



2019

DEVOIR
NOTE DE SYNTHÈSE B

Thème : archivage numérique

Durée : 3 heures

Sujet :

Vous êtes agent de catégorie B au sein du service d'archives du Département de X. Votre directeur vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, une note relative à l'archivage numérique.



SOMMAIRE

- Document 1 Archivage numérique : un rapport pointe l'urgence des réformes, la gazette.fr, 16/6/2017, 2 pages
- Document 2 Archivistes et informaticiens doivent travailler ensemble, la gazette.fr, 24/5/2016, 1 page
- Document 3 Archives et numérique : encore un long chemin à parcourir pour les collectivités, la gazette.fr, 20/4/2017, 3 pages
- Document 4 Le numérique dépoussière les archives, la gazette.fr, 30/1/2018, 2 pages
- Document 5 Numérisation : sous quel format conserver les documents ? 29/8/2018, archimag.fr, 2 pages
- Document 6 Archivage électronique : de l'original à la copie fiable, 5/5/2017, archimag.fr, 3 pages
- Document 7 Comment mettre en place et gérer un système d'archivage électronique, archimag.fr, 16/6/2016, 4 pages
- Document 8 L'administration à l'heure du numérique, francearchives.fr, 13/9/2018, 2 pages
- Document 9 La NF Z42-026 est enfin publiée ! archimag.fr, 9/6/2017, 2 pages
- Document 10 Numérisation fidèle et destruction des originaux papiers, c'est parti ! fntc-numerique.com, 20/4/2017, 2 pages

Ce document comprend un sujet de 2 pages et un dossier de 23 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué. S'il est incomplet veuillez en avertir le surveillant(e)

Certains documents peuvent comporter des renvois à des notes ou à des documents volontairement non fournis car non indispensables à la compréhension du sujet.

ARCHIVES

Archivage numérique : un rapport pointe l'urgence de réformes

Publié le 16/06/2017 • Par **Isabelle Verbaere** • dans : Actualité Culture, Documents utiles, France



Phovoir

Malgré les évolutions juridiques et réglementaires récentes, l'infobésité fait peser une véritable menace sur les archives. C'est la principale conclusion du rapport de Christine Nougaret, vice-présidente du Conseil supérieur des Archives, publié le 6 juin 2017. Elle y détaille une trentaine de mesures pour améliorer la collecte et l'accès aux données.

La production de documents électroniques a explosé au cours de ces dernières années et ce n'est qu'un début. Dans le même temps, la collecte des archives papiers n'est pas prête de se tarir. Le cadre juridique et réglementaire et les pratiques des archivistes sont-elles encore pertinents dans ce contexte d'infobésité ? Ce n'est pas l'avis de Christine Nougaret, vice-présidente du Conseil supérieur des Archives et professeure à l'Ecole nationale des Chartes.

Dans un [rapport](#) rendu public le 6 juin et intitulé «Une stratégie nationale pour la collecte et l'accès aux archives à l'ère numérique» (commandé en octobre 2016 par Audrey Azoulay alors ministre de la Culture), elle détaille 30 propositions. Elles concernent à la fois les archives nationales et territoriales, le numérique et le papier, la collecte et l'accès aux archives à l'ère du numérique.

Le sens du mot « donnée »

Dans la première partie, l'auteure en appelle à une clarification de la définition des archives mais aussi du rôle des archivistes.

Elle suggère ainsi dans sa première proposition « de préciser le sens du mot « donnée », «dans le champ d'application du code du patrimoine, afin d'assurer l'archivage définitif des données numériques essentielles ». Des données qui, selon elle, « devraient être conservées sur le territoire national ou, à défaut, dans un pays offrant les mêmes garanties de sécurité que la France, et chez un prestataire hébergeur placé sous le contrôle de l'autorité publique ».

Christine Nougaret s'inquiète également que le numérique a fait voler en éclats le cadre territorial dans lequel s'était coulé jusqu'alors le réseau des archives.

« La reconfiguration de l'État déconcentré dans un cadre régional et interrégional rompt l'uniformité des compétences entre départements qui caractérisait la France depuis plus de deux siècles », pointe-t-elle.

Adaptation aux nouveaux cadres territoriaux

Elle propose ainsi « d'adapter le réseau des archives aux nouveaux cadres territoriaux ». Ces reconfigurations impliqueraient entre autres, de mettre en place «une coordination régionale entre services d'archives départementales, qui pourrait être confiée au directeur du service d'archives chef-lieu de région, sous réserve de reconnaître et de valoriser cette fonction supplémentaire ».



©CCO

Formation numérique des archivistes

Dans sa proposition n° 8, l'auteure souligne qu'il faut renforcer la formation au numérique des archivistes. « La compétence numérique, nouvelle dans le bagage des archivistes, doit être reconnue dans les référentiels des métiers et valorisée dans le déroulement de leur carrière, estime-t-elle.

Et la vice-présidente du Conseil supérieur des Archives de glisser qu'il serait bien que les référentiels de certains métiers de l'informatique évoluent aussi et comprennent des compétences en matière de traitement des données et d'archivage numérique !

Macro-évaluation des archives

La seconde partie pointe les enjeux de la collecte. « Pour garantir une collecte durable à l'ère numérique, il convient de concentrer l'action des services d'archives sur la conservation des archives définitives, c'est-à-dire celle de valeur pérenne, à garder sans limite de durée ». Pour y parvenir l'auteure suggère de déterminer les archives essentielles, tant papier que numériques, grâce à la macro-évaluation. Mais aussi « d'affirmer la responsabilité de l'État dans la conservation de ses archives définitives en régions, pour une répartition équitable des coûts entre État et collectivités. »

Mutualisation de l'archivage numérique

Quatre propositions visent les données numériques. Le rapport souligne que l'État déconcentré et les collectivités territoriales, pourraient mutualiser l'archivage numérique à l'échelon régional ou départemental. « Sous réserve d'une répartition équitable des charges qui ne peuvent incomber aux seules collectivités territoriales », insiste l'auteure.

Enfin, la dernière partie se penche sur l'accès aux archives à l'ère du numérique. L'auteure dénonce « l'ensemble de l'édifice législatif et réglementaire français qui rend inintelligible le système de droit d'accès à l'information publique ». Le rapport compte plusieurs propositions pour le simplifier.

FOCUS

Quel avenir pour les archives papier ?

Le rapport compte trois propositions qui concernent spécifiquement les archives papier. Christine Nougaret note par exemple : il s'agirait d'économiser l'espace de stockage et donc réduire les coûts à long terme, grâce « à la réévaluation » du stock d'archives et à la mutualisation des magasins.

Document 2

La gazette.fr

CULTURE

Archivistes et informaticiens doivent travailler ensemble

Publié le 24/05/2016 • Par **Hélène Girard** • dans : France



©Archivo SFP CC BY-SA 3.0 via Wikimedia
D.R.

Pierre-Frédéric Brau, directeur des Archives départementales de l'Yonne, a été élu président de l'Association des archivistes français (AAF) le 29 avril 2016. Dans quelques jours, au Salon des maires et des collectivités locales (Paris, du 31 mai au 2 juin 2016), où, pour la troisième année consécutive, l'AAF tiendra un stand, il plaidera auprès des élus pour la place des archives dans la gestion administrative des collectivités dans les univers papier et numérique.

