière douanière, le droit de l'Union européenne et le droit français ont progressivement opéré un glissement de certaines procédures « ***papier*** » **vers la voie électronique**.

Au niveau de l'Union européenne

Le régime juridique des opérations douanières est soumis à l'article 28, paragraphe 1, du traité sur le fonctionnement de l'Union européenne [348] . Ce dernier établit que : « *L'Union comprend une union douanière qui s'étend à l'ensemble des échanges de marchandises et qui comporte l'interdiction, entre les États membres, des droits de douane à l'importation et à l'exportation et de toutes taxes d'effet équivalent, ainsi que l'adoption d'un tarif douanier commun dans leurs relations avec les pays tiers.* ».

Dans cette logique et afin d'adopter un cadre commun pour les opérations douanières, l'Union européenne s'est dotée, dès 1992, d'un Code des douanes communautaires avec l'adoption de deux règlements, dont le règlement CEE n°2913/9 [349] qui prévoyait en son article 61 :

« *La déclaration en douane est faite :*

- *a) soit par écrit ;*
- *b) soit en utilisant un procédé informatique, lorsque cette utilisation est prévue par les dispositions arrêtées selon la procédure du comité ou autorisée par les autorités douanières ; [...]* ».

Ces dispositions ont progressivement évolué notamment avec l'adoption :

+ Du Règlement (CE) N°450/2008 du Parlement européen et du Conseil du 23 avril 2008 établissant le Code des douanes communautaire (Code des Douanes Modernisé) [350] dont l'article 5 - Échange et stockage de données disposait :

  « *Tout échange de données, de documents d'accompagnement, de décisions et de notes opéré entre autorités douanières ou entre opérateurs économiques et autorités douanières requis en vertu de la législation douanière ainsi que le stockage de ces données en vertu de la législation douanière doivent doit être effectués en utilisant un procédé informatique de traitement des données. [...]* ».

(348) Version consolidée en date du 26.10.2012 disponible sous le lien : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A12012E%2FTXT.

(349) À savoir le Règlement CEE n° 2913/92 du Conseil du 12 octobre 1992 établissant le Code des douanes communautaire (J.O.CE L 302 du 19.10.1992)- Version consolidée en date du 01.01.2007 disponible sous le lien : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1992R2913:20070101:FR:PDF et le Règlement CEE n° 2454/93 de la Commission du 2 juillet 1993 fixant certaines dispositions d'application du règlement (CEE) n° 2913/92 du Conseil établissant le Code des douanes communautaire (J.O. L 253 du 11.10.1993)Version consolidée en date du 01.01.2012 disponible sous le lien : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993R2454:20120101:FR:PDF.

(350) Règlement (CE) N°450/2008 du Parlement européen et du Conseil du 23 avril 2008 établissant le Code des douanes communautaire (Code des Douanes Modernisé) disponible sous le lien : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:145:0001:0064:FR:PDF

- Du Règlement UE n° 952/2013 du Parlement européen et du Conseil du 9 octobre 2013 établissant le Code des douanes de l'Union (refonte) [351] abrogeant le règlement n°450/2008 avant même que celui-ci soit mis entièrement en application. Ce nouveau règlement a affirmé la place prépondérante de la voie électronique au sein des échanges douaniers faisant des procédures papier l'exception. Ses dispositions s'appliquent depuis le 1er mai 2016 [352].
- du Règlement (UE) 2016/2339 du Parlement européen et du Conseil du 14 décembre 2016 [353],
- du Règlement (UE) 2019/474 du Parlement européen et du Conseil du 19 mars 2019 [354],
- et du Règlement (UE) 2019/632 du Parlement européen et du Conseil du 17 avril 2019 [355].

Il résulte de ces textes que la dématérialisation de certaines procédures en matière douanière repose sur des fondements juridiques communautaires.

En France, les procédures douanières par voie électronique ont progressivement été intégrées dans le droit national.

À titre principal, on citera :

- La loi n° 2004-1485 du 30 décembre 2004 [356] de finances rectificatives pour 2004 qui a intégré la voie électronique aux articles 85 et 95 du Code des douanes pour les déclarations dans le cadre des opérations de dédouanement. Ces dispositions ont conduit à la mise en place de téléprocédures accessibles à partir du site des douanes [357].
- La loi n° 2011-1978 du 28 décembre 2011 [358] qui a introduit au sein du Code des douanes l'article 322 permettant, **dans le cadre des contentieux et recouvrement, le recours à la signature électronique** :

(351) Disponible sous le lien http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:269:0001:0101:FR:PDF .

(352) Ce Règlement a toutefois été modifié par le Règlement (UE) 2016/2339 du Parlement européen et du Conseil du 14 décembre 2016 (J.O.UE du 23/12/2016, L354/32), le Règlement (UE) 2019/474 du Parlement européen et du Conseil du 19 mars 2019 (J.O.UE du 25/03/2019, L83/38) et le Règlement (UE) 2019/632 du Parlement européen et du Conseil du 17 avril 2019 (J.O.UE du 25/04/2019, L111/54). Voir : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02013R0952-201905

(353) J.O.UE du 23/12/2016, L354/32.

(354) J.O.UE du 25/03/2019, L83/38.

(355) J.O.UE du 25/04/2019, L111/54 (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02013R0952-201905).

(356) J.O. du 31 décembre 2004.

(357) Site accessible à l'adresse https://www.douane.gouv.fr/service-en-ligne.

(358) Loi n° 2011-1978 du 28 décembre 2011 de finances rectificative pour 2011, J.O. du 29 décembre 2011.

+ « *Les procès-verbaux et les autres actes établis en application du présent code peuvent être revêtus d'une signature numérique ou électronique. La liste des actes concernés ainsi que les modalités de cette signature et les personnes qui peuvent y recourir sont précisées par décret en Conseil d'État.*

  Les actes mentionnés au premier alinéa peuvent être conservés sous forme dématérialisée dans des conditions garantissant leur intégrité et leur sécurité. »

+ En application de cette loi, le décret n° 2013-956 du 24 octobre 2013 relatif à la dématérialisation de certains actes établis en application du code des douanes [359] a été adopté.

  Il précise **les modalités du recours à la signature électronique dans le cadre de la répression des infractions relatives à la taxe sur les véhicules de transport de marchandise et détermine notamment les documents sur lesquels la signature peut être apposée, les acteurs pouvant en faire usage et les modalités d'archivage des documents signés électroniquement.**

Sur le fondement de ces textes, les services des douanes françaises ont mis à disposition, via leur site internet **ProDou@ne** [360], une plateforme interactive permettant de naviguer entre les différentes applications douanières.

Parmi les nombreux téléservices mis en place, on notera l'application Delta-G [361] qui permet aux opérateurs télédéclarants d'établir leurs déclarations en douane simplifiées et leurs déclarations en douane complètes par voie électronique.

(359) Décret n° 2013-956 du 24 octobre 2013 relatif à la dématérialisation de certains actes établis en application du Code des douanes, J.O. du 26 octobre 2013, p.17523.

(360) Site disponible sous le lien : https://pro.douane.gouv.fr/.

(361) Venu remplacer début 2016 les anciens programmes DELT@-C (Déclaration de droit commun en une étape) et DELT@-D (Déclaration simplifiée domiciliée en deux étapes). Pour plus de détail voir le lien : https://www.douane.gouv.fr/fiche/delta-g-un-service-en-ligne-unifie-pour-le-dedouanement.

En outre, le **guichet unique national du dédouanement (GUN)** désigne le dispositif informatique permettant le contrôle automatisé et instantané des documents d'ordre public dont la présentation est exigée lors de l'accomplissement des formalités douanières.

Débutée en 2015, cette initiative tend à rendre possible à terme le dédouanement de tous les types de marchandises de manière dématérialisée (362).

À titre indicatif, il est précisé que le gouvernement a annoncé qu'aux fins de simplification administrative pour les entreprises, **la refonte de plusieurs téléservices dédiés aux professionnels est prévue.**

Dans ce cadre, début 2023, le projet portailpro.gouv.fr devrait permettre aux entreprises d'accéder dans un seul et même espace, à l'aide d'un identifiant unique, aux services des impôts, des URSSAF et de la Douane. Sont concernées les formalités de déclaration et de paiement (363).

4. Procédure électronique de légalisation de signature et d'apostille

Les procédures de légalisation et d'apostille permettent d'attester de la véracité de la signature de l'auteur d'un acte, de la qualité en laquelle le signataire a agi et le cas échéant, de l'identité du sceau ou timbre dont l'acte est revêtu.

Le décret n° 2021-1205 du 17 septembre 2021 (364) pose les principes de la dématérialisation des formalités de légalisation et d'apostille. Ce texte précise que l'autorité compétente délivrant la légalisation ou l'apostille devra utiliser un procédé de signature électronique qualifiée « *conforme aux exigences du décret du 28 septembre 2017* » (dernier alinéa de l'article 3 du décret). Il est précisé qu'un certain nombre d'informations y afférent devra être enregistré dans une base de données nationale.

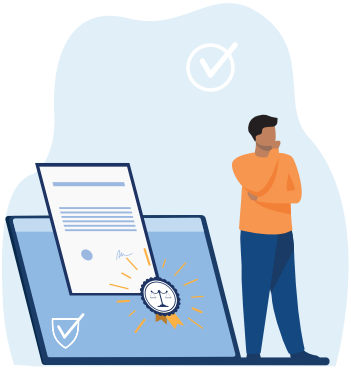
L'autorité compétente sera tenue de donner suite aux demandes de légalisation et d'apostille électronique, seulement si elle dispose des moyens nécessaires pour réaliser ces formalités par voie électronique. À défaut, la procédure se fera sur support papier.

(362) A propos du GUN, v. le rapport établi par la Direction générale des douanes, le GUN, novembre 2019, accessible à l'adresse : https://www.douane.gouv.fr/sites/default/files/uploads/files/Documentations-Brochures/Professionnels/le-guichet-unique-national-du-dedouanement-%28GUN%29-2019.pdf.

(363) V. la communication à l'adresse : https://www.gouvernement.fr/la-vie-des-entreprises-simplifiee-avec-de-nouvelles-plateformes-en-ligne.

(364) Loi n° 2011-1978 du 28 décembre 2011 de finances rectificative pour 2011, J.O. du 29 décembre 2011.

Enfin, toutes les légalisations et apostilles délivrées par voie électronique devront être enregistrées par chaque autorité compétente pour les délivrer dans un même registre électronique. Les dispositions règlementaires relatives à la base de données des signatures publiques s'appliqueront à compter du 1er janvier 2023. Les autres dispositions entreront en vigueur le 1er septembre 2023.



Les arrêtés prévus en application de ce décret apporteront des éclaircissements quant aux modalités opérationnelles et technologiques requises.

Les Prestataires de service de confiance pourraient en ce domaine tenir un rôle.

5. La dématérialisation de certaines procédures d'urbanisme

Avec la loi n° 2018-1021 du 23 novembre 2018 portant évolution du logement, de l'aménagement et du numérique (dite loi Elan [365]), le processus de dématérialisation des autorisations d'urbanisme a été encadré. Sont concernés les demandes de permis de construire et de démolir, les déclarations préalables, les demandes de permis d'aménager et les certificats d'urbanisme. En revanche, ces dispositions ne s'appliquent ni aux demandes relatives aux ouvrages particuliers (établissements recevant du public, immeubles de grande hauteur…) ni aux déclarations d'intention d'aliéner (DIA), ces dernières n'étant pas à proprement parler des autorisations d'urbanisme.

L'article L. 423-3 du Code de l'urbanisme prévoit ainsi que les communes de plus de 3500 habitants doivent disposer d'une téléprocédure spécifique leur permettant de recevoir et d'instruire sous forme dématérialisée les demandes d'autorisation d'urbanisme déposées. Cette obligation s'applique depuis le 1er janvier 2022.

L'article L. 423-3 du Code de l'urbanisme prévoit la possibilité de mutualiser cette téléprocédure au travers du service en charge de l'instruction des actes d'urbanisme.

(365) V. plus particulièrement l'article 62 de cette loi.

LA DIGITALISATION DANS LA SPHÈRE PUBLIQUE

La dématérialisation des actes d'urbanisme est enfermée dans des modalités issues de dispositions éparses codifiées dans la partie réglementaire du Code de l'urbanisme. Il en est ainsi de certains articles créés ou modifiés par le décret n° 2019-472 du 20 mai 2019 relatif à la collecte et la transmission d'informations et de documents relatifs aux déclarations et autorisations d'occupation des sols et plus récemment par le décret n° 2021-981 du 23 juillet 2021 portant diverses mesures relatives aux échanges électroniques en matière de formalité d'urbanisme.

En application de ce dernier texte, la téléprocédure devra notamment respecter certaines exigences spécifiques dont, par exemple, la mention d'un numéro d'enregistrement dans l'accusé de réception pour les demandes d'urbanisme (art. R. 410-3 du Code de l'urbanisme), la possibilité de prévoir la publication d'un extrait de permis, voire de la décision, par voie électronique en lieu et place d'un affichage en mairie (art. R. 424-15 du Code de l'urbanisme), ou bien encore la dispense de produire des exemplaires supplémentaires et des copies de pièce pour le pétitionnaire (art. R. 474-1 du Code de l'urbanisme).

L'article A423-5 du Code de l'urbanisme créé par l'arrêté du 27 juillet 2021 détermine quant à lui les exigences fonctionnelles que la téléprocédure doit garantir tant pour le demandeur (particulier, promoteur…) que pour l'administration destinatrice de la demande ou de la déclaration.

En application de ces textes, l'État a développé la plateforme PLAT'AU [366] (Plateforme des Autorisations d'Urbanisme) qu'il met à disposition des communes qui souhaitent y interfacer leur système d'information. Cette chaîne de télétransmission thématique vient compléter l'application @CTES déjà existante. Elle s'inscrit dans la logique de l'article R. 331-10 du Code de l'urbanisme et des obligations afférentes au contrôle de légalité (notamment sur la base de l'article L. 2131-1 du Code général des collectivités territoriales).

L'État entend également proposer des outils comme RIE'AU (Réception, information et échanges des Autorisations d'Urbanisme) aux communes éligibles afin qu'elles réceptionnent via une interface les demandes des pétitionnaires ou le portail AD'AU (Assistance aux Demandes d'Autorisation d'Urbanisme) accessible depuis le site : service-public.fr qui permet aujourd'hui au pétitionnaire de constituer sa demande en ligne, et de la transmettre prochainement de manière dématérialisée à son guichet unique.

Ceci étant, il est important de rappeler qu'**en vertu du principe de libre administration des collectivités territoriales** [367]**, les communes peuvent choisir d'élaborer et d'utiliser une téléprocédure d'actes d'urbanisme indépendamment de celle proposée par l'État**.

(366) V. pour une présentation : https://www.collectivites-locales.gouv.fr/institutions/ctes-dematerialisation-de-la-transmission-des-actes.

(367) Principe constitutionnel issu de l'article 72 de la Constitution du 4 octobre 1958.

Cette téléprocédure devra toutefois respecter les exigences fonctionnelles posées par les dispositions du Code de l'urbanisme en la matière. La mutualisation de la téléprocédure entre plusieurs collectivités reste envisageable.

Les prestataires de services de confiance doivent pouvoir les accompagner dans la réalisation de tels projets que ce soit par exemple pour les procédures de numérisation de pièces jointes, l'offre de service d'horodatage fiable, la génération d'accusés d'enregistrement et de réception, la signature des demandes par le pétitionnaire…

6. Les procédures consultatives en ligne

Sur la base de l'article L. 131-1 du CRPA, les consultations en ligne du public sont devenues courantes même lorsqu'elles ne sont pas obligatoires. À titre d'illustration, en matière de cyber-sécurité et bonnes pratiques, l'ANSSI a pris l'habitude de solliciter les acteurs des secteurs privé et public concernés par ses divers guides afin de les inviter à partager leurs expériences, questions et suggestions sur un sujet donné [368].

Dans ce contexte juridique, l'avis donné reste consultatif et ne saurait de droit s'imposer aux administrations. Toutefois, l'article L. 131-1 du CRPA précise que lorsqu'elle choisit de consulter le public, l'administration doit rendre publiques les informations utiles et offrir un délai raisonnable permettant la participation des intéressés. La publication des résultats et des suites envisagées est également obligatoire.

Dans certains cas, l'autorité administrative est tenue de procéder à la consultation d'une **commission consultative préalablement à l'édiction d'un acte réglementaire. Le cas échéant, elle peut organiser sur un site internet une consultation ouverte pour recueillir les observations des personnes concernées conformément à l'article L. 132-1 du CRPA** [369].

(368) Lorsque l'ANSSI souhaite mettre à jour la version d'un guide de bonnes pratiques qu'elle a élaboré, elle fait souvent appel à la consultation en ligne des personnes intéressées (usagers comme professionnels). Tel a été le cas par exemple de la mise à jour des Bonnes pratiques à l'usage des professionnels en déplacement (« outils nomades »), consultable à l'adresse : https://www.ssi.gouv.fr/administration/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/ (consulté le 25/11/2019).

(369) Initiée à l'article 16 de la loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, J.O. du 18 mai 2011 p. 8537 ; cette possibilité a été codifiée après modification par l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du CRPA (réf. cit. supra).

Les articles L.132-2 et L.132-3 du CRPA fixent les principes relatifs aux informations portant sur une telle consultation, aux conditions de communication de son résultat (synthèse rendue publique) ainsi que sa durée d'ouverture (qui ne peut être inférieure à 15 Jours).

Les articles R.132-4 et suivants [370] du CRPA fixent quant à eux les modalités de cette consultation électronique. Ces articles prévoient notamment que la publication de la décision d'organiser une consultation soit 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 [371].

De plus, cette décision d'organiser une consultation ouverte doit être publiée sur un site internet du Premier ministre lorsque c'est une administration d'État ou un de ses établissements publics qui est concerné ou sur le site internet choisi par l'autorité administrative territoriale lorsque la décision est prise par une administration locale.

Il est également prévu que la synthèse des observations recueillies dans le cadre de la consultation ouverte soit 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 [372].

L'article R.132-8 du CRPA oblige par ailleurs les administrations de l'État à publier sur un site du Premier ministre les consultations organisées en application de dispositions législatives ou réglementaires qui imposent la consultation du public préalablement à l'adoption d'un acte réglementaire ayant un champ d'application national. Il en est ainsi par exemple du droit de l'environnement et des procédures de participation du public à l'élaboration de certaines décisions susceptibles d'avoir une incidence sur l'environnement qui prévoit les modalités électroniques de cette consultation, en parallèle des modalités « physiques » qui perdurent [373].

Les consultations sur des projets de loi doivent également être publiées sur un site du Premier ministre (article R.132-9 du CRPA).

(370) Décret n° 2011-1832 du 8 décembre 2011 relatif aux consultations ouvertes sur l'internet, J.O. du 9 décembre 2011, modifié par le Décret n° 2015-1342 du 23 octobre 2015 relatif aux dispositions réglementaires du Code des relations entre le public et l'administration (réf. cit. supra).

(371) V. art. R.132-5 du CRPA.

(372) V. art. R.132-6 du CRPA.

(373) V. notamment les articles L.121-16 et s. du Code de l'environnement issus de la loi n° 2018-148 du 2 mars 2018 ratifiant les ordonnances n°2016-1058 du 3 août 2016 relative à la modification des règles applicables à l'évaluation environnementale des projets, plans et programmes et n°2016-1060 du 3 août 2016 portant réforme des procédures destinées à assurer l'information et la participation du public à l'élaboration de certaines décisions susceptibles d'avoir une incidence sur l'environnement, J.O. du 3 mars 2018.

Enfin, en dehors de ces cas, l'article R.132-10 du CRPA laisse la possibilité aux administrations de l'État et à ses établissements publics de rendre publiques sur un site du Premier ministre, les procédures de consultation du public qu'ils organisent préalablement à l'adoption d'un acte réglementaire.

En pratique, la consultation en ligne du public avant l'adoption d'actes réglementaires apparaît comme une procédure de plus en plus usitée. Les administrations doivent toutefois savoir qu'une telle consultation est encadrée, et ce, tant pour les administrations d'État que pour les administrations territoriales.

À défaut de respecter les modalités posées en la matière, une illégalité formelle pourrait entacher l'acte adopté par la suite. Dès lors, la consultation en ligne, obligatoire ou facultative, devra reposer sur un système permettant de rapporter la preuve du respect des exigences formelles posées.

De même, les conditions générales d'utilisation de la téléconsultation mise en place devront être pertinemment rédigées.

Les prestataires de service de confiance peuvent apporter une valeur ajoutée certaine, aux administrations dans la mise en œuvre de leur projet de consultation par voie électronique.

7. Les espaces personnels numériques des usagers

La digitalisation s'accompagne de la volonté de simplifier les procédures administratives. A cette fin, la création d'espaces personnels pour les usagers, particuliers et professionnels, constitue une pratique de plus en plus répandue dans la sphère publique. Il en est ainsi par exemple des comptes fournisseurs dans Chorus Pro pour la commande publique, des comptes élèves, étudiants, parents ou professeurs dans les espaces numériques de travail (ENT) dans le secteur de l'enseignement, des espaces numériques fiscaux pour les particuliers et les entreprises dans le domaine fiscal…

D'un point de vue juridique, ces espaces personnels doivent respecter **le régime général des télé-procédures** [374]**, les dispositions spécifiques applicables selon le domaine le cas échéant et la réglementation relative à la protection des données personnelles traitées**. Le respect de ces exigences peut conditionner la légalité des échanges réalisés, des décisions éventuellement prises et de leur opposabilité et engager la responsabilité de l'administration concernée. L'enjeu est donc de taille. C'est pourquoi tout projet « *d'espace personnel* » nécessite la collaboration de compétences expertes tant juridiques que technologiques.

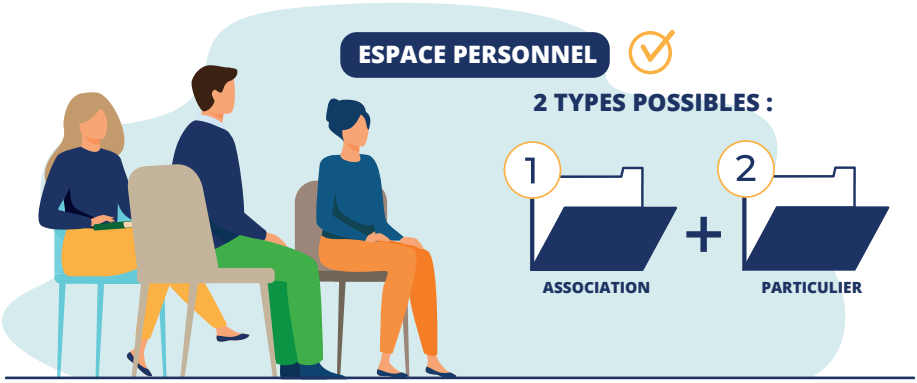
Ceci étant précisé, les développements qui suivent font référence aux textes juridiques applicables à certains espaces personnels numériques créés. Ils ne constituent pas une analyse de la conformité légale des exemples traités.

Au niveau de l'État, l'article 7 de l'ordonnance n° 2005-1516 du 8 décembre 2005 [375] a créé un service public mettant à disposition de l'usager un espace de stockage accessible en ligne. Ce téléservice est exploité sous la responsabilité de l'État. Cet espace de stockage est placé sous le contrôle de l'usager qui en est titulaire.