Dans quel état d'esprit abordez-vous votre mandat ?

Il s'agit bien sûr, pour l'ensemble de l'association, de faire entendre la voix des archivistes, pour promouvoir et défendre notre métier. Mais pas seulement. Il s'agit aussi de développer largement la culture des archives. Disposer d'archives organisées et pérennes est un gage de démocratie, de transparence et de garantie des droits individuels. L'AAF a déjà eu l'occasion de montrer qu'elle est capable de contribuer à développer cette culture. Le dernier exemple en date est celui du projet de loi « liberté de création, architecture et patrimoine » (dit projet de loi « CAP »), dans lequel elle a réussi à introduire un volet sur les archives, absent dans la version initiale présentée par le gouvernement. C'est ainsi que la définition des archives a pu être révisée pour y inclure les données.

(...)

La gazette.fr

NUMÉRIQUE

Archives et numérique : encore un long chemin à parcourir pour les collectivités

Publié le 20/04/2017 • Par Isabelle Verbaere • dans : Dossiers d'actualité, France



Flickr CC by sa DRs Kulturarvsprojekt

La dématérialisation des procédures administratives pose la question de la sécurisation de l'archivage des documents qui peuvent faire foi. Mais peu de collectivités en ont mesuré les enjeux.

La dématérialisation ? Aucune collectivité ne peut désormais y échapper ! La montée en charge de la facturation électronique en est la preuve. Depuis le 1^{er} janvier 2017, les plus grandes sociétés françaises doivent transmettre des factures dématérialisées à leurs clients publics, qui sont tenus de les accepter. Toutes les entreprises seront soumises à cette obligation dès 2020 (ordonnance du 26 juin 2014 définissant le calendrier d'obligation de facturation électronique).

L'Agence pour l'informatique financière de l'Etat a mis gratuitement à disposition des fournisseurs, mais aussi des collectivités, une solution intitulée « Chorus pro ». Lorsqu'une facture est déposée sur la plateforme, le portail la stocke dans son serveur Atlas, sur lequel la direction générale des finances publiques archive aussi toutes les pièces justificatives transmises par les ordonnateurs au comptable public.

« L'Etat est allé au bout de la démarche en proposant une solution pour l'archivage de ces documents pendant le temps de leur durée d'utilité administrative », se félicite Catherine Junges, responsable du pôle des archives départementales des Yvelines. « C'est essentiel, car, jusqu'alors, les collectivités n'envoyaient que des copies scannées et gardaient précieusement les originaux papier. Mais avec la dématérialisation, l'original, c'est la facture numérique. Et la plupart des communes n'ont pas les moyens de sécuriser ces documents. »

En 2000, la reconnaissance de l'écrit électronique comme preuve (loi n° 2000-230 du 13 mars 2000) a ouvert la voie à la dématérialisation des procédures administratives. Les collectivités ont emboîté le pas à l'Etat, multipliant les chantiers de dématérialisation.

Des données vulnérables

« Cette dématérialisation tous azimuts, sans réflexion sur la sécurité des données, comporte une somme considérable de risques pour les collectivités, prévient Catherine Junges. Dans un environnement papier, nous savons maîtriser la fiabilité, l'organisation et la sécurité de l'information. C'est beaucoup plus difficile dans un environnement numérique. »

En effet, les données numériques sont très vulnérables, pour au moins deux raisons : d'abord, elles sont aisément modifiables ; ensuite, elles peuvent être perdues, leurs supports et formats étant devenus obsolètes. Et surtout, la durée de vie de ces supports et formats est, dans certains cas, plus courte que celle de conservation des documents.

La perte de ces informations représente un risque juridique : de nombreuses pièces ont une durée d'utilité administrative définie par le service interministériel des archives de France. Certains mails, par exemple, peuvent faire foi en cas de litige avec un administré. La perte de données numériques peut aussi altérer le fonctionnement d'un service.

« Les mesures de pluviométrie, par exemple, n'ont pas de valeur légale, mais les services d'assainissement ont besoin de garder des statistiques fines sur plusieurs dizaines d'années pour assurer un dimensionnement et un fonctionnement corrects des canalisations », précise Céline Sename, cheffe du service des archives de la métropole européenne de Lille (90 communes, 1,12 million d'hab.).

D'autres documents, enfin, ont aussi une valeur historique, à l'instar des données d'état civil. La conservation de ces informations numériques représente donc des enjeux considérables. Pourtant, peu de collectivités en ont déjà pris la mesure. Sur 202 collectivités interrogées, seules 20 % ont déployé un système d'archivage électronique. C'est le résultat d'une enquête diffusée par l'Association des archivistes français (AAF), réalisée en mars 2016.

Dématérialisation sans filet

Plusieurs freins limitent le développement de l'archivage électronique. « Nombre d'administratifs n'ont pas conscience que les bases de données ou les mails sont clairement définis comme des archives dans le code du patrimoine, observe Pierre-Frédéric Brau, directeur des archives de l'Yonne et président de l'AAF. C'est beaucoup plus simple, et, a priori, plus séduisant, de rechercher un fichier conservé dans un répertoire sur un ordinateur ou par le biais d'un système de gestion électronique de documents, que d'aller fouiller dans des cartons. Du coup, ils se sentent libérés des contraintes de gestion des documents auxquelles ils se pliaient plus ou moins avec le papier. »

De multiples exemples de dématérialisation sans filet illustrent cette quasi-insouciance. « Certaines collectivités dématérialisent leurs arrêtés, alors que c'est une obligation d'avoir un original papier signé, soupire Cyril Longin, directeur des archives de Saint-Etienne [170 800 hab.]. C'est lui qui fait office de preuve. »

L'Etat ne montre pas forcément l'exemple. « La loi de modernisation de la justice du XXI^e siècle propose aux communes d'être dispensées de l'élaboration du double des registres de l'état civil conservé au tribunal de grande instance, rappelle Catherine Junges. A condition que la conservation des données entrées dans le logiciel lors d'une naissance ou d'un mariage, par exemple, bénéficie de dispositions de sécurité renforcées. Le décret qui doit les définir n'est pas encore paru. »

Cyril Longin s'interroge : « Il paraît qu'il serait possible de confier le stockage de ces données à un tiers, avec le prérequis qu'il soit sur le territoire français, mais sans qu'un agrément ne soit prévu. C'est prendre ces données à la légère. »

Des économies à la clé

Le contexte budgétaire constitue un autre obstacle à l'archivage électronique, car il ne peut se réduire à la seule acquisition d'un outil informatique pour la conservation des données. «

L'archivage numérique suppose une stratégie transversale de pilotage. Il est au cœur des préoccupations actuelles, expose Katell Auguié, responsable de l'information à la direction des finances et des affaires juridiques de la ville d'Orvault [25 300 hab., Loire-Atlantique].

Au centre de toute stratégie numérique se trouve la question des données, de leur qualité et de leur conservation. On ne peut plus créer des pièces ou des données sans s'interroger en amont sur leur utilité et leur devenir. »

Sans compter que cette démarche est synonyme d'économies. « Elle nous permet d'identifier les documents importants et de supprimer les autres, et, par conséquent, de faire des économies en termes de stockage et de serveurs », estime Anthony Claverie, directeur adjoint « innovation organisationnelle » de la ville d'Antibes (75 700 hab., Alpes-Maritimes). Et sa collaboratrice, Emilie Debled, responsable de l'unité « archives contemporaines », de préciser : « On ne conserve qu'une toute petite partie de la production, qui n'excède pas 10 %. »

Bien que les directions informatiques soient avant tout préoccupées par des questions de sauvegarde, elles n'ont pas toujours conscience de l'intérêt à collaborer avec les archivistes. « Le travail de pédagogie est très long à mener pour faire prendre conscience que nous avons un objectif commun : sécuriser l'information et la rendre accessible », analyse Pierre-Frédéric Brau.

Ce travail de pédagogie, les archivistes du conseil départemental d'Indre-et-Loire ont choisi de le mener en proposant des ateliers de la dématérialisation ouverts à tous, élus et agents, une fois par mois. « Nous accueillons 140 participants à chaque fois, se félicite Lydiane Gueit-Montchal, directrice des archives départementales. Il ne s'agit pas de leur vendre une solution, mais de vulgariser certaines problématiques, comme la signature électronique ou la sécurisation des données. »

FOCUS

Dématérialisation obligatoire : le calendrier des échéances d'ici à 2020

- **2016**

Tout usager peut saisir les administrations par voie électronique. Celles-ci sont obligées de l'informer sur la façon dont il peut exercer ce droit. Elles sont également tenues d'envoyer un accusé de réception électronique.

- **2017**

Factures et avis des sommes à payer. Obligation d'accepter toutes les factures électroniques. Obligation d'émettre des factures électroniques à l'encontre d'autres entités publiques.

« **Full-démat** ». Obligatoire pour les métropoles.

- **2018**

Comedec. La procédure de vérification de l'état civil par voie dématérialisée devra obligatoirement être mise en oeuvre par les communes sur le territoire desquelles est ou a été située une maternité.

Protection des données personnelles. Règlement européen sur la protection des données du 4 mai 2016 qui entrera en application le 25 mai 2018.

Marchés publics – Dématérialisation des procédures de marché public à partir du 1er octobre 2018.

- **2019**

« **Full-démat** ». Collectivités de plus de 10 000 habitants. Factures. Obligation d'accepter les factures électroniques des petites et moyennes entreprises.

- **2020**

Actes. Dématérialisation obligatoire du contrôle de légalité pour les régions, les départements, les communes de plus de 50 000 habitants et les établissements publics de coopération intercommunale.

Urbanisme. Transmission de tous les documents uniquement via Géoportail.

FOCUS

Stocker, ce n'est pas archiver

Certains termes n'ont pas le même sens pour les archivistes et les informaticiens. Ces derniers assimilent parfois le stockage à l'archivage. « Conserver des données numériques sur un disque dur externe ou un serveur revient à ranger des dossiers dans une armoire », souligne Lydiane Gueit-Montchal, directrice des archives départementales d'Indre-et-Loire. Ce n'est pas de l'archivage, pour au moins trois raisons : les données sont enregistrées dans leur format d'origine ; le serveur ne garantit pas leur lisibilité dans le temps ; elles sont accessibles à ceux qui les ont produites et leur contenu peut être modifié et altéré. Elles ne sont donc pas fiables et ne pourront pas constituer une preuve. Enfin, elles sont généralement conservées sur un site unique. Ce qui peut faire courir le risque de perte en cas d'incident.

FOCUS

Claire Sibille-de Grimoüard, sous-directrice de la politique archivistique au service interministériel des archives de France

« **Il s'agit de sécuriser la destruction de documents papier numérisés** »

Dans le cadre de la réforme du droit des contrats, l'article 1348 du code civil, devenu l'article 1379, a été remanié. Il dispose qu'est présumée fiable toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est maintenue dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'Etat [décret du 5 décembre 2016]. Il s'agit de sécuriser la destruction de documents papier qui ont été numérisés. Le décret définit les situations dans lesquelles une copie sera présumée fiable. Il dispose, d'abord, qu'elle n'a pas nécessairement besoin d'être sur un support papier et fixe ensuite les conditions dans lesquelles la copie peut être faite par voie électronique.

Document 4

La **gazette.fr**
PATRIMOINE

Le numérique dépoussière les archives

Publié le 30/01/2018 • Par **Nathalie Levray** • dans : Dossiers d'actualité, France, Innovations et Territoires



STEPHANIE RENARD/VILLE DE TOULOUSE

Le numérique est une opportunité pour décupler la valorisation des fonds. La numérisation des archives élargit les diffusions. Les archivistes étendent leur périmètre traditionnel des chercheurs et des généalogistes au grand public. Ils collaborent avec les internautes autour des contenus. Au-delà d'une présence en ligne, les archivistes investissent les réseaux sociaux.

CHIFFRES-CLÉS

Agenda – Événement

29 mai, Paris

Assises de la dématérialisation : quels défis pour les collectivités ?

« Si on n'existe pas sur le numérique, on n'existe plus du tout », assène Catherine Bernard, directrice adjointe des archives municipales de Toulouse (466 300 hab.). Elle ne sera pas contredite par Martine Cardin, professeure titulaire en archivistique à l'université Laval de Québec (Canada), selon laquelle il est urgent de « penser des plateformes pour mettre en forme les archives et rendre l'archivistique ouverte et vivante ».

Alors, l'archiviste toulousaine n'a pas ménagé ses efforts quand son directeur lui a passé commande d'« un écosystème de moyens numériques » visant à communiquer avec les usagers et « sortir les archives des archives ». Afin de relever le pari d'une existence en ligne, Catherine Bernard a « élaboré une stratégie numérique à long terme, rédigé des contenus et fédéré une équipe ». Elle rit en se souvenant « d'avoir un peu forcé la main aux contributeurs dans le but d'écrire la newsletter mensuelle ».

La stratégie numérique toulousaine s'est construite sur un « ancrage dans le présent, pour apporter aux usagers des clés de compréhension et les projeter dans l'avenir », mais le site est un

« socle pour construire des contenus d'informations et de connaissances, et valoriser les fonds sur deux axes prioritaires : l'évolution urbaine de Toulouse et les images », précise-t-elle.

Ces thèmes « attractifs » n'ont pas été choisis par hasard : il s'agit d'amener le grand public à surfer sur le site des archives afin qu'il utilise ensuite « les bases de données documentaires, les réseaux sociaux et le site UrbanHist [\(1\)](#) de connaissance de la ville ».

Expertise bénévole

Chargée de la communication et de la valorisation aux archives municipales et communautaires d'Orléans métropole (22 communes, 281 900 hab.), Christelle Bruant, archiviste responsable des fonds modernes, iconographiques et privés, administre aussi le site internet de l'agglo et le compte Twitter.

« Les archivistes ne sont plus condamnés à ne rencontrer que des initiés, et à ne croiser le grand public qu'au moment des Journées européennes du patrimoine », se réjouit-elle. Elle cite l'espace de commémoration de la guerre de 1914-1918 en ligne, « impossible à réaliser physiquement faute de lieu suffisamment grand pour accueillir le public ».

Elle reconnaît que cette intrusion numérique l'a conduite à « revoir sa réflexion sur la façon de transmettre ». Et de recevoir également.

Opérationnelles en ligne depuis 2011, les archives, principalement l'état civil, les cartes postales et les plans – soit « 1 % des fonds seulement », regrette-t-elle – bénéficient de l'expertise bénévole des usagers du site après accès validé.