Seuls deux types de compte intégrant un espace de stockage en ligne sont possibles :

+ un compte « *particulier* » pour les besoins des particuliers
+ et un compte « *association* » pour les besoins des associations.

L'espace de stockage est ouvert et clos à la demande de son titulaire. Il permet à l'intéressé de conserver et de communiquer ses informations et documents aux autorités administratives pour l'accomplissement de ses démarches.



(374) V. les points A, B, C et E de la partie II du présent Vade-Mecum pour avoir une vision générale des principes juridiques applicables.

(375) Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, ratifiée par l'article 138 I de la loi n° 2009-526 du 12 mai 2009.

Sous réserve de l'autorisation de l'usager concerné, les administrations peuvent y déposer des documents ou obtenir la transmission d'informations ou de documents dont elles ont à connaître.

En l'état des derniers textes applicables début 2022, les modalités de cet espace de stockage ont été fixées par le décret n° 2016-186 du 24 février 2016 [376] et par l'arrêté du 24 février 2016 [377].

Il résulte de ces dispositions réglementaires que seuls les usagers « *bénéficiant au préalable d'un compte sur un portail en ligne, créé par arrêté du Premier ministre* » peuvent ouvrir un tel espace de stockage.

Les conditions d'inscription et d'utilisation, les fonctionnalités et les contraintes de sécurité y sont également décrites. L'arrêté du 24 février 2016 énumère limitativement les informations pouvant être stockées. Enfin, le téléservice est régi par des conditions générales d'utilisation qui s'imposent aux usagers [378].

En pratique, selon la direction de l'information légale et administrative (DILA), « *service-public.fr compte 7 millions de comptes personnels ouverts (dont 2 millions créés sur la seule année 2020) et près de 5 millions de démarches en ligne réalisées directement (près de 2 millions de demandes d'acte d'état civil et 1 million de déclarations de changement de coordonnées ont été réalisées en 2020)* » [379].

Parallèlement, il est intéressant de signaler que le décret du 29 novembre 2021 [380] a créé à titre expérimental le téléservice « *Mon FranceConnect* ». À destination des usagers des administrations et des administrations elles-mêmes, ce téléservice a pour objet de mettre à disposition de l'usager un espace en ligne lui permettant d'obtenir un accès aux informations ou données le concernant que des administrations peuvent se partager entre elles, via une API, sur la base de l'article L.114-8 du CRPA [381]. En utilisant Mon FranceConnect, l'usager peut également obtenir un accès aux informations utiles le concernant dans le cadre de ses échanges avec les administrations (par exemple pour connaître l'avancement de ses démarches).

(376) Décret n° 2016-186 du 24 février 2016 modifiant le 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 26 février 2016.

(377) Arrêté du 24 février 2016 portant intégration au site internet « service-public.fr » d'un téléservice permettant à l'usager d'accomplir des démarches administratives en tout ou partie dématérialisées et d'avoir accès à des services d'informations personnalisés, J.O. du 26 février 2016.

(378) Conditions accessibles à l'adresse : https://www.service-public.fr/P10050.

(379) V. DILA, Rapport d'activité 2020, mai 2021, p. 25.

(380) Décret n° 2021-1538 du 29 novembre 2021 relatif à l'expérimentation du téléservice dénommé « Mon FranceConnect » (MFC), J.O. du 30 novembre 2021.

(381) V. sur ces échanges nos développements points II.A et B.

Il est également prévu que ce téléservice prodigue des conseils ciblés au bénéfice de l'usager, sur ses droits et devoirs, élaborés sur la base des informations et données traitées par Mon FranceConnect. Enfin, ce téléservice doit permettre à l'usager de générer des justificatifs pouvant être produits auprès des administrations dans le cadre de ses démarches. La connexion à ce téléservice doit se faire via FranceConnect (381).

Cette expérimentation prévue pour une durée de 12 mois est limitée à 25.000 usagers volontaires. Un bilan sera établi 6 mois après la fin de l'expérimentation afin d'en apprécier les points forts et les lacunes. Selon les résultats de l'expérimentation Mon FranceConnect, le téléservice de l'espace de stockage « *service-public.fr* » pourrait être impacté. Il conviendra donc de suivre les évolutions à cet égard.

Au niveau des collectivités territoriales, plusieurs d'entre elles ont mis à disposition de leurs usagers des espaces numériques « *locaux* » (382). Cette possibilité repose sur le **principe constitutionnel de libre administration des collectivités territoriales** (383).

Ce service doit néanmoins a minima respecter les exigences juridiques applicables aux téléprocédures et à la protection des données à caractère personnel (cf. supra notamment les points II.A, B et E). D'autres textes peuvent en outre s'appliquer selon les spécificités de la démarche (aides médico-sociales, mineurs…).

Les collectivités territoriales doivent pouvoir s'appuyer sur des outils et services de confiance leur permettant d'offrir à leurs usagers un service « *espace numérique* » de qualité. Dans cette finalité, les prestataires de services de confiance ont un véritable rôle à jouer.

(381) V. sur FranceConnect nos développements au point II.A.2).

(382) Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, ratifiée par l'article 138 I de la loi n° 2009-526 du 12 mai 2009.

Citons par exemple au niveau des régions, le « compte jeune » mis à disposition des bénéficiaires du service régional « Pass'Région » de la Région Auvergne-Rhône-Alpes ; au niveau des départements, le compte « mesdémarches06 » pour les usagers résidents dans le 06 et mis en place par le département des Alpes-Maritimes ; au niveau des communes, « mon espace de démarches en ligne » mis à disposition par la ville de Rouen à ses usagers sous réserve de l'ouverture d'un compte.

(383) Principe constitutionnel issu de l'article 72 de la Constitution du 4 octobre 1958.

8. Les espaces personnels dans le domaine médico-social

Dans le domaine de la santé, la digitalisation est devenue un enjeu aux multiples facettes [384].

Plusieurs acteurs sont concernés : bien évidemment le **patient**, mais également les services de soins, d'aide et de remboursement qui peuvent être **des personnes publiques ou des personnes morales de droit privé chargées de mission de service public** (hôpitaux, centres médico-sociaux, caisse d'assurance maladie, centre communal d'action social, service départemental…) et/ou **des personnes de droit privé** (médecins indépendants, pharmaciens, cliniques, mutuelles…).

En outre, les données de santé revêtent une nature particulière [385]. **Parfois vitales, toujours intimes, elles sont soumises à un régime juridique spécifique qui tente de trouver un équilibre entre les différents intérêts en présence. Le droit doit alors relever le défi de permettre les échanges et la diffusion des informations relatives aux données de santé tout en maintenant le respect du secret professionnel et la protection de la vie privée des personnes concernées** [386].

Ces différents éléments expliquent que les téléservices et les téléprocédures en matière médico-sociale sont en pleine évolution, tout comme leur régime juridique [387]. Il s'agit de l'un des grands chantiers de la transformation digitale de notre société, et les PSCo doivent s'assurer d'y tenir un rôle primordial. Les développements qui suivent offrent une approche partielle de certains aspects juridiques de la dématérialisation dans ce domaine.

De plus, les régimes juridiques nationaux des espaces personnels de santé devraient évoluer sous l'impulsion de l'Union européenne. En effet, le 3 mai 2022, la Commission européenne a proposé un Règlement pour instituer un espace européen des données de santé [388]. Il conviendra de suivre l'adoption de ce texte ambitieux afin de connaître son impact sur le régime juridique français actuellement en vigueur.

(384) La traçabilité et la transparence induites par la digitalisation du système de santé poursuivent ainsi différentes finalités dont une meilleure gestion de la santé publique (suivi médical des patients plus informé) mais également des finances publiques (gestion des établissements de santé, de la sécurité sociale, des remboursements…).

(385) Les données de santé sont traitées dans la présente partie exclusivement au regard des téléservices et téléprocédures envisagés. Le régime propre aux données de santé au regard de la législation relative à la protection de ce type de données, sur la base du RGPD et de la loi Informatique et libertés n'est pas traité ici. V. sur la question des données à caractère personnel et des Prestataires de services de confiance nos développements dans la partie dédiée dans le présent Vade-mecum.

(386) V. E. Debiès, Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ?, Revue française d'administration publique 2018/3 (N° 167), pages 565 à 574.

(387) V. en ce sens, la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, J.O. 26 juillet 2019, dont le titre III « Développer l'ambition numérique en santé » parle de lui-même. Ce texte législatif prévoit au demeurant l'adoption de nombreuses ordonnances et décrets, dont certains ont déjà été adoptés et d'autres restent à venir.

(388) Commission européenne, Proposition de Règlement instituant un espace européen de données de santé, COM(2022) 197/2, 3 mai 2022, accessible en anglais à partir de l'adresse : https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en.

a. L'espace numérique de santé, le dossier médical partagé et le dossier pharmaceutique

Les articles L. 1111-13 à L. 1113-2 (389) du Code de la santé publique et R. 1111-26 à R. 1111-39 (390) du Code la santé publique régissent désormais l'espace numérique de santé (391) qui est ouvert automatiquement, sauf opposition de la personne ou de son représentant légal.

Conçu et mis en œuvre sous la responsabilité conjointe du ministre chargé de la santé et de la Caisse nationale de l'assurance maladie (CNAM) (392), l'espace numérique de santé est censé permettre à son titulaire « *dûment identifié et authentifié* » (393) d'accéder en ligne à un certain nombre de données le concernant et à des outils et services numériques énumérés de façon particulièrement large à l'article L. 1111-13-1 §II du Code de la santé publique.

À cet égard, il est précisé que lesdits services et outils numériques en santé, qui peuvent être développés par des éditeurs publics ou privés, doivent respecter les référentiels d'interopérabilité et de sécurité établis par l'Agence nationale des systèmes d'information partagés (394).

De plus, les règles relatives aux modalités d'hébergement des données de santé devront être scrupuleusement suivies (article L. 1111-8 et s. du Code de la santé publique (394)).

La création de ces espaces numériques de santé a donc vocation à concerner un très vaste public tant au niveau des usagers que des professionnels impliqués (CNAM, centre hospitalier, médecin, pharmacien, maison de convalescence conventionnée, maison des personnes handicapées, services sociaux départementaux…) avec des services et outils dont la diversité est clairement affirmée.

Au titre de l'une des composantes de l'espace numérique de santé, se trouve le dossier médical partagé (DMP) comme l'indique expressément l'article L. 1111-13 du Code de la santé publique.

(389) Dernièrement modifiés par la loi n° 2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique, J.O. du 8 décembre 2020, v. article 98.

(390) Issus du décret n° 2021-1048 du 4 août 2021 relatif à la mise en œuvre de l'espace numérique de santé, J.O. du 7 août 2021.

(391) La plupart de ces dispositions sont en effet entrées en vigueur depuis le 1er janvier 2022.

(392) Comme précisé à l'article R.1111-26 du Code de la santé publique.

(393) Cette identification repose notamment sur le numéro national de santé, c'est-à-dire sur le numéro d'inscription au répertoire national d'identification des personnes physiques (plus connu sous les acronymes NIR), lorsque la personne concernée en a un (article L.1111-13-1 et L.1111-8 du Code de la santé publique). V. plus largement pour une réflexion sur l'utilisation du NIR : É. Debiès, Renforcement des droits des individus sur leurs données personnelles : quelles conséquences sur l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ?, Regards 2019/1 (N° 55), pages 149 à 155.

(394) V. articles L.1111-13-1, §III et R.1111-37 et s. du Code de la santé publique.

(395) V. également sur ce point nos développements II.B relatifs aux échanges entre administrations.