Ce pari de l'annotation collaborative, testée avec les généalogistes, bénéficie tant aux usagers dans leurs recherches qu'à la collectivité pour qui c'est « un révélateur de pépites qui valorise ses sources ».

« Notre mission ultime est de mettre à disposition les documents archivés, sous toutes les formes, afin que les usagers s'en emparent », confirme Hugues Courant, responsable de la valorisation aux archives de la ville et de la métropole de Brest (8 communes, 208 500 hab.).

(...)

Numérisation : sous quel format conserver les documents ?

Le 29/08/2018 Michel Thomas

photo_scan.jpg



PDF (ISO 32000) est un format normalisé internationalement. Disposant de visionneuses gratuites il est le format préférentiel de tout document numérisé. (Pixabay/Toomanyloginnames)

Source : [Serda Conseil](#)

La dématérialisation s'impose aujourd'hui dans toutes les organisations. Beaucoup de documents sont dès lors numérisés, encore faut-il savoir sous quel format les conserver.

Le Référentiel Général d'Interopérabilité version 2 (RGI) recommande 5 formats utilisables pour les objets images :

- **JPEG** : Joint Photographic Experts Group
- **TIFF** : Tag Image File Format
- **PDF** : Portable Document Format
- **GeoTIFF** : Geographical Tag Image File Format
- **PNG** : Portable Network Graphics

Le format JPEG

Défini par et pour la photographie, ce format présente des inconvénients pour la numérisation de documents. Les techniques de compression utilisées par JPEG, ne sont pas optimales pour le texte. L'utilisation du format JPEG à la numérisation interdit quasiment tout traitement ultérieur sur l'image.

Le format TIFF

Ce format est couramment utilisé par les logiciels de numérisation. Il permet de créer des fichiers multipages, ce qui est intéressant pour la numérisation de documents plus ou moins volumineux.

L'inconvénient de ce format est double :

Sa pérennité dans le temps n'est pas garantie, car il n'est pas soutenu par une organisation internationale de normalisation, à l'exception de ses deux variantes qui sont des standards de la télécopie noir et blanc ou couleur, gérés par l'UIT-(Union Internationale des Télécommunications). Les visionneuses TIFF sont des outils propriétaires, même s'il existe des logiciels gratuits comme IrfanView ou XnView et une bibliothèque OpenSource : LibTIFF.

Il est le format privilégié pendant la phase de traitement post-numérisation des documents. Mais il est préférable de le convertir ensuite en PDF pour la conservation.

Le format PDF

PDF (ISO 32000) est un format normalisé internationalement. Disposant de visionneuses gratuites il est le format préférentiel de tout document numérisé.

- Il est multipage et multi documents ;
- Il permet d'intégrer les métadonnées documentaires,
- Il peut sécuriser le document électronique,
- Il permet la signature électronique des documents.

La norme ISO 19005 définit un PDF Archive pour la conservation.

Elle a 3 versions publiées et une quatrième en cours de publication :

- La version PDF/A-1, antérieure à l'adoption de la norme ISO 32000, est basée sur la version 1.5 d'Adobe PDF. Elle ne dispose pas des technologies de compression les plus modernes ; elle ne permet pas l'encapsulation de plusieurs documents dans le PDF.
- La version PDF/A-2 est basée sur l'ISO 32000. C'est la version recommandée pour l'archivage. Elle peut archiver en un seul fichier un dossier de documents PDF.
- La version PDF/A-3 répond à un besoin spécifique d'archivage de documents d'origine numérique, lorsqu'il est souhaité de conserver le format original en plus de sa conversion en PDF.
- Enfin la norme ISO32000 étant en révision pour incorporer entre autres les nouveaux formats 3D, une version PDF/A-4 est en développement.

Note : quel que soit la version de PDF, les documents numérisés seront pérennes, car par nature ils ne comportent pas d'éléments susceptibles d'empêcher leur lecture ultérieure.

Les formats GeoTIFF et PNG

GeoTIFF est une standardisation particulière du format TIFF et PNG est un format peu pratique à utiliser pour la numérisation.

Michel THOMAS

MT CONSEIL

Source : Serda Conseil

Archivage électronique : de l'original à la copie fiable

Le 05/05/2017 Sylvain Martin

[the_copie.jpg](#)



Sylvain Martin : "le décret reconnaît implicitement que le changement de support peut générer pendant la migration des pertes de données minimales qui ne remettent pas en cause la fidélité de la copie" (Photo via Visualhunt)

Après l'entrée en vigueur le 1er juillet 2016 d'un règlement européen sur l'identification électronique et le 1er octobre 2016 de la réforme des dispositions du Code civil sur la preuve, puis la publication en décembre 2016 du décret sur la fiabilité des copies électroniques, une synthèse des règles applicables à l'archivage électronique s'impose.

Le numérique est entré dans le Code Napoléon en même temps que le nouveau millénaire avec la reconnaissance légale de l'écrit et de la preuve électronique par une loi du 13 mars 2000. En 2016, une réforme globale du droit de la preuve a été l'occasion d'introduire dans le Code civil les dernières évolutions des règles technico-juridiques relatives à l'égalité entre l'écrit papier et l'écrit électronique.

Ainsi, le nouvel article 1379 du Code civil affirme qu'une copie électronique « fiable » a la même force probante que l'original. 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 d'origine, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret.

Ce décret 2016-1673 du 5 décembre 2016 prévoit deux procédés permettant de présumer la fiabilité d'une copie électronique, c'est-à-dire sa fidélité à l'original et son incorruptibilité.

Le premier procédé est vieux comme la norme NF Z42-013 de 1999. Il s'agit de la reproduction sur un support physique modifié de manière irréversible, à savoir un disque Worm (write once read many).

Le second procédé de reproduction reconnu par le décret de 2016 est la voie électronique. S'agissant d'un procédé immatériel, le décret exige de nombreuses conditions techniques destinées à assurer la fiabilité juridique.

1. La reconnaissance juridique de la reproduction électronique

Il faut tout d'abord que le dispositif de reproduction électronique produise des informations liées à la copie et destinées à l'identification de cette copie. Ces informations précisent le contexte de la numérisation, en particulier la date de création de la copie. Autrement dit, il faut recourir aux technologies de la cryptologie dans les conditions du décret 2001-272 du 30 mars 2001 qui définit les conditions techniques dans lesquelles on peut juridiquement générer des données attachées à un document électronique (un fichier numérique en PDF, par exemple) de telle manière que toute modification ultérieure de ce document soit détectable.

Empreinte électronique

Le décret du 5 décembre 2016 dispose ainsi, dans la logique de la technologie de la cryptologie, que cette intégrité de la copie résultant du procédé de reproduction par voie électronique utilisé est attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable. C'est exactement ce que cherchent les prestataires d'archivage électronique et leurs clients pour assurer la force probante des documents archivés sous forme électronique.

Le décret ajoute que cette condition de traçabilité d'une modification est présumée remplie par l'usage d'une empreinte qui peut être un horodatage et/ou un cachet électronique et/ou une signature électronique à condition que l'empreinte à laquelle on recourt soit « qualifiée » au sens du règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques. Ce règlement européen définit le cadre technico-juridique de qualification de ces trois empreintes auxquelles on peut avoir recours pour associer de manière sûre un horaire à une opération sur un document, ou assurer de manière sûre l'intégrité d'un document après apposition d'un sceau par une personne morale, ou encore affirmer de manière sûre l'identité d'une personne physique qui signe de manière électronique un document numérique.

Le métier d'un prestataire d'archivage

Horodater le document dont ils prennent en charge l'archivage, sceller ce document pour que son intégrité soit assurée et engager son employé en lui faisant apposer sa signature sur son travail d'archivage, c'est le métier d'un prestataire d'archivage. Grâce aux technologies de la cryptologie prises en compte par le règlement européen du 23 juillet 2014, les prestataires d'archivage peuvent donc respecter le décret du 5 décembre 2016.

Ce décret exige que la copie électronique soit conservée dans des conditions propres à éviter toute altération de sa forme ou de son contenu. La reproduction doit donc être faite à l'identique et doit le rester. Se pose alors la question du transfert d'une copie fixée sur un support matériel fonctionnant dans un système informatique (DVD sur lequel on retranscrit un document électronique et son lecteur) vers un autre support fonctionnant dans un autre système informatique (serveurs du cloud dans lesquels on fixe les copies). Le décret reconnaît implicitement que le changement de support peut générer pendant la migration des pertes de données minimales qui ne remettent pas en cause la fidélité de la copie. Ainsi, il précise que les opérations requises pour assurer la lisibilité de la copie électronique dans le temps ne constituent pas une altération de son contenu ou de sa forme dès lors qu'elles sont tracées et donnent lieu à la génération d'une nouvelle empreinte électronique de la copie.

2. Les limites de la reconnaissance réglementaire

Les empreintes et les traces générées en application des opérations d'archivage sont conservées aussi longtemps que la copie électronique peut être produite et dans des conditions ne permettant pas leur modification. L'accès aux dispositifs de reproduction et de conservation fait l'objet de mesures de sécurité appropriées. Toute l'organisation de l'archivage est décrite dans une documentation conservée aussi longtemps que la copie électronique produite. La qualité du procédé doit être établie par des tests sur des documents similaires à ceux reproduits et vérifiée par des contrôles.

Appréciation du juge

Malgré toutes ces exigences, le décret du 5 décembre 2016 considère que la fiabilité reste à l'appréciation du juge. Le décret ne valide donc pas de manière irréfragable le processus de la copie électronique qu'il décrit, ce qui laisse en suspens la question aussi ancienne que l'archivage électronique : peut-on se passer des originaux en papier ?

L'ordonnance 2017-29 du 12 janvier 2017 apporte une réponse claire pour les documents comportant des données de santé à caractère personnel produits par un professionnel de santé. Elle vient d'introduire dans le Code de la santé publique un nouvel article L1111-26 qui autorise expressément la destruction de tels documents originaux avant la fin de la durée légale de conservation dès lors que les copies numériques remplissent les conditions de fiabilité prévues par le deuxième alinéa de l'article 1379 du Code civil, à savoir remplissent les conditions du décret du

5 décembre 2016. On peut détruire ces originaux puisque la loi le permet au motif que la copie a la même force probante que le document original sur support papier.

Future norme Afnor

Lorsque l'on ne dispose pas d'un texte aussi clair que le Code de la santé publique, on se reportera à l'article 1379 du Code civil, troisième alinéa, qui dispose que : « Si l'original subsiste, sa présentation peut toujours être exigée ». Cette disposition est sibylline si on y cherche l'autorisation sans réserve de la destruction des originaux. Il est donc recommandé de détruire volontairement ses originaux uniquement à bon escient, avec parcimonie et dans le respect de la future norme Afnor Z 42-026, qui va prochainement sortir, et dont l'objet est notamment la définition d'un état de l'art de la copie fiable en conformité avec le décret du 5 décembre 2016.

Sylvain Martin

Avocat à la Cour

www.sylvain-martin.com

Membre du conseil d'administration de l'Adij

Comment mettre en place et gérer un système d'archivage électronique

Le 16/06/2016 Michel Thomas



Les étapes de déploiement au reste des services, fonctions et documents de l'organisation devront être menées avec un suivi assuré par le comité de pilotage pluridisciplinaire. (Photo via Visualhunt)

N'est pas un système d'archivage électronique qui veut. Devant l'importance de ses enjeux liés au cycle de vie des documents, il convient d'obéir scrupuleusement à une méthodologie de mise en place, en s'appuyant sur une importante famille de normes, puis de gestion dans le temps. Des procédures sont à prévoir dès la conception.

La mise en place et la gestion d'un système d'archivage électronique (SAE) dans une organisation publique ou privée doit suivre les étapes classiques de toute conduite de projet informatique :

1. Étude d'opportunité et environnement juridique
2. Étude de faisabilité et environnement financier et technique
3. Le cahier des charges
4. L'analyse des réponses et le choix du prestataire
5. Les spécifications détaillées
6. Installation d'un système pilote
7. Déploiement du SAE
8. La gestion du SAE (migrations nécessaires, questions à se poser lors d'une évolution, considérations sur le choix d'un support d'archivage)

1. Étude d'opportunité et environnement juridique

Mon organisation reçoit-elle ou émet-elle des documents dématérialisés (comme des factures EDI ou des PDF signés, des appels d'offres publics dématérialisés, des courriers électroniques ayant valeur légale d'engagement, etc.) ? Si oui : quels types de documents recevons-nous électroniquement ? A ce niveau, il est nécessaire de disposer d'une étude sérieuse de l'existant sur les documents échangés dans et en dehors de l'entreprise afin de définir le périmètre du SAE :

- Les types de documents à archiver (messagerie électronique, documents bureautiques, données informatiques, documents au format PDF, etc.) ;
- La valeur juridique des documents échangés.

Cette étude d'opportunité permettra de délimiter très précisément le contexte juridique et réglementaire dans lequel se situent l'organisation et ses échanges documentaires. Tout particulièrement, c'est à ce stade qu'il faudra décider s'il convient de respecter la norme NF Z42-013 (Iso 14641) et à quel niveau de conformité. Faire appel à des juristes et à des archivistes dès cette étape est fondamental pour une bonne réussite du projet.

2. Étude de faisabilité et environnement financier et technique

Si l'étude d'opportunité révèle la nécessité de mettre en place un SAE, reste alors à établir sa faisabilité et à choisir la solution la plus adaptée : un SAE en interne est-il réalisable ou est-il préférable de l'externaliser ?

Pour ce faire, voici un ensemble de points à examiner sous leurs aspects organisationnels, techniques et financiers : avons-nous besoin d'archives en ligne ou pouvons-nous archiver nos documents et données sur des supports électroniques amovibles, disques optiques numériques ou bandes magnétiques ?

S'il est nécessaire de disposer d'archives en ligne :

- Existe-t-il un espace pouvant accueillir un local informatique sécurisé permettant le respect des normes de sécurité obligatoires d'un SAE (normes de la série Iso 27000, respect du Référentiel général de sécurité ou RGS, haute protection des accès humains et informatiques, etc.) ;
- Disposons-nous d'équipes d'exploitation capables de respecter les normes Iso 14641, Iso27000, avec des procédures de suivi des incidents rigoureuses ?
- Quelle solution de recours sécurisée pouvons-nous envisager pour la duplication des documents archivés ? Est-il impératif de développer un deuxième centre informatique sécurisé ou pouvons-nous utiliser des archives "off line", comme des disques optiques numériques ou des bandes magnétiques ?