Après plusieurs modifications textuelles [396], le DMP est désormais automatiquement créé à l'ouverture de l'espace numérique de santé (lui-même créé automatiquement sauf opposition de la personne). Son régime juridique résulte notamment des articles L. 1111-14 à L. 1111-22 du Code de la santé publique. Créé pour favoriser la prévention, la coordination, la qualité et la continuité des soins, le DMP répond à des exigences spécifiques en matière d'accès aux données qu'il contient.

La Caisse nationale d'assurance maladie (CNAMTS) est chargée de sa conception, de sa mise en œuvre et de son administration dans le respect des procédures techniques et organisationnelles définies.

Ceci étant précisé, les articles R. 1111-26 à R. 1111-39 du Code de la santé publique relatifs à l'espace numérique de santé sont applicables au DMP. Dès lors, les éditeurs publics ou privés concernés devront respecter les référentiels d'interopérabilité et de sécurité établis par l'Agence nationale des systèmes d'information partagés [397].

Parallèlement à la mise en place du dossier médical partagé, le dossier pharmaceutique a été créé [398]. Il vise à favoriser la coordination, la qualité, la continuité des soins et la sécurité de la dispensation des médicaments, produits et objets définis à l'article L. 4211-1 du Code de la santé publique [399]. Sauf opposition du patient, le pharmacien est tenu d'alimenter ce dossier. Les fonctionnalités et caractéristiques du dossier pharmaceutique sont posées à l'article L. 1111-23 du Code de la santé publique.

Désormais, les modalités de sa mise en œuvre et de son fonctionnement relèvent des règles applicables à l'espace numérique de santé (c'est-à-dire des articles R.1111-26 à R.1111-39 du Code de la santé publique auxquels il est renvoyé).

(396) Dont les dispositions ayant conduit à la création du dossier médical personnel et à son remplacement par le dossier médical partagé ; v. la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (J.O. 5 mars 2002), la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (J.O. 17 août 2004), la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (J.O. 27 janvier 2016) et plus récemment la loi n° 2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique (J.O. 8 décembre 2020) et l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie (J.O. 13 mai 2021).

(397) V. articles L.1111-13-1, §III et R.1111-37 et s. du Code de la santé publique.

(398) V. initialement la loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique (1) (Titre résultant de la décision du Conseil constitutionnel n° 2007-546 DC du 25 janvier 2007) et récemment la loi n° 2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique (J.O. 8 décembre 2020).

(399) Article L.1111-23 du Code de la santé publique, antérieurement article L.161-36-4-2 du Code de la sécurité sociale. Cette modification est intervenue par le biais de l'article 50 de la Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, J.O. du 22 juillet 2009.

b. La force probante des documents électroniques comportant des données « médico-sociales »

La section 4 (articles L. 1111-25 et suivants) du chapitre 1er du Titre 1er du Livre 1er « *Protection des personnes en matière de santé* » de la 1ère partie législative du Code de la santé publique traite spécifiquement de la force probante de certains documents.

L'article L. 1111-25 du Code de la santé publique détermine, de façon très large, le périmètre d'application de ces dispositions.

Ainsi, il s'agit des documents :

+ Comportant des données de santé à caractère personnel,
+ qui ont été produits, reçus ou conservés,
+ « *à l'occasion d'activités de prévention, de diagnostic, de soins, de compensation du handicap, de prévention de perte d'autonomie, ou de suivi social et médico-social réalisées dans les conditions de l'article L. 1110-4, » par :*

  « 1° Un professionnel de santé, un établissement ou service de santé ;

  2° Un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code ;

  3° Le service de santé des armées ;

  4° Un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du Code de l'action sociale et des familles. ».

Dès lors, tous les téléservices ou téléprocédures qui traiteront des documents entrant dans ce périmètre (très large) seront soumis aux articles L. 1111-25 à L. 1111-29 du Code de la santé publique et par voie de conséquence, aux règles fixant la force probante desdits documents.

L'article L. 1111-26 du Code de la santé publique détermine le régime juridique de la copie numérique. Cette disposition renvoie aux conditions de fiabilité de la copie numérique posées au deuxième alinéa de l'article 1379 du Code civil.

Dès lors que ces conditions sont remplies, la copie numérique a la même force probante que le document original sur support papier.

De plus, la destruction de l'original est possible si une copie numérique fiable a été réalisée, selon les délais et formes définis (alinéa 2 et 3 de l'article L. 1111-26 du Code de la santé publique).

L'article L. 1111-27 du Code de la santé publique traite des documents créés sous forme numérique. Il pose le principe que ledit document « *a la même force probante qu'un document sur support papier lorsqu'il a été établi et conservé dans les conditions prévues à l'article 1366 du Code civil.* ».

L'article L. 1111-28 du Code de la santé publique détermine les principes relatifs à la signature électronique. D'abord, il précise les fonctionnalités de la signature apposée sur les documents concernés. Ainsi, lorsqu'elle est apposée par le patient (personne prise en charge), la signature signifie qu'il a pris connaissance du contenu de l'acte et, le cas échéant y consent. Alors que lorsque la signature est apposée par le professionnel, elle signifie que ce dernier valide le contenu du document électronique.

Le texte ajoute : « *Lorsque le document sur lequel la signature est apposée est créé sur un support numérique, le procédé de signature respecte les conditions du second alinéa de l'article 1367 du Code civil*. »

Il s'ensuit qu'un même procédé de signature électronique va emporter des effets juridiques différents selon la qualité de son utilisateur (signataire). Mais dans tous les cas, la signature consistera (techniquement) « *en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* ».

L'article L. 1131 du Code de santé publique renvoie à cet égard aux référentiels définis en matière médico-sociale par l'Agence nationale des systèmes d'information partagés de santé (ASIP).

L'article L. 1111-29 du Code de la santé publique définit les conditions et modalités selon lesquelles un « *formulaire* » électronique peut être rempli « *à partir d'un ou plusieurs documents numériques existants sans en modifier le sens et le contenu, et dans le respect du secret médical et de la confidentialité des données collectées et traitée* ». Il est précisé :

« *Le document ainsi créé est présumé fiable jusqu'à preuve du contraire lorsqu'a été utilisé un procédé de production permettant d'insérer les métadonnées nécessaires à la garantie de l'identification de l'émetteur et de l'intégrité des données ainsi matérialisées. Le document créé peut être matérialisé sur support papier.*

Lorsque le document ainsi créé fait l'objet d'une obligation légale de signature, celle-ci est réputée satisfaite si le document respecte les conditions du précédent alinéa et s'il est issu d'un ou plusieurs documents signés de façon électronique conformément aux dispositions du dernier alinéa de l'article L. 1111-28 ».

En définitive, ces dispositions encadrent la création des documents électroniques en matière médico-sociale, de telle sorte que le droit reconnaisse leur force probante. Compte tenu des conditions posées, les prestataires de service de confiance y ont toute leur place.

9. La dématérialisation des procédures contentieuses en droit administratif

Le droit administratif a fait de la voie électronique le principe pour les procédures contentieuses. Ce principe a été introduit dans le Code de justice administrative par le décret n° 2012-1437 du 21 décembre 2012 (400) récemment modifié par le décret n° 2020-1245 du 9 octobre 2020 (401).

Les nouvelles dispositions sont entrées en application le 1er janvier 2021. Le régime juridique applicable aux téléprocédures en matière de contentieux administratif repose désormais sur les versions actualisées des articles R. 414-1 à R. 414-7 du Code de justice administrative.

En application de l'article R. 414-1 du Code de justice administrative, l'utilisation obligatoire de la téléprocédure mise en place pour déposer les requêtes, les mémoires et les appels s'impose aux avocats, aux avocats au Conseil d'État et à la Cour de cassation, aux personnes morales de droit public et aux organismes de droit privé chargé de la gestion permanente d'un service public. Seules les communes de moins de 3 500 habitants et les personnes physiques ou morales de droit privé autres que celles chargées de la gestion permanente d'un service public ne sont pas tenues d'utiliser la voie électronique, sous réserve que le ministère d'avocat ne soit pas obligatoire bien évidemment.

La possibilité de recourir à un téléservice dédié leur est toutefois ouverte ; étant précisé que c'est la seule voie électronique recevable le cas échéant (article R. 414-2 du Code de justice administrative).

Tout en distinguant la téléprocédure de l'article R. 414-1 du Code de justice administrative du téléservice visé à l'article R. 414-2 du Code de justice administrative, l'article R. 414-3 du Code de justice administrative indique que leurs caractéristiques techniques doivent garantir « *la fiabilité de l'identification des parties ou de leur mandataire, l'intégrité des documents adressés ainsi que la sécurité et la confidentialité des échanges entre les parties et la juridiction* ».

(400) Décret n° 2012-1437 du 21 décembre 2012 relatif à la communication électronique devant le Conseil d'État, les cours administratives d'appel et les tribunaux administratifs, J.O. du 23 décembre 2012.

(401) Décret n°2020-1245 du 9 octobre 2020 relatif à l'utilisation des téléprocédures devant le Conseil d'État, les cours administratives d'appel et les tribunaux administratifs et portant autres dispositions, J.O. du 11 octobre 2020.

La date et l'heure de la mise à disposition d'un document et de sa première consultation par le destinataire doivent également être établies de manière certaine. Un arrêté d'application est prévu.

À défaut de texte plus récent, l'arrêté du 2 mai 2018 relatif aux caractéristiques techniques de l'application mentionnée à l'article R. 414-1 du Code de justice administrative [402] reste applicable. La téléprocédure « *Télérecours* » est notamment décrite en ce qui concerne les fonctionnalités offertes, les obligations à respecter, les garanties apportées, et les droits et effets juridiques reconnus. Ainsi, l'application informatique « *Télérecours* » permet aux avocats et aux administrations de transmettre à une juridiction administrative toutes leurs productions et de recevoir de la juridiction tous les actes de procédure.

Afin d'en faciliter l'usage et d'en généraliser l'utilisation, le Conseil d'État et le Conseil national des barreaux ont signé une convention concernant l'utilisation de la communication électronique devant les juridictions administratives [403].

Dans ce cadre, le Conseil d'État s'engage notamment à permettre l'inscription des avocats dans l'application « *Télérecours* », leur authentification à chacune de leur connexion ainsi que la signature électronique de leurs productions par l'intermédiaire du certificat électronique utilisé pour accéder au « *réseau privé virtuel des avocats* » (RPVA).

Les avocats peuvent également se connecter à l'application par l'intermédiaire de leur connexion au RPVA. On constate donc une centralisation des moyens de communication électronique utilisés dans le cadre de procédures judiciaires et administratives et une volonté des juridictions et ordres professionnels à encourager une telle digitalisation [404].

(402) J.O. du 6 mai 2018.

(403) Convention du 5 juin 2013 conclue entre le Conseil d'état et le Conseil national des barreaux concernant l'utilisation de la communication électronique devant les juridictions administratives. Cette convention prise sur la base de l'arrêté du 12 mars 2013 demeure applicable faute de nouvelle convention adoptée.

(404) E. Caprioli et I. Choukri, De la dématérialisation des contentieux au contentieux de la dématérialisation : état des lieux des procédures sur Télérecours, JCP éd. A et CT, n°7, 22 février 2016, p. 30 à 34.

En ce qui concerne les modalités de la transmission de documents par voie électronique pour les personnes visées à l'article R. 441-2 du Code de justice administrative, ce sont les dispositions de l'arrêté du 2 mai 2018 relatif aux caractéristiques techniques du téléservice mentionné à l'article R. 414-6 du Code de justice administrative[405] qui demeurent applicables, faute d'arrêté plus récent.

Ce texte détermine ainsi les modalités du téléservice « *Télérecours citoyens* » mises en œuvre pour garantir l'identification des utilisateurs, l'intégrité des documents ainsi que l'exactitude des dates et heures apposées dans le cadre de ce téléservice, en ce, y compris pour les accusés d'enregistrement et de réception et les opérations de consultation.