S'il l'on peut archiver sur des supports amovibles :

- Notre infrastructure comporte-t-elle deux emplacements de stockage sécurisés pour le rangement des supports ?
- Pouvons-nous mettre en place des procédures sécurisées pour l'enregistrement, la manipulation, le transfert des supports ?

Cette étape vise donc directement la direction financière, la direction informatique et la direction juridique, et les représentants des métiers concernés par le SAE, puisque ce sont eux qui détermineront les points d'accès aux archives.

3. Le cahier des charges

Le cahier des charges du SAE sera très différent suivant que la solution retenue sera un SAE interne ou externe.

Des documents normatifs existent pour nous aider dans cette étape, en particulier le fascicule de documentation Afnor FD Z42-018, et bien entendu la norme Afnor NF Z42-013 (ou Iso 14641).

Mais attention : si la mise en place du SAE demande l'installation d'un nouveau centre de calcul sécurisé, le cahier des charges ne sera pas uniquement du matériel et du logiciel informatique, mais également du bâtiment, de l'alimentation énergétique, de la climatisation, etc. La mise en place peut ainsi être une opération relativement complexe ou à l'opposé assez simple, si, comme cela est possible, la solution retenue est un archivage sur supports amovibles, comme des CD-R ou DVD-R, avec une station d'enregistrement basique et la réalisation de copies multiples.

Dans tous les cas, le cahier des charges d'un SAE comportera un volet organisationnel, qui n'est pas nécessairement à usage externe à l'organisation, mais qui est aussi à usage interne. En effet, l'organisation, les procédures et l'environnement humain d'un SAE sont une composante à ne pas oublier si des normes comme l'Iso 14641 (Afnor NF Z42-013) doivent être respectées.

4. L'analyse des réponses et le choix du prestataire

À cette étape, il faudra regarder non seulement la conformité de la réponse au cahier des charges, mais également la pérennité du prestataire. En effet, il serait dangereux, tout particulièrement pour le choix d'un archivage externalisé, de retenir un prestataire qui ne présenterait pas des garanties sérieuses de pérennité.

Pour une solution interne, le choix du prestataire est à ce niveau moins critique, tant que les solutions mises en place peuvent facilement être reprises soit par le service informatique de l'organisation, soit par un autre prestataire. Pour cela le respect des standards informatiques et documentaires et l'accès possible aux sources des programmes sont des éléments fondamentaux qui doivent être soigneusement examinés.

5. Les spécifications détaillées

Cette étape est bien entendue généralement menée par le prestataire retenu, mais pour un SAE il est très important qu'une équipe pluridisciplinaire, comportant des juristes, des financiers, des référents métier, des informaticiens, des archivistes, constitue le comité de pilotage vérifiant et validant toutes les spécifications mises en place.

6. Installation d'un système pilote

Toutes les étapes précédentes devraient avoir permis de définir un environnement pilote : quels services, quelles fonctions, quels documents vont constituer le premier test du SAE ? Il serait toutefois dangereux de vouloir archiver la totalité des informations de l'organisation dès l'ouverture du SAE. Il pourrait alors être difficile de tester convenablement la conformité du système. Le cas échéant, un premier audit de conformité du SAE à la norme Iso 14641 est à mener pour une validation finale du système pilote.

7. Déploiement du SAE

Les étapes de déploiement au reste des services, fonctions et documents de l'organisation devront être menées avec un suivi assuré par le comité de pilotage pluridisciplinaire. Chaque nouvelle implémentation devra faire l'objet d'un audit de conformité initial. Notez qu'outre les coûts de maintenance matériel et logiciel, un SAE entraînera chaque année des frais associés à son audit de conformité.

8. La gestion du SAE

Il reste alors à bien définir comment gérer le système dans le temps, car le SAE a la particularité de devoir conserver ses documents en les gardant lisibles et intègres. Or avec les enregistrements numériques, plusieurs facteurs vont influencer sur cette conservation (format et support des enregistrements, lecteur des supports, pilotes des lecteurs, logiciels, etc.).

De plus, des évolutions réglementaires ou normatives pourraient entraîner un ajustement du SAE, sinon pour la totalité des enregistrements, du moins pour les nouveaux, qu'il convient d'anticiper dès sa conception.

Des migrations nécessaires

Dès que la durée de conservation des archives dépasse 5 ans, l'obsolescence des technologies matérielles et logicielles utilisées dans le SAE va contraindre à faire évoluer le système. Il est donc impératif de prévoir la migration des archives. Les grandes fonctions d'un processus de migration sont identiques, que cette migration soit « interne » (modification des supports, modification de version de logiciels...) ou « externe » au SAE (remplacement d'un ancien SAE par un nouveau).

Un processus de migration des archives doit permettre de réaliser les fonctions suivantes :

- vérification de la bonne lisibilité des archives à migrer dans l'ancienne version du SAE ;
- si ce n'est pas déjà fait dans les métadonnées, calcul d'une information d'intégrité (checksum ou empreinte) ;
- si la nouvelle version du SAE n'est pas capable de coexister avec l'ancienne version, extraction des archives et de leurs métadonnées associées sur un support temporaire ;
- mise en place de la nouvelle version du SAE ;
- si les deux versions coexistent, recopie des archives et de leurs métadonnées depuis l'ancienne version vers la nouvelle version, sinon importation de l'extraction réalisée préalablement ;
- vérification de l'intégrité des archives, par comparaison de l'information d'intégrité ;
- si toutes les archives ont été migrées, désinstallation de l'ancienne version du SAE.

Les questions à se poser lors d'une évolution

Le module Pérennisation du modèle OAIS assure une veille sur tous les aspects de la vie des archives : évolution des normes, obsolescence des matériels et des logiciels, surveillance de la qualité des supports. Lorsqu'il détecte une évolution, il faut se poser les questions suivantes :

- dans quel laps de temps le SAE doit-il évoluer ?
- quelles archives doivent être migrées, compte tenu de leurs durées de conservation ?
- peut-on conserver le même format pour les informations entre l'ancien et le nouveau SAE ?

- comment vérifie-t-on que la totalité des archives retenues a été migrée ?
- comment vérifie-t-on la conservation de l'information entre l'ancien et le nouveau SAE, tout particulièrement si le format de représentation de l'information change ?

Indépendamment des considérations normatives, telles que celles décrites dans la norme NF Z 42-013 ou Iso 14461, il est de bonne pratique de rédiger un dossier de migration présentant les évolutions à réaliser, les méthodes de migration retenues, le contrôle qualité prévu. Il permettra de réfléchir à l'avance sur tous les points, et d'être certain de ne pas oublier un élément important de la migration.

Considérations sur le choix d'un support d'archivage

Le choix d'un support d'archivage se doit d'anticiper les migrations à réaliser, qui seront d'autant plus rapides et économiques si le support peut être lu et écrit rapidement et avec le minimum d'intervention humaine.

Dans cette optique, la bande magnétique, telle que la bande LTO, présente un avantage certain sur les autres supports, car elle permet des vitesses de lecture et d'enregistrement très rapide pour de grandes capacités.

Les disques RAID pourraient présenter des caractéristiques intéressantes, mais il faudra éventuellement, dans le pire des cas, mettre en place deux SAE complets :

- la migration des informations de l'ancien SAE vers le nouveau SAE se fera via un réseau local de débit probablement inférieur à celui des bandes magnétiques d'aujourd'hui ;
- la consommation énergétique de la migration sera très probablement beaucoup plus importante que pour des technologies sur supports amovibles.