On relèvera également que l'article R. 414-4 du Code de justice administrative dispose : « *L'identification de l'auteur de la requête, selon les modalités prévues par l'arrêté mentionné à l'article R. 414-3, vaut signature pour l'application des dispositions du présent code* » et que l'article R. 414-7 du Code de justice administrative prévoit : « *L'arrivée de la requête et des différents mémoires est certifiée par l'accusé de réception délivré par voie électronique* ».

Même si des dérogations et procédures particulières existent, il ressort de ces textes que la justice administrative a fait des échanges par voie électronique le principe. La mise en œuvre de cette dématérialisation nécessite des garanties fortes qui ne sont pas étrangères aux prestataires de service de confiance.

(405) J.O. du 6 mai 2018.

NOTES

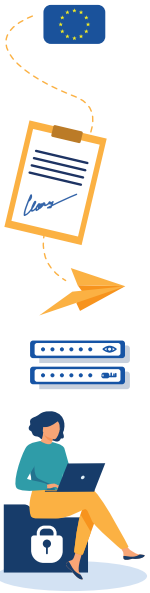
Cet espace vous est dédié pour prendre des notes.

Sommaire

fntc

LE RÈGLEMENT EUROPÉEN SUR L'IDENTIFICATION ET LES SERVICES DE CONFIANCE

La Commission européenne a organisé plusieurs consultations dans le but de réviser la directive n° 1999/93/CE portant sur un cadre communautaire pour les signatures électroniques du 13 décembre 1999 (406) et en vue de la préparation d'une initiative concernant la reconnaissance mutuelle des procédés d'identification et d'authentification électroniques. L'objectif était de contribuer à la confiance sur le marché en développant les signatures électroniques, encore trop peu utilisées dans les États membres, selon la Commission européenne.



Suite à ces consultations, le 4 juin 2012, la Commission européenne a présenté une Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (407) composée essentiellement des deux parties identifiées par son titre. Ce projet de règlement a été adopté le 23 juillet 2014 et publié le 28 août 2014 (408).

Selon les termes de son article 1er, ce règlement :

+ « *fixe les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre,*

(406) J.O.U.E n° L. 13 du 19 janvier 2000, p. 12.

(407) PE et Cons. UE, prop. de règl. COM(2012) 238 : http://ec.europa.eu. - V. notamment Th. Piette Coudol, Une législation européenne pour la signature électronique : RLDI juill. 2012, n° 2838 ; É. A. Caprioli et P. Agosti, La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance, Comm. Com. Electr. n°2, février 2013, étude 3.

(408) Règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, J.O.UE L.257 du 28 août 2014 p.73 s., disponible sous le lien : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.FRA

établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques et instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, d'envoi recommandé électronique et les services de certificats pour l'authentification de sites Web. ».

Le règlement eIDAS, d'application directe, ne nécessite par principe, pas de texte de transposition en droit national à la différence d'une directive (409). Un certain nombre de marges de manœuvre est cependant prévu par le texte (410).

En France, le règlement eIDAS a conduit le législateur à procéder à une mise à niveau des textes en matière d'identification électronique et de services de confiance et non à une transposition stricto sensu comme cela est le cas en Belgique par exemple.

En effet, nous disposions déjà de textes adéquats tels que la loi du 13 mars 2000 en matière de signature électronique dont les articles créés ont été modifiés et renumérotés dans le Code civil par l'ordonnance du 10 février 2016 (411).

(409) Article 288 du Traité sur le fonctionnement de l'Union européenne modifié, J.O. C326, 26 octobre 2012.

(410) V. Pour aller plus loin sur ce point : D. Gobert, Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie, juin 2015, dossier publié sur le site www.caprioli-avocats.com.

(411) Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations J.O. 18 juin 2019.

A. Identification électronique

Le régime juridique de l'identification électronique [412] **passe par la reconnaissance et l'acceptation mutuelles des moyens d'identification électronique délivrés par un Etat membre par le biais de règles de notification des schémas d'identification à la Commission.**

Dans le cadre de ce règlement, l'identification électronique est distincte des services de confiance et renvoie à des règles spécifiques. L'identification électronique, telle qu'elle est traitée au sein du règlement, ne porte pas sur les services d'identification entre personne privée, sauf si l'État en a décidé autrement, mais sur **une identification effectuée par la puissance publique (ou par un fournisseur de service qu'elle a reconnu**).

En effet, il s'agit d'assurer la reconnaissance mutuelle des moyens d'identification électroniques délivrés dans un État membre (soit par l'État membre, soit dans le cadre d'un mandat de l'État membre, ou soit indépendamment de l'État membre mais reconnu par lui [413]) afin d'accéder à un service en ligne fourni par un organisme du secteur public dans un État membre.

Pour ce faire, l'article 6 fixe plusieurs conditions impératives que sont :

+ *« La délivrance de ce moyen d'identification électronique relève d'un schéma d'identification électronique qui figure sur la liste publiée par la Commission en application de l'article 9 ;*

+ *Le niveau de garantie de ce moyen d'identification électronique correspond à un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne dans le premier État membre, à condition que le niveau de garantie de ce moyen d'identification électronique corresponde au niveau de garantie substantiel ou élevé ;*

+ *L'organisme du secteur public concerné utilise le niveau de garantie substantiel ou élevé pour ce qui concerne l'accès à ce service en ligne.* ».

La reconnaissance mutuelle s'appuie sur un **processus de notification du schéma d'identification électronique dans son ensemble, en ce y compris son régime de contrôle et ses niveaux de garantie, à destination de la Commission** à charge pour elle, après étude de ces notifications, d'en **publier la liste afin que chaque État membre puisse s'assurer que le moyen d'authentification qui lui a été soumis a bien fait l'objet d'une notification et d'une acceptation par la Commission.**

(412) E. Caprioli, I. Cantero, I. Choukri et P. Agosti, L'identité numérique dans le droit et la pratique, éd. Revue Banque, Collect. Les essentiels, 2021.

(413) Article 7 a) du règlement eIDAS.

De plus, la reconnaissance repose également sur **la responsabilité** de l'État membre notifiant. De manière générale, celui-ci doit être vigilant sur la fiabilité du schéma car celui-ci est responsable des dommages causés intentionnellement ou par négligence à toute personne physique ou morale dans une transaction transnationale en raison d'un manquement à certaines obligations qui lui incombent.

Techniquement, l'État membre doit suspendre ou révoquer l'authentification en cas d'atteinte ou d'altération partielle du schéma d'identification électronique notifié et, s'il n'est pas remédié à l'atteinte dans un délai de trois mois à compter de la suspension ou de la révocation, de notifier le retrait du schéma d'identification électronique aux autres États membres et à la Commission.

Enfin, le système repose **sur la coopération et l'interopérabilité des systèmes**, le règlement établissant les lignes directrices de cette interopérabilité (principes, documents de référence, thématiques, actions) et laissant à la Commission le soin d'arrêter au moyen d'actes d'exécution les modalités de procédure nécessaires.

En outre, divers actes d'exécution sont venus préciser les modalités propres à l'identification électronique :

+ Les modalités de collaboration entre Etats membres en matière d'identification électronique (art. 12-7, Règlement eIDAS) [414] ;
+ Les Spécifications techniques minimums et procédures pour les niveaux d'assurance pour l'identification électronique (art. 8-3, Règlement eIDAS) [415] ;
+ Le cadre d'interopérabilité (art. 12-8, Règlement eIDAS) [416].

Notons qu'à présent que les actes d'exécution ont été publiés, ces textes ont été complétés par divers documents d'ordre technique :

+ eIDAS - Cryptographic requirements for the Interoperability Framework TLS and SAML, V.1.0 du 6 novembre 2015 ;
+ eIDAS Message Format, V.1.2 ;
+ eIDAS SAML Attribute profile V.1.2 ;
+ eIDAS – Interoperability Architecture V.1.2 du 31 août 2019.

La stratégie française en matière d'identification électronique s'articule autour de France Connect qui est ouvert tant aux téléservices publics que privés [417].

(414) Décision d'exécution n°2015/296 du 24 février 2015 de la Commission établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, § 7, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE L. 53 du 25 février 2015, p. 14 et s.

(415) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique (…), J.O.UE L. 235 du 9 septembre 2015, p. 7 et s.

(416) Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité (…), JOUE L. 235 du 9 septembre 2015, p. 1.

(417) Voir supra partie II.C.2.a) relative à France Connect.

En outre, la reconnaissance mutuelle des moyens d'identification pour un téléservice donné est applicable depuis le mois de septembre 2018.

À ce titre, la France dispose d'un schéma eID notifié au niveau substantiel « *France Connect* + » / Identité numérique de La Poste [418].

La nécessité d'assurer la reconnaissance transfrontière d'un système d'identité numérique dans tous les États membres ne peut être atteinte par des initiatives propres des États membres, dont la portée, l'ambition, l'architecture technique, les solutions retenues et les dispositions juridiques varient, y compris les questions de responsabilité et la disponibilité de l'utilisation par le secteur privé.

Les solutions individuelles conduiraient à la fragmentation du marché unique et encourageraient le forum shopping pour les prestataires de services de confiance, conduisant à une offre inégale au détriment des opportunités commerciales, de l'offre de services et de l'expérience utilisateur.

Si le recours à l'identification électronique régalienne au sens du Règlement eIDAS semble réservé aux services en ligne fournis par des organismes du secteur public, le Règlement eIDAS laisse une opportunité ouverte à chaque Etat membre pour que ces moyens d'identification électronique soient également utilisés dans le secteur privé comme ce fut le cas pour le SPID en Italie (qui regroupe tant des acteurs publics que privés).

La France a décidé d'intégrer cette possibilité dans le cadre législatif [419].

(418) Les schémas notifiés et prénotifiés figurent à l'adresse suivante : HYPERLINK «https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS» Overview of pre-notified and notified eID schemes under eIDAS - eID User Community - (europa.eu).

(419) : E Caprioli et P. Agosti, HYPERLINK «https://www.usine-digitale.fr/article/revision-du-reglement-eidas-et-identite-numerique.N1116709» Révision du Règlement eIDAS et identité numérique (usine-digitale.fr), 1er juillet 2021.

LE RÈGLEMENT EUROPÉEN SUR L'IDENTIFICATION ET LES SERVICES DE CONFIANCE

La loi pour une République numérique [420] a ouvert au niveau national l'identification électronique au secteur privé et créé une alternative à France Connect.

L'ANSSI doit établir, à la suite d'un audit, que le moyen d'identification utilisé est fiable. L'article L. 102 du Code des Postes et des Communications Electroniques [421] dispose que :

1. « *L'identification électronique est un processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale.*
2. *Un moyen d'identification électronique est un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne.*
3. *La preuve de l'identité aux fins d'accéder à un service de communication au public en ligne peut être apportée par un moyen d'identification électronique.*
4. *Ce moyen d'identification électronique est présumé fiable jusqu'à preuve du contraire lorsqu'il répond aux prescriptions du cahier des charges établi par l'autorité nationale de sécurité des systèmes d'information, fixé par décret en Conseil d'État*. »

   Cette autorité certifie la conformité des moyens d'identification électronique aux exigences de ce cahier des charges.
5. *Le prestataire fournissant un moyen d'identification électronique autre que celui mentionné au III et qui en fait la demande peut se voir délivrer par l'autorité nationale de sécurité des systèmes d'information une certification attestant du niveau de garantie associé à ce moyen d'identification électronique.*

   L'autorité nationale de sécurité des systèmes d'information établit à cette fin, après avis de la Commission nationale de l'informatique et des libertés, les référentiels définissant les exigences de sécurité associées au moyen d'identification électronique. Ces exigences précisent notamment les critères retenus pour la délivrance du moyen d'identification électronique, pour la gestion de ce moyen, pour l'authentification, ainsi que pour la gestion et l'organisation des prestataires. Ces référentiels sont mis à disposition du public par voie électronique.

   Les modalités de cette certification sont définies par décret en Conseil d'État ».

(420) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, J.O. du 8 octobre 2016.

(421) Issu de la numérotation modifiée par l'ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques, J.O. du 5 octobre 2017 du CPCE.

Le Décret n° 2022-1004 du 15 juillet 2022 fixe le contenu de ce cahier des charges, le niveau de fiabilité exigé du moyen d'identification électronique aux fins de bénéficier de la présomption de fiabilité, ainsi que les modalités de la certification des moyens d'identification électronique mentionnée à l'article précité.

L'art. R.51-1 du CPCE traite des **définitions et présentation des principes de la certification**, en distinguant utilisateur, demandeur et fournisseur.

L'art. R. 54-2 du CPCE est particulièrement important en ce qu'il renvoie à un **référentiel d'exigences** pour les moyens d'identification électronique publié sur le site de l'ANSSI, le 11 août 2022.

Les art. R. 54-3 et s. du CPCE renvoient aux **modalités de la procédure de certification**.

La Section 3 pose le contenu du Cahier des charges. Ainsi, l'art. R. 54-16 du CPCE précise que le moyen d'identification électronique présumé fiable respecte a minima **les conditions, les spécifications techniques et les procédures minimales du niveau de garantie « élevé »** définies par le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique mentionnés à l'article 8, paragraphe 3 du Règlement eIDAS.

En outre, conformément à l'art. R. 54-17 du CPCE, « *le fournisseur du moyen d'identification électronique est chargé de vérifier l'identité déclarée par le demandeur avec les informations provenant d'une source faisant autorité* ». L'art. R. 54-18 du CPCE précise **les six données à caractère personnel pouvant être collectées pour un moyen d'identification électronique, comme l'identité pivot prévue dans les jetons d'identité figurant dans le cadre de France Connect**. Les traitements de données à caractère personnel doivent être conformes au RGPD.

Les art. R. 54-20 et s. du CPCE traitent des **exceptions à la vérification d'identité des demandeurs.**

Les art. R. 54-23 et s. du CPCE renvoient vers les modalités de gestion de la confidentialité par le biais de processus cryptographiques.

Enfin, **un Comité de suivi de la certification** est instauré afin de :

+ Présenter une synthèse des usages de ces moyens d'identification électronique ;
+ Apprécier les risques pesant sur ces moyens ;
+ Anticiper le renouvellement éventuel de la certification de ces moyens.

LE RÈGLEMENT EUROPÉEN SUR L'IDENTIFICATION ET LES SERVICES DE CONFIANCE

Dans le cadre du Décret n°2022-676 du 26 avril 2022 [422], le Service de garantie de l'identité numérique (SGIN) entend proposer aux détenteurs d'un équipement terminal de communications électroniques (téléphone portable) doté d'un dispositif de lecture sans contact, une application mobile visant à permettre une identification et une authentification électroniques. À cet effet, le Décret autorise le traitement à lire les données enregistrées dans le composant électronique des cartes nationales d'identité, à l'exception de l'image numérisée des empreintes digitales.

La création du moyen d'identification électronique et son utilisation relèvent de l'unique volonté des usagers.

Le moyen d'identification électronique peut être utilisé par les usagers pour l'accès à des services en ligne proposés par des fournisseurs liés par convention à FranceConnect.

Le Décret définit enfin les finalités du traitement, la nature et la durée de conservation des données enregistrées ainsi que les catégories de personnes ayant accès à ces données ou en étant destinataires. Il précise les modalités d'exercice des droits des personnes concernées.

Le cadre réglementaire et technique est donc complet en matière d'identification électronique.

À ce jour, dix-huit États membres ont d'ores et déjà notifié leur schéma d'identification à la Commission européenne [423], dont la France.

(422) J.O. du 27 avril 2022.

(423) Schémas d'identification électronique notifiés conformément à l'article 9, paragraphe 1, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur : accessible à l'adresse file :https://op.europa.eu/fr/publication-detail/-/publication/ccf123b5-5994-11ec-91ac-01aa75ed71a1/language-fr

Ainsi, FranceConnect mis en place par la Direction du numérique constitue le « *noeud eIDAS* » comme indiqué à l'article 2, 4° de l'arrêté du 8 novembre 2018 (J.O. du 15 novembre 2018) et l'Identité numérique de la Poste (niveau substantiel) est le seul moyen d'identification couplé à France Connect + qui a été notifié par la France dans le cadre du schéma d'identification à la Commission européenne à la date de rédaction du présent Vade-Mecum.

En dehors du schéma de notification de moyens d'identification prévu par le règlement eIDAS, plusieurs moyens d'identification électroniques sont proposés. Ainsi, l'ANSSI a certifié au niveau national d'autres moyens d'identification électronique conformément aux pouvoirs qui lui ont été reconnus.

B. Les Prestataires de services de confiance (PSCo)

Le régime juridique des prestataires de services de confiance (PSCo) prévoit les principes relatifs à leur responsabilité mais également les mécanismes relatifs à leur qualification et à leur contrôle par les États membres.

Le règlement dispose, en effet, que les prestataires sont **responsables des dommages causés intentionnellement ou par négligence en raison d'un manquement à leurs obligations** (art. 13).

Cela étant, lorsque les prestataires informent leurs clients au préalable des limites qui existent à l'utilisation de leurs services et que ces limites peuvent être connues des tiers, les prestataires ne peuvent être tenus responsables des dommages découlant de l'utilisation des services au-delà des limites indiquées.

À cette responsabilité s'ajoute une **obligation relative à la mise en œuvre de mesures de sécurité**, le niveau de sécurité devant être proportionné au degré de risque, une **obligation de notification de toute atteinte à la sécurité ou toute perte d'intégrité (art. 19) ayant une incidence importante sur le service de confiance ou les données personnelles.**

LE RÈGLEMENT EUROPÉEN SUR L'IDENTIFICATION ET LES SERVICES ...

Le règlement établit également **les mécanismes de surveillance de l'application de ces règles prévoyant les organes de contrôle nécessaires** (et leur assistance mutuelle) (art. 17 et 18) ainsi que **la fixation par les États membres d'un régime de sanction (art. 16).**

Le règlement institue **l'équivalence sur le plan juridique des services de confiance fournis par des prestataires établis dans un pays tiers par le biais d'accords conclus entre l'Union et le pays tiers concerné (art. 14).** Enfin, le règlement prévoit un **corps de règles relatives à la mise en œuvre d'un service de confiance qualifié** allant de son lancement (art. 21) et des exigences applicables à son contrôle en passant par la mise en œuvre **d'une liste de confiance (art. 22) et d'un label de confiance de l'Union européenne (art. 23).**

Les modalités d'attribution de ce label figurent au Règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés [424].

La *European Trusted List* (EUTL) est une liste de prestataires de services de confiance qui fournissent les plus hauts niveaux de conformité au règlement eIDAS. Le recours à un tel prestataire est un gain de sécurité juridique et technique indéniable.

Des évaluations des services de confiance (envois recommandés, certificats, cachets électroniques, horodatage...) sont menées par l'ANSSI. Cette dernière a la charge de contrôler le respect des exigences du règlement par les prestataires de service de confiance qualifiés et la conformité des services de confiance qualifiés qu'ils fournissent.

Les critères d'évaluation de la conformité aux exigences du règlement pour un service de confiance donné sont décrits sur son site Internet en complément des exigences portant sur le Prestataire lui-même (qui doit également être qualifié [425]).

(424) J.O.UE L 128 du 23 mai 2015, p.13 et s.

(425) Référentiels d'exigences applicables à la qualification des prestataires de services de confiance https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi

C. Les services de confiance

Le règlement introduit des régimes applicables aux différents services de confiance (art. 35 et suivants) dont la signature électronique et des nouveaux services tels que les cachets électroniques, l'horodatage électronique, les services d'envoi de recommandés électronique, l'authentification de site internet et les documents électroniques.

1. Signature électronique

Le régime de la signature électronique a été révisé avec des règles relatives à l'effet juridique des signatures électroniques et des signatures électroniques qualifiées.

Prenant acte des difficultés soulevées par le rapport sur la mise en œuvre de la directive 1999/93/CE [(426)] notamment quant au déploiement de la signature électronique, le règlement a pour élément central la révision du régime juridique de la signature électronique.

Trois niveaux de sécurité de la signature coexistent : la signature électronique simple, la signature électronique avancée et la signature électronique qualifiée.

Elles sont toutes juridiquement reconnues, mais pour les deux premiers niveaux, celui qui s'en prévaut devra rapporter la preuve de la fiabilité du procédé, contrairement à la troisième catégorie de signature.

À ce titre, le règlement introduit la notion de *« signature électronique qualifiée »* (SEQ), notion qui préexistait dans le cadre de la directive mais qui n'était pas dénommée de façon explicite. Il en fait l'essentiel de ses dispositions et il institue **la signature électronique qualifiée comme fondement juridique et technique de l'interopérabilité dans le marché européen de la confiance** [(427)].

En effet, si le règlement fixe les effets de la signature électronique de manière générale, affirmant que *« L'efficacité juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée »* (art. 25-1), seule la signature électronique qualifiée est dotée d'un effet juridique *« équivalent à celui d'une signature manuscrite »* (art. 25-2).

(426) Rapport de la Commission au Parlement européen et au Conseil - Rapport sur la mise en œuvre de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques / COM/2006/0120 final disponible sous le lien : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52006DC0120.*

(427) É. A. Caprioli et P. Agosti, La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance : Comm. Com. Electr. n°2., février 2013, étude 3. P. Agosti, Commerce électronique, la confiance électronique, entre droit et technique, Expertises, Décembre 2014, p.416 et s. T. Douville, Identification électronique et services de confiance : les apports du règlement européen eIDAS, JCP E., 2017, 1005.

En réalité, cette SEQ bénéficie d'une présomption simple de fiabilité, comme c'est le cas actuellement et dans le cadre de l'ordonnance du 10 février 2016, en droit français (art. 1367 du Code civil).

La signature électronique avancée connaît un changement important (article 26, c)) étant donné que l'exigence est d' *« avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé,* ***utiliser sous son contrôle exclusif.*** » Cette modification a pour but de consacrer la gestion centralisée des certificats (et des clés privées/données de création) comme les solutions de signature électronique fondées sur des certificats à la volée (ou à usage unique) à côté des données de création de signature figurant sur un support matériel (exemple : clé USB, carte).

De plus, le règlement définit à l'article 3-12 la signature électronique qualifiée comme *« une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique. ».*

Pour l'heure, la Décision d'exécution n°2016-650 du 25 avril 2016 est venue indiquer les normes applicables pour les dispositifs de création de signature électronique qualifié *« lorsque les données de création de signature électronique ou de cachet électronique sont conservées dans un environnement dont l'utilisateur a la gestion totale, mais pas nécessairement exclusive »* [(428)].

Cette définition reprend, à s'y méprendre, l'article 2 du décret du 30 mars 2001 qui attache à ces trois éléments la présomption de fiabilité. En ce sens, on peut considérer que cette signature qualifiée bénéficiera d'une présomption de fiabilité, alors que la charge de la preuve de cette fiabilité avec les autres signatures électroniques (simples et avancées) reposera sur la partie qui s'en prévaut.

Enfin, le règlement complète le dispositif introduit par la directive en incluant les services de validation (art. 33) et de conservation de la signature électronique qualifiée (art. 34).

(428) D'autres actes d'exécution sont donc à prévoir au sujet des dispositifs de création de signature électronique qualifié. Décision n°2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement eiDAS.