Michel Thomas
[consultant expert]

L'administration à l'heure du numérique

13/09/2018

Dématérialisation et valeur probante de la copie numérique

Le développement de la dématérialisation au sein de l'administration pose la question du transfert de la valeur probante de l'écrit sur support papier à sa copie sur support électronique, et, au-delà, de la possibilité d'éliminer l'original une fois numérisé.

Dès 2005, une première instruction est rédigée par les Archives de France sur les modalités de délivrance du visa d'élimination des documents papier transférés sur support numérique ou micrographique (instruction DITN/DPACI/RES/2005/001 du 14 janvier 2005).

Elle est complétée, en 2014, par un outil d'aide à la décision, le vade-mecum intitulé « Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision ? ». Cet outil méthodologique, destiné aux personnes en charge du contrôle scientifique et technique sur les archives publiques, leur permet d'évaluer les projets de dématérialisation portés à leur connaissance et de mesurer les risques de destruction anticipée des documents originaux sur support papier.

Le vade-mecum s'articule désormais avec la norme NF Z42-026 relative à la définition et aux spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations, parue en 2017 (disponible sur la boutique de l'Afnor). Cette nouvelle norme détermine les responsabilités des différents acteurs de la numérisation et définit les mesures qui concourent à la mise en place d'une numérisation « fidèle ». Cette norme s'attache au processus de numérisation ; elle a été conçue en complément à la norme NF Z42-013 (Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes) dont elle est issue. La norme NF Z42-013 permet en effet de définir, une fois la numérisation effectuée, les conditions de conservation de la copie afin de garantir son intégrité et sa pérennité.

L'adoption de ces outils s'est accompagnée en parallèle d'une évolution du droit français. En effet, l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations a modifié l'article 1379 du code civil. Désormais, une copie électronique jugée fiable a la même force probante que l'original, le caractère « fiable » de la copie étant laissé à l'appréciation du juge. Toutefois, la copie est présumée fiable si certaines conditions de reproduction (reproduction à l'identique de la forme et du contenu de l'acte) et de la conservation (intégrité garantie dans le temps) sont remplies.

Le décret n°2016-1673 du 5 décembre 2016, pris en application de l'article 1379, vient préciser les conditions permettant à une copie de bénéficier d'une présomption de fiabilité (test et contrôle de la chaîne de numérisation, conservation de l'empreinte de la copie, etc.)

Les référentiels généraux d'interopérabilité et de sécurité

Le développement de l'administration électronique a donné lieu à plusieurs textes réglementaires qui définissent les pratiques à adopter pour harmoniser, sécuriser et faciliter la mise en place des nouvelles procédures, de façon à rendre cette nouvelle forme d'administration efficace et pérenne.

Ces référentiels ont des implications non négligeables en matière d'archivage électronique.

Référentiel général d'interopérabilité

Le Référentiel général d'interopérabilité (RGI) recommande un certain nombre de standards à même de faciliter le fonctionnement de l'administration française et de ses systèmes d'information. Le référentiel traite notamment du périmètre de l'interopérabilité (trois principaux cas sont ainsi identifiés : échanges entre autorités administratives, entre une autorité administrative et une

entreprise, entre une autorité administrative et un citoyen), ainsi que des différents niveaux d'interopérabilité (politique, juridique, organisationnel, sémantique et technique).

Plutôt que de dresser une simple liste des différents standards recommandés ou en observation, le RGI identifie plusieurs profils d'interopérabilité correspondant à autant de cas d'usage d'intégration. Pour chacun de ces profils, le référentiel spécifie un ensemble de standards et de recommandations. Le profil pour l'archivage numérique établit une distinction entre trois catégories de formats :

- des formats de gestion et d'échange, pour les besoins d'interopérabilité immédiate avec des systèmes d'archivage, comme le Standard d'échange de données pour l'archivage (SEDA) ;
- des formats de diffusion/consultation, utiles pour des besoins à court terme ;
- des formats de conservation, considérés comme une garantie sur le moyen, voire le long terme.

La première version du RGI est parue en mai 2009. La version 2.0, actuellement en vigueur, a été publiée en mai 2016.

Référentiel général de sécurité

Le Référentiel général de sécurité (RGS) est un recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information.

Rédigé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Direction interministérielle du numérique et du système d'information et de communication (DINSIC), il s'adresse aux autorités administratives (DSI, RSSI et chefs de projet) et à leurs prestataires.

Le RGS est destiné à sécuriser les échanges électroniques de la sphère publique, en établissant les exigences de sécurité auxquelles les autorités administratives doivent se conformer pour protéger les données (notamment à caractère personnel) qu'elles exploitent et échangent, à la fois dans les relations qu'elles entretiennent entre elles, mais également avec tout autre organisme ou usager.

La version 2.0 du référentiel, publiée le 24 juin 2014, remplace la première version publiée par arrêté du Premier ministre le 6 mai 2010. C'est une version de transition, en attendant une troisième version prenant en compte la réglementation européenne en cours d'évolution.

La NF Z42-026 est enfin publiée !

Le 09/06/2017

[printer-2178752_1920.jpg](#)



L'application de cette norme permet de supprimer physiquement le support papier.

La Commission de normalisation CN171 vient de publier la nouvelle norme NF Z 42-026 qui couvre la définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations.

Cette norme était particulièrement attendue, car elle fait suite au nouvel article du Code civil 1379 (copie fiable ayant la même force probante que l'original) et au décret N° 2016-1673 du 5 décembre relatif à la fiabilité des copies et pris pour application de ce même article du Code civil.

Qu'apporte-t-elle ?

Elle spécifie les conditions dans lesquelles doivent être numérisés les documents sur support physique afin de permettre une équivalence avec le document d'origine.

À qui s'adresse-t-elle ?

Avant tout, aux prestataires en externalisation et à leurs clients, afin de livrer des fichiers et leurs métadonnées conformes aux exigences d'une copie fiable, et de répondre de ce fait, aux textes réglementaires cités ci-dessus. Elle s'adresse aussi aux service courrier des organisations qui ont pour objectif de supprimer le papier après numérisation. Cette norme est, en effet, applicable en interne comme en externe.

Avec quelles conséquences ?

L'application de cette norme permet de supprimer physiquement le support papier, ce qui se traduira par des économies directes en matière de stockage physique notamment.

Faut-il effectuer des analyses préalables ?

Avant toute chose, chaque organisation a intérêt à analyser ses données au regard de ses processus et de ses risques. Il faut pouvoir spécifier différents niveaux de sensibilité avec les documents à haute sensibilité d'un côté (signature, preuve, engagement, etc.) et les

documents de moindre sensibilité de l'autre. Pour cela, l'organisation aura recours aux indications explicitées dans les normes de records management (ISO 30301, ISO 15489, ISO 26122, ISO 18128)

Un système de records management est-il nécessaire (SGDA) ?

Oui, un référentiel de cycle de vie intégré ou non dans une solution de gouvernance de données est fortement recommandé.

Un système d'archivage électronique est-il nécessaire (SAE) ?

Oui, si la vocation probatoire est recherchée et que les risques sont récurrents et impactants.

Enfin, un coffre fort numérique (CFN) est-il nécessaire ?

Dans certains cas, il l'est, notamment pour répondre à des enjeux de risques élevés ou des enjeux de certaines catégories de données (données personnelles, santé-médicale, etc.). Le CFN peut d'ailleurs être complémentaire à un SAE.

Pierre Fuzeau

Consultant Senior, Serda Conseil

fntc-numerique.com

Avis d'experts « La numérisation fidèle selon la future NF Z42-026 et la destruction des originaux papiers »

COMMUNIQUE DE PRESSE

Paris, le 20 avril 2017

**NUMERISATION FIDELE ET DESTRUCTION
DES ORIGINAUX PAPIERS, C'EST PARTI !
www.fntc-numerique.com**

Après avoir été soumise à enquête publique par l'AFNOR, une nouvelle norme relative à la numérisation fidèle devrait voir le jour dans les semaines à venir, elle a été présentée aujourd'hui par les experts de la Fédération des Tiers de Confiance du Numérique (FNTC). Cette norme NFZ42-026 constituera un référentiel permettant de concevoir, auditer et certifier des systèmes dont les objectifs seront d'apporter les garanties nécessaires pour envisager la destruction des originaux papiers et de permettre la production de copies numérisées fidèles.

Face au développement exponentiel de la digitalisation des processus documentaires au sein des entreprises, collectivités et administrations, et des évolutions législatives, il devient nécessaire de faire évoluer le cadre normatif lié à ces pratiques. Cette norme permettra de guider les utilisateurs dans la mise en œuvre de leurs solutions de numérisation en formalisant les bonnes pratiques en terme de fiabilité de la copie.

LA DESTRUCTION DES ORIGINAUX PAPIERS

Dans le prolongement du Décret du 5 décembre 2016 pris en application de l'article 1379 du Code civil, il est à noter qu'un arrêté du 22 mars 2017 fixe les modalités de numérisation des factures papiers des entreprises à destination de l'administration fiscale, ce qui prouve bien, précise Alain Borghesi, vice-président de la FNTC que : « *la démarche du groupe de travail de la FNTC, à l'origine de ce projet, va dans le sens d'une nécessité de sécurisation dans la production de données fiables mais aussi des évolutions législatives, des besoins exprimés par le marché et des initiatives législatives et réglementaires* ».

La numérisation des documents papier permet une meilleure accessibilité à leur contenu et accroît, par l'emploi de systèmes conformes, la sécurité de la conservation de l'information (intégrité, confidentialité, disponibilité et pérennité). Dès lors, l'opportunité de s'affranchir d'une double conservation (document d'origine et copie numérique fidèle) se pose. Ce sujet s'inscrit dans une tendance Européenne amorcée depuis plusieurs années, et la norme NF Z42-026 sur la numérisation fidèle, permettra de disposer d'une référence notamment concernant les exigences de qualification des procédés, de conservation, d'intégrité et de sécurité.

Parallèlement, selon le décret du 5 décembre 2016 six points doivent être respectés pour la reproduction par voie électronique :

- Les **informations relatives à la copie**, son contexte et son identification (art. 2) ;
- Les conditions entourant **l'intégrité de la copie** (horodatage, cachet ou signature électroniques qualifiés au sens du Règlement eIDAS) (art. 3) ;
- Les modalités de **conservation des copies (art. 4)**
- La **conservation des empreintes numérique (art. 5)**
- Les conditions de **sécurité du procédé** (art.6).
- La **documentation** des dispositifs et mesures (art. 7) ;

L'article 1379 du Code civil et le décret du 5 décembre 2016 ne précisent pas explicitement la possibilité de la destruction des originaux papiers. Cependant, le fait d'introduire le texte par « *La copie fiable a la même force probante que l'original.* » suffit à répondre au besoin de disposer d'une sécurité juridique de la copie numérique équivalente à celle portée par l'original.

La prise de risque sur la destruction des originaux papiers est en conséquence considérablement limitée, notamment si les procédés de numérisation sont conformes à la norme NFZ 42-026. Par ailleurs, l'ordonnance du 12 janvier 2017 relative aux documents

comportant des données de santé à caractère personnel fait explicitement référence à la destruction de l'original papier.

Nouvelle norme NFZ42-026, comment ça marche...

La norme identifie les quatre **cas d'usages** couvrant la plupart des configurations de numérisation qu'elle soit externalisée ou réalisée dans une organisation. Les cas d'usage sont déterminés selon deux critères :

- numérisation de **stocks** d'archives ou de **flux**, par exemple de courrier entrant ;
- numérisation **centralisée** dans un atelier de numérisation ou **décentralisée**, par exemple avec une station de numérisation au guichet.

Les principales thématiques d'exigences à mettre en œuvre concernent :

- la **qualification** du processus et des outils de numérisation : il s'agit de tester les capacités de chaque outil mis en œuvre dans la chaîne de numérisation pour identifier à partir de quels seuils il existe un risque sur la fidélité : résolution, colorimétrie, méthode de suppression de pages blanches, détection de doublons, ... Pour chaque typologie de documents, des échantillons représentatifs doivent être numérisés pour valider que les profils paramétrés sont conformes aux exigences de fidélité.
- la mise en œuvre d'une **chaîne de traçabilité**: il s'agit d'enregistrer chaque opération du processus de numérisation (préparation, numérisation, traitements post numérisation, contrôle, ...) de manière à pouvoir démontrer que la numérisation a été réalisée conformément à la **convention de numérisation** établi avec le propriétaire des documents.
- Les moyens techniques pour la **préservation de l'intégrité** et notamment les marques d'intégrité et de temps (empreinte numérique, horodatage, cachet électronique, ...) de chaque document afin de garantir qu'il n'y a aucune perte d'intégrité des documents entre les opérations de numérisation et d'archivage.
- la **production de livrables** vers un système d'archivage électronique (SAE) dans lesquels seront conservées les copies fidèles. Il s'agit d'un format d'interopérabilité permettant de transférer les copies numériques, les métadonnées produites et les marques d'intégrité et de temps.

La norme propose une option:

- la **numérisation fidèle** consistant à fournir les métadonnées techniques relatives à l'intégrité au système de destination.

Et une recommandation de produire des attestations de numérisation :

- la **numérisation fidèle attestée** consistant à produire une attestation de numérisation comportant tous les éléments de traçabilité de la chaîne de numérisation. Il s'agit d'un moyen de « portabilité » de la journalisation et des éléments de preuve qui permettront de démontrer que le procédé de numérisation a été respecté.

La numérisation attestée permet notamment de récupérer les éléments de preuve lorsqu'une prestation de numérisation est externalisée ou de renforcer la sécurité sur la fidélité de la copie, notamment s'il s'agit, par la suite, de détruire un original sensible, par exemple un contrat signé

FNTC (www.fntc-numerique.com). *La Fédération des Tiers de Confiance du Numérique, créée en 2001 par un ensemble de professionnels réglementés et de prestataires de services, regroupe 130 acteurs Français et étrangers qui entendent prendre une part active dans la mise en œuvre et la promotion de la Confiance dans l'Economie Numérique. Son action s'articule autour de trois missions : construire la confiance dans le numérique de demain ; promouvoir les techniques et méthodes pour garantir la confiance dans le numérique et favoriser la connaissance des meilleures pratiques ; accompagner les institutions publiques.*