Il est à noter qu'une Décision d'exécution n°2015/1506 de la Commission du 8 septembre 2015 établit les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés **devant être reconnus par les organismes du secteur public** visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur [429].

Le décret du 28 septembre 2017 [430] précise les caractéristiques techniques du procédé permettant de présumer la fiabilité d'une signature électronique, toujours au moyen d'un certificat. Le texte reprend l'article 2 du décret du 30 mars 2001 (abrogé) ainsi que la définition du règlement européen pour le bénéfice de la présomption de fiabilité du procédé de signature (*réfragable*).

Les normes applicables évoluent ; elles concernent donc la signature électronique avancée (SEA) (art. 26 du règlement eIDAS), le dispositif de création de signature électronique qualifiée (art. 29 du règlement eIDAS) et le certificat qualifié (art. 28 du règlement eIDAS). C'est cette signature électronique qualifiée (SEQ) qui donne le bénéfice de la présomption ; ce qui implique un renversement de la charge de la preuve et non la remise en cause de la validité ou de la preuve de la signature en cause.

2. Le cachet électronique

Il est défini comme étant *« des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données électroniques pour garantir l'origine et l'intégrité des données associées »* (art. 3-25). Il est important de noter que cette définition se rapproche de la définition de signature électronique et que le règlement lui associe un régime qui se rapproche également de celui de la signature électronique dans ses premiers articles.

De fait, si le règlement associe la signature électronique aux personnes physiques et à leur manifestation de consentement (cette dernière fonction n'est pas explicitement énoncée), le cachet électronique est associé aux personnes morales, le considérant 59 du règlement précisant que *« Les cachets électroniques devraient servir à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document. »*

(429) J.O.UE L. 235 du 9 septembre 2015, p. 37 et s.

(430) Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, J.O. 30 septembre 2017.

Le cachet électronique qualifié bénéficie d'une présomption de fiabilité (intégrité et exactitude de l'origine des données) contrairement au cachet électronique simple ou plus exactement qui n'est pas qualifié dont l'effet juridique et la recevabilité ne peuvent être refusés en raison de son caractère électronique ou qu'il ne répond pas aux exigences du cachet électronique qualifié. Des dispositions particulières sont prévues pour les signatures électroniques et pour les cachets électroniques dans les services publics (articles 27, 37) [431].

3. Horodatage électronique et service d'envoi recommandé électronique

Ces deux services, mentionnés aux article 41 et 43, sont traités sous l'angle de l'effet juridique et des exigences applicables, l'ensemble instituant la recevabilité de ces éléments en justice et les présomptions qui s'y rattachent lorsque ces services ont fait l'objet d'une qualification conformément aux textes et normes de référence.

4. Authentification de site Web

Ce service figure à l'article 45 du règlement. Il fait l'objet d'une brève mention qui renvoie à l'annexe IV fixant les Exigences applicables aux certificats qualifiés d'authentification de site internet et aux actes d'exécution pris par la Commission pour déterminer les normes applicables.

En matière bancaire, la question de l'authentification est double. Il ne faudra pas confondre l'authentification de sites Internet, qui concerne les « *Third Party Providers* » ou TPP qui dépend du règlement eIDAS et l'authentification forte des clients (PSP) qui dépend de la DSP2 [432] et donc des standards techniques précités [433].

(431) T. Piette-Coudol, Règlement européen n°010/2014 : le renouveau de la signature électronique et la consécration du cachet électronique, RLDI, Février 2015, p.43-45. T. Douville, La signature électronique après le règlement 910/2014 eIDAS, D. 2016, p. 2124.

(432) Directive (UE) 2015/2366 du parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE, J.O.UE L. 337/35 du 23 décembre 2015 transposée et codifiée dans le Code monétaire et financier par l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, J.O. 12 janvier 2018.

(433) Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication J.O.UE 13 mars 2018, L. 69/23.

En pratique cette analyse nécessite une articulation judicieuse sur les plans techniques et juridiques. Les prestataires de service de paiement devront mettre à profit les éléments mis en place pour être conformes à eIDAS de façon à remplir les conditions élaborées par la DSP2, et inversement.

L'articulation de ces deux textes est fondamentale pour garantir un service conforme aux exigences qu'ils fixent.

5. Documents électroniques

Le sujet est traité à l'article 46. Les documents électroniques bénéficient du principe de non-discrimination à leur égard. Cela permet de leur conférer des effets probatoires et d'éviter une irrecevabilité de principe au seul motif qu'ils ont été établis sous forme électronique.

D. Quelles perspectives avec la proposition eIDAS 2 ?

Une proposition de modification du règlement eIDAS, émanant de la Commission européenne en date du 3 juin 2021 [434] a précisé les principales pistes d'amélioration soumises aux États membres pour discussion et adoption.

(434) Disponible à l'adresse : P1_e15907.pdf (senat.fr).

LE RÈGLEMENT EUROPÉEN SUR L'IDENTIFICATION ET LES SERVICES...

De façon synthétique, on peut dire que cette proposition emprunte quatre directions :

+ La généralisation de l'identité numérique avec une innovation phare : le portefeuille d'identité (*wallet*), qui est envisagé dans sa multiplicité de supports et de sources (publiques et privées). Cela devrait faciliter l'utilisation des signatures et cachets qualifiés. Ces portefeuilles pourront bénéficier d'un label de confiance dès lors qu'ils répondent aux exigences. Il convient de noter l'introduction de la notion d'attribut ou rôle/qualité associé à une personne.

+ Les services qualifiés de signatures et de cachets électroniques activés à distance (*remote*).

+ La création d'un nouveau service de confiance : l'archivage électronique à l'instar de ce qui existe au niveau national, en Belgique, au Luxembourg pour l'UE ou encore en Principauté de Monaco. Ce service pourra être qualifié comme les autres services de confiance existants.

+ Les services de registre électronique (Ledger) sont considérés comme permettant des enregistrements inviolables des données qu'ils contiennent. Ils assurent l'authenticité et l'intégrité des données, tout en garantissant l'exactitude de leur date (horodatage) et de leur ordre chronologique d'enregistrement dans ledit registre. Les registres qualifiés seront présumés fiables, sous réserve d'avoir recours à un PSCo qualifié, ce qui semble a priori exclure les *blockchains* publiques. Ces dernières ne pourront pas non plus utiliser des signatures électroniques qualifiées.

Le 1er avril 2022, un texte de compromis de la présidence du Conseil de l'Union européenne est venu modifier le projet initial en prévoyant notamment une clause sur la responsabilité des Prestataires de services de confiance non qualifiés, en précisant certains points sur les moyens d'identification électronique, en modifiant la définition d'archivage électronique et en précisant ses effets juridiques...

Cette proposition devrait aboutir à un texte définitif en 2023. Mais d'autres textes modificatifs interviennent au gré des présidences de l'UE.

NOTES

Cet espace vous est dédié pour prendre des notes.

Sommaire

fntc

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (435)

IV

Avant l'entrée en vigueur le 25 mai 2018 du Règlement (UE) 2016/679 du 27 avril 2016 (ci-après le « RGPD ») (436), la réglementation française sur la protection des données à caractère personnel comportait des dispositions *sui generis* ayant vocation à s'appliquer aux prestataires de services de certification électronique (PSCE) (437). Ainsi, ces prestataires particuliers étaient expressément visés par l'article 33 (438) de la loi n° 78-17 du 6 janvier 1978 (ci-après « *Loi Informatique et Libertés* »), dans sa version en vigueur du 07 août 2004 au 1er juin 2019 (439) reprenant l'article 8 de la Directive 1999/93/CE du 13 décembre 1999 (440).

Un prestataire de services de certification électronique se définissait alors comme *« toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique »* (441).

L'article 33 de la loi n°78-17 imposait 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 était précisé que les données ne pouvaient être traitées *« que pour les fins en vue desquelles elles ont été recueillies »*, c'est-à-dire la délivrance et la conservation des certificats liés aux signatures électroniques.

(435) I. Cantero et E. Caprioli, Services de confiance et données à caractère personnel : implications multiples à venir pour le délégué à la protection des données, in AFCDP, Correspondant Informatique et Libertés : Bien plus qu'un métier, 2015, (disponible en ligne : www.afcdp.net), v. p.153 et s.

(436) Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données).

(437) Article 1-11 du décret 2001-272 du 30 mars 2001 (issu 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 ».

(438) 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. »

(439) Loi N°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(440) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

(441) 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.

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

En raison notamment de la surexploitation des données à caractère personnel, qualifiées d'*« or noir »* pour le développement du commerce électronique et plus généralement de l'ère numérique, le cadre juridique défini par la Directive européenne de 95/46/CE du 24 octobre 1995 s'est avéré très insuffisant.

Dans ce contexte, la Commission européenne a publié le 25 janvier 2012 une *« Proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »* (442) . Harmoniser la règlementation au sein de l'Union européenne, renforcer les droits des personnes et répondre aux enjeux de l'ère numérique figuraient parmi les objectifs principaux de la proposition de la Commission européenne.

Adoptée avec modifications par le Parlement européen le 12 mars 2014 (443), cette proposition a changé substantiellement le régime de la protection des données à caractère personnel. Le 15 décembre 2015, la version finale du texte du RGPD a fait l'objet d'un accord entre le Conseil, le Parlement et la Commission. Le Conseil de l'Union Européenne a confirmé cet accord le 12 février 2016 et le RGPD a été formellement adopté le 27 avril 2016, abrogeant la directive 95/46/CE. Il est entré en application le 25 mai 2018.

Le RGPD reprend les grands principes applicables à la protection des données dont, à titre principal : le respect de la finalité du traitement (objectif poursuivi par le traitement), la limitation de la durée de conservation des données, les garanties à mettre en œuvre au titre de leur sécurité et de leur confidentialité, sans oublier les droits reconnus aux personnes concernées.

(442) Proposition de Règlement européen du Parlement et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

(443) Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

Les changements fondamentaux par rapport à l'ancienne règlementation relèvent plus d'une nouvelle logique de responsabilisation de tous les acteurs, quelle que soit leur qualité (responsable du traitement [444] ou sous-traitant [445]).

Ainsi, il appartient aux organismes de rapporter la preuve de leur conformité au RGPD et ce, pendant tout le cycle de vie des données à caractère personnel qu'ils traitent. En attestent les nouvelles obligations qui se situent en amont des traitements, telles que :

La réalisation d'une analyse d'impact sur la protection des données pour les traitements présentant un risque élevé à l'égard des personnes concernées (exemple biométrie, surveillance à grande échelle). [446]

ou

Le recours au *Privacy by design* ou *by default* [447]. L'obligation de tenir un registre des traitements qui se substitue aux anciennes formalités déclaratives auprès de l'autorité de contrôle relève de la même logique.

Désormais, les PSCo qui ont remplacé les PSCE [448] sont soumis aux règles et principes issus du RGPD et de la Loi Informatique et Liberté modifiée. Dans ce contexte, le statut du tiers de confiance doit être clairement déterminé dans le cadre de ses relations avec ses partenaires.

(444) Selon l'article 4.7 du Règlement UE 2016/679 général sur la protection des données du 27 avril 2016 (J.O.UE 4 mai 2016 n° L119/1) « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conJointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

(445) Selon l'article 4.8 du RGPD « la personne physique ou morale l'autorité publique, le service ou un autre organisme qui traite des données pour le compte du responsable du traitement

(446) Article 35 du RGPD.

(447) Article 25 du RGPD.

(448) En effet, les PSCE sont désormais une catégorie de « prestataires de services de confiance » dont la définition est donnée à l'article 3.19 du Règlement eIDAS (J.O.UE L257/73 du 28 aout 2014) « une personne physique ou morale qui fournit un ou plusieurs services de confiance en tant que prestataire de confiance qualifié ou non qualifié ». En France, cette qualification est délivrée par l'organisme d'évaluation de la conformité LSTI actuellement seule société à qualifier les prestataires de service de confiance habilitée par l'ANSSI.

De fait, le tiers de confiance peut intervenir en tant que sous-traitant de son client ou en tant que responsable conjoint du traitement. L'analyse factuelle de la relation prévaut sur l'analyse formelle (les dispositions contractuelles). Cette analyse doit être menée au cas par cas.

Concrètement, la qualification des parties est fondamentale en ce qu'elle détermine les obligations et la responsabilité des parties (client/PSCo), étant souligné que le RGPD fixe des obligations spécifiques pour le responsable de traitement (A), le sous-traitant (B) et impose d'encadrer la responsabilité conjointe (C).

A. Obligations et responsabilité du tiers de confiance en tant que responsable du traitement

Dans le cadre de la fourniture de sa prestation, le tiers de confiance peut réaliser les traitements de données à caractère personnel relatives à des personnes physiques (collecte et conservation des données, recueil du consentement…), en tant que responsable du traitement.

Un tiers de confiance peut être qualifié de responsable du traitement lorsqu'il détermine la finalité (*« le pourquoi »*) et les moyens du traitement (*« le comment »*). Si la détermination de la finalité caractérise le responsable du traitement, la question des moyens du traitement a dû être précisée[449]. En effet, seule la définition des moyens essentiels du traitement doit être retenue pour qualifier un responsable du traitement.

Concrètement, les moyens essentiels du traitement ont trait à la détermination des catégories de personnes concernées ou des catégories de données, de la durée de conservation et des accès aux données.

Dès lors que le tiers de confiance intervient sur l'un des moyens essentiels du traitement, il est susceptible d'être responsable du traitement au sens du RGPD.

Le principe de responsabilisation (*Accountability*) qui est posé par l'article 24 du RGPD[450] impose au responsable du traitement de rapporter la preuve de sa conformité, notamment au titre des obligations ci-dessous :

+ La désignation d'un délégué à la protection des données lorsque les conditions posées à l'article 37 sont remplies ;

+ Le *privacy by design* (article 25§1 du RGPD) selon lequel la protection des données doit être prise en compte dès la conception du traitement de données personnelles et le *privacy by default* (article 25§2 du RGPD) selon lequel seules les données nécessaires sont traitées par défaut ;

+ La réalisation d'une analyse d'impact préalable (article 35 du RGPD) lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques. Elle prend en compte la nature, la portée le contexte et les finalités du traitement.

(449) Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD -Version 2.0, Adoptées le 7 juillet 2021.

(450) Le principe est le suivant « […] le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement […] ».

La CNIL a publié la liste des traitements pour lesquels une analyse d'impact est requise[451] et la liste des traitements pour lesquels une analyse d'impact n'est pas requise[452].

+ L'analyse d'impact doit au moins contenir une description des opérations de traitement envisagées, des finalités du traitement, une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, une évaluation des risques pour les droits et les libertés des personnes concernées, les mesures envisagées et les mesures de sécurité mises en œuvre ;

+ La mise en place des mesures de sécurité du traitement (article 32 du RGPD) ;

+ La notification de la violation de données à caractère personnel à la CNIL (article 33 du RGPD) et aux personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique (article 34 du RGPD).

+ L'élaboration d'une documentation relative aux traitements de données à caractère personnel telle que le registre des activités de traitement de l'article 30 du RGPD[453], le registre des violations de données à caractère personnel de l'article 33 du RGPD[454] et la politique de protection des données à caractère personnel au sein de l'organisme de l'article 24 du RGPD[455].

(451) Liste des types d'opération de traitement pour lesquels une analyse d'impact relative à la protection des données est requise ; accessible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf.

(452) Liste des traitements pour lesquels l'analyse d'impact n'est pas requise ; accessible à l'adresse : https://www.cnil.fr/fr/liste-traitements-aipd-non-requise.

(453) Art. 30.1 du RGPD : « Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité ».

(454) Art. 33 du RGPD : « Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. ».

(455) Art. 24 du RGPD : « Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement. »

De plus, le tiers de confiance doit s'assurer du respect des obligations d'information qui lui incombent à l'égard de la personne concernée par le traitement et il doit permettre à celle-ci d'exercer les droits qui lui sont reconnus par le RGPD, à savoir :

- Le droit d'accès à ses données (art. 15 du RGPD) ;
- Le droit à la rectification de ses données (art. 16 du RGPD) ;
- Le droit à l'effacement de ses données (art. 17 du RGPD) ;
- Le droit à la limitation du traitement de ses données (art. 18 du RGPD) ;
- Le droit à la portabilité (art. 20 du RGPD) ;
- Le droit d'opposition au traitement (art. 21 du RGPD).

En cas de manquement à ses obligations, le tiers de confiance s'expose à des sanctions administratives prévues par le règlement[456] ainsi que, le cas échéant, à des sanctions pénales[457].

Cela étant, en tant que fournisseur de services, le tiers de confiance peut intervenir en tant que sous-traitant vis-à-vis de son client et, dans ce contexte, être soumis à des obligations spécifiques.

B. Obligations et responsabilité du tiers de confiance en tant que sous-traitant

Dans le cadre de la fourniture de la prestation à son client (personne morale), le tiers de confiance est amené à réaliser des traitements de données à caractère personnel relatives à des personnes physiques (les clients du partenaire, son personnel ou les utilisateurs de ses services). Dès lors que ces traitements (collecte des données, recueil du consentement, conservation des données…) sont opérés pour le compte du client, responsable du traitement, et sous ses instructions documentées, le tiers de confiance a la qualité de sous-traitant au sens du RGPD.

Le RGPD pose des obligations spécifiques applicables au sous-traitant, telles que : la désignation d'un délégué à la protection des données dans les conditions de l'article 37 du RGPD, la réalisation d'un registre des traitements lié à ses activités[458], la notification des violations de données à caractère personnel au responsable du traitement[459], l'assistance et la coopération dues à ce dernier[460].

Les manquements avérés aux obligations prescrites sont passibles des sanctions administratives prévues par le RGPD[461].

(456) Selon l'article 83-4 du RGPD : « 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ». Selon l'article 83-5 du RGPD : « 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ».

(457) Article 226-16 et suivant du code pénal.

(458) Article 30 du RGPD.

(459) Article 33 §2 du RGPD.

(460) Article 28 du RGPD.

(461) Article 83 du RGPD.

Intrinsèquement lié à sa qualité, le sous-traitant doit apporter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse les droits de la personne concernée[462].

Concrètement, la certification inhérente à la qualification des tiers de confiance peut permettre de répondre aux exigences du RGPD quant aux garanties requises.

L'encadrement de la sous-traitance doit être formalisé, de façon dématérialisée ou non, étant noté que l'accord doit *indiquer a minima* les éléments suivants :

+ L'objet de la sous-traitance, ce qui implique la description des opérations de traitement réalisées par le tiers de confiance ainsi que leur finalité ;
+ La durée de la sous-traitance ;
+ Le type et les catégories de données à caractère personnel traitées ;
+ Les catégories de personnes concernées ;
+ Les droits et obligations du responsable du traitement, notamment la supervision des traitements réalisés (via des audits) ;
+ Le fait que le sous-traitant n'opère que sur instruction documentée du responsable de traitement ;
+ Les garanties mises en œuvre quant au respect de la confidentialité et de la sécurité des données ;
+ Le sort des données à l'issue de la prestation (restitution ou destruction des données).

La sous-traitance ultérieure est également encadrée par le RGPD. Il doit être noté que lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat doivent être imposées à cet autre sous-traitant par contrat.

(462) Article 28 §1 du RGPD.

Enfin, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par ses sous-traitants ultérieurs de leurs obligations.

Si l'article 28 du RGPD recense les mentions qui doivent obligatoirement figurer dans l'accord de sous-traitance, il s'agit du socle de base de l'accord formel entre les parties qui peut/doit être complété au regard de la spécificité de la relation entre le tiers de confiance et son client. Ces mentions sont précisées dans les clauses contractuelles types qui ont été adoptées par la Commission européenne le 4 juin 2021 (463).

Toutefois, compte tenu des caractéristiques inhérentes au tiers de confiance, la possibilité d'une responsabilité conjointe ne saurait être écartée.

C. Obligations et responsabilité du tiers de confiance en tant que responsable conjoint

La relation entre le tiers de confiance et son client peut relever de la responsabilité conjointe au sens de l'article 26 du RGPD. Selon cet article, les parties déterminent conjointement les finalités et les moyens (essentiels) du traitement des données à caractère personnel.

La participation conjointe à la détermination de la finalité et des moyens du traitement peut prendre la forme d'une décision commune prise par les entités concernées ou découler de décisions convergentes, nécessaires à la réalisation du traitement.

Pour le Comité européen à la protection des données qui reprend les critères dégagés par la jurisprudence de la Cour de justice de l'Union européenne en la matière : *« Un critère important est que le traitement ne serait pas possible sans la participation des parties en ce sens que le traitement par chacune des parties est indissociable de celui de l'autre, c'est-à-dire inextricablement lié »* (464).

Cette situation mérite attention dans la mesure où le tiers de confiance, en raison de son statut, peut être directement impliqué dans la détermination de moyens essentiels du traitement tels que la durée de conservation des données

(463) Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil.

(464) Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD -Version 2.0, Adoptées le 7 juillet 2021.

susceptible de lui être imposée légalement.

Concrètement, le tiers de confiance et son client doivent fixer leurs obligations et leurs responsabilités respectives au titre du RGPD dans un accord, conformément à leur rôle effectif eu égard au traitement réalisé, et compte tenu de leurs relations avec les personnes concernées.

Les grandes lignes de l'accord doivent être mises à la disposition des personnes dont les données à caractère personnel sont traitées (article 26 § 2 du RGPD) qui peuvent exercer leurs droits à l'égard de l'un ou de l'autre responsable conjoint et indépendamment des termes de l'accord (art. 26 § 3 du RGPD).

Dans ce contexte, outre le respect du principe de finalité, les responsables conjoints doivent également veiller à :

+ Minimiser la collecte des données ;
+ Conserver les données pour une durée limitée ;
+ Assurer la confidentialité et la sécurité des données par des mesures techniques et organisationnelles ;
+ Garantir les droits des personnes concernées par le traitement (droit d'accès, droit d'opposition, droit de rectification et de suppression des données).

In fine, la détermination de la qualité des parties au regard du RGPD revêt une importance capitale en ce qu'elle conditionne la répartition des obligations et des responsabilités respectives. Une analyse factuelle au cas par cas s'avère ainsi indispensable que les services du PSCo s'adressent à la sphère privée ou publique.

NOTES

IV

Cet espace vous est dédié pour prendre des notes.

Janvier 2023

QUI SOMMES-NOUS ?

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

Elle regroupe les principaux professionnels de la dématérialisation répartis en 4 collèges en fonction de leur activité professionnelle, tous concernés directement ou indirectement par la sécurisation des échanges électroniques et la conservation des informations. Elle réunit les opérateurs et prestataires de services de confiance (acteurs de l'archivage électronique, de la certification, de l'horodatage et des échanges dématérialisés ; les éditeurs et intégrateurs de solutions de confiance ; les experts et les représentants des utilisateurs ainsi que les institutionnels et les professions réglementées).

Elle a pour but d'établir la confiance, de promouvoir la sécurité et la qualité des services dans le monde de l'économie numérique, d'offrir une garantie aux utilisateurs et de défendre les droits et intérêts liés à la profession des Tiers de Confiance.

Fédération Nationale des Tiers de Confiance
14 rue de Bruxelles
75009 – PARIS
Tél. : 01 47 50 00 50

infos@fntc-numerique.com
www.fntc-numerique.com

FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE