

L'archiviste, les normes et le droit

Antoine Meissonnier, Rémy Roques

Citer ce document / Cite this document :

Meissonnier Antoine, Roques Rémy. L'archiviste, les normes et le droit. In: La Gazette des archives, n°240, 2015-4. Voyages extraordinairement numériques : 10 ans d'archivage électronique, et demain? pp. 135-151;

doi : 10.3406/gazar.2015.5290

http://www.persee.fr/doc/gazar_0016-5522_2015_num_240_4_5290

Document généré le 01/02/2018

L'archiviste, les normes et le droit

Antoine MEISSONNIER

Rémy ROQUES

Introduction

Depuis les premières réflexions du *Consultative Committee for Space Data Systems*, auteur en 2002 de la recommandation connue ensuite sous le nom d'OAIS¹, et la publication de la première version de la norme NF Z 42 013 en 1999, les normes et standards visant à définir les fonctions d'un système d'archivage électronique se sont développés et améliorés. Ils se sont aussi multipliés au point de devenir un élément de complexité, au même titre que la technique informatique, et de déconcerter les archivistes qui se lancent dans un projet d'archivage électronique. Aujourd'hui, pas moins de soixante normes traitent de l'archivage électronique et du *records management*. Ces textes, auxquels s'ajoutent des guides d'application² ou d'auto-évaluation, évoluent au rythme des révisions, afin de s'adapter aux besoins des différents acteurs du marché.

La multiplication des normes pose d'autant plus question que l'archiviste a besoin de se positionner clairement par rapport à une offre logicielle protéiforme (gestion électronique de courrier ou de documents, *enterprise content management*, *electronic document management system*, système d'archivage électronique, etc.). Au sein de cette galaxie d'outils, on peut définir simplement un système d'archivage électronique comme un ensemble de ressources humaines, techniques et logicielles permettant de collecter des documents électroniques (natifs ou issus d'une numérisation) et de garantir, tout au long d'un cycle de vie défini en amont, leurs accessibilité, fidélité, intégrité et traçabilité.

¹ Les normes citées dans cet article sont développées en annexe.

² Par exemple, le GA Z 42 019, guide d'application de la NF Z 42-013.

Notre article s'emploiera à dresser une catégorisation des principales normes et standards en usage en France, mais aussi de ceux, moins connus, employés chez nos proches voisins européens. Au-delà de donner des repères au lecteur et lui faire connaître les outils existants, il établira le bilan de l'intégration de ces normes dans le droit français.

Un état des lieux normatif

Malgré leur foisonnement, les normes peuvent être réparties en deux domaines : les normes techniques, d'une part, et les normes fonctionnelles, d'autre part. Au sein de la seconde catégorie, qui fait l'objet d'une attention particulière dans les pages suivantes, peuvent être distinguées les normes ayant pour objet le *records management*, celles plus spécifiquement consacrées à la pérennisation des informations électroniques et, enfin, celles davantage centrées sur l'intégrité des données.

Avant d'entrer dans le vif du sujet, le lecteur ne doit pas perdre de vue que si les normes applicables aux archives utilisent parfois des concepts et un vocabulaire non harmonisés, c'est en partie parce que ces textes sont le résultat de consensus plus ou moins larges ainsi que d'enjeux commerciaux, financiers et de pouvoir.

Les normes consacrées au records management

La norme ISO 15 489 a suscité bien des commentaires, articles et ouvrages¹. Actuellement en cours de révision², le texte, dans sa version initiale, a été pensé comme un guide pour l'organisation et la gestion des documents (hors archives historiques pour la version française de 2001³). Il définit des bonnes pratiques en matière de *records management*, précisé comme un champ d'organisation et de

¹ Au sein d'un océan bibliographique, on peut retenir : ROBERGE (Michel), *L'essentiel du records management : système intégré de gestion des documents analogiques et des documents numériques*, Québec, Gestar, 2004 ; SHEPHERD (Elisabeth) et YEO (Geoffrey), *Managing record : a handbook of principles and practices*, Londres, Facet publishing, 2006 ; *La Gazette des archives*, n° 228 « Normalisation et gestion des documents d'activité (*records management*) : enjeux et nouvelles pratiques pour notre profession », octobre 2012, Association des archivistes français, Paris.

² Le nouveau texte de la norme ISO 15 489 sera publié courant 2016.

³ ISO 15 489, note 1, p. 1.

contrôle de la production documentaire, en relation avec l'environnement réglementaire et les besoins de traçabilité et d'authenticité des documents. Le *records management* se focalise sur une partie de l'ensemble de la production documentaire, en déterminant les documents à risques et en leur appliquant des exigences de traitement élevées.

Ces principes s'appliquent aussi bien à l'électronique qu'au papier. L'expérience démontre que la mise en place d'un système d'archivage électronique (SAE) n'induit pas la disparition du papier. Bien au contraire, la dématérialisation amène souvent à penser l'organisation de dossiers hybrides¹. La norme ISO 15 489 retient quatre caractéristiques que devrait posséder tout système d'archivage, à savoir :

- la fiabilité, c'est-à-dire la protection des documents et de leurs métadonnées intégrés dans le système contre toute modification ou élimination abusive ;
- l'intégrité, qui repose sur le contrôle de la circulation et de l'accès aux documents *via* la gestion des droits d'accès et l'identité des utilisateurs ;
- le respect de l'environnement réglementaire, interne et externe, dans lequel évolue l'organisation ;
- et le traitement complet et systématique des documents dès leur création ou leur réception par l'organisation (identification, classement, détermination du délai de conservation et du sort final du dossier).

Plusieurs textes découlent de l'ISO 15 489 : les normes de management ISO 30 300² et ISO 30 301, centrées sur les systèmes de gestion des documents, l'ISO 26 122, sur la description des processus métiers, ou encore l'ISO 23 081 « Métadonnées pour les *records* ». Dans le contexte électronique, les normes et standards ICA-Req, d'origine australienne, et MoReq2010, dont la Commission européenne est à l'initiative, ou encore le DOMEA-Concept relèvent bien d'une démarche de *records management* compte-tenu de leur attachement à la prise en compte des processus métiers de création de l'information dans leur approche de l'archivage électronique, au détriment

¹ Dans le cadre du projet de dématérialisation des documents des ressources humaines mené à La Poste, il a été nécessaire de penser l'articulation entre le dossier papier et le dossier électronique de l'agent (consultable dans le SAE), dont les périmètres ne sont pas exactement les mêmes. Un outil de suivi, dont les fonctionnalités sont directement accessibles aux utilisateurs habilités *via* le SAE, permet de tracer les mouvements de documents physiques.

² COTTIN (Michel), DUPOIRIER (Gérard) et NESME (Marie-Françoise), « Gestion des enregistrements : norme ISO 30300 - Objectifs, moyens et méthode - Historique du *records management* », publié le 10 mai 2014 sur le site techniques-ingenieur.fr.

d'une réponse précise aux enjeux des deux autres domaines que nous allons voir.

Ces normes ont été pensées pour aider une maîtrise d'ouvrage dans la conduite d'un projet d'archivage en rappelant les fonctionnalités essentielles d'un système d'archivage et en donnant des clés pour obtenir l'adhésion des décideurs et des utilisateurs.

Les normes consacrées à la pérennisation de l'information

La référence dans ce domaine reste l'OAIS, devenu une norme internationale en 2003 (ISO 14 721) et sur lequel s'appuient d'autres textes comme le référentiel général d'interopérabilité pour les systèmes d'archivage électronique, PAIMAS (ISO 20 652) et la norme d'audit ISO 16 363. Très théorique, l'OAIS définit les fonctions, responsabilités et organisation d'un système d'archivage électronique¹. Élaboré dans le cadre spatial, ce modèle privilégie les données (le contenu) plutôt que le processus générateur des documents et leur mode d'utilisation. Il se focalise sur le transfert des données dans un SAE et leur conservation sur le long terme dans celui-ci. S'il peut laisser supposer que l'archivage se limite à ces procédures, il permet de comprendre le rôle de chaque fonction d'un SAE dans la pérennisation de l'information. Il propose également une modélisation de l'information numérique qui permet d'identifier les difficultés de sa pérennisation et le rôle des différentes couches de normalisation technique.

La normalisation dans le domaine de la pérennisation sur le long terme reste assez peu développée. Elle s'accorde en effet peu avec les priorités politiques (cyber sécurité, lutte contre les fraudes, confiance dans l'économie numérique) et au temps du décideur, de plus en plus court, en attente d'un retour rapide sur investissements. On peut noter la publication récente de la norme ISO 13 008 abordant la question de la conversion de format à des fins de pérennisation.

À l'heure actuelle, il n'existe pas de solution unique en matière de pérennisation. Et les solutions existantes ont leurs inconvénients. Longtemps présenté comme le format d'archivage à long terme, le PDF/A (ISO 19 005-1)

¹ Sur les impacts de l'OAIS dans un service d'archives, en particulier en matière d'organisation et de compétences requises, voir HUC (Claude), « Un modèle pour l'organisation d'un centre d'archives numériques », *Document numérique*, n° 2/2004 (vol. 8), p. 87-100.

pose quelques problèmes¹. Le consensus n'est pas encore fait : l'ETSI TS 102 573 n'hésite pas à mettre en avant la nécessaire conservation des logiciels et des infrastructures, quand la norme ISO 13 008 recommande en priorité les migrations de format.

Les normes consacrées à l'intégrité de l'information

Les normes fonctionnelles d'archivage électronique centrées sur la question de la conservation de l'intégrité de l'information numérique sont parmi les plus nombreuses. Contrairement aux normes de pérennisation, elles sont au cœur d'enjeux qui dépassent le strict milieu des archivistes.

Plus encore que les normes rattachées aux deux autres domaines de notre classification, celles relatives à la conservation de l'intégrité de l'information numérique ne s'accordent pas sur les fonctionnalités nécessaires à une telle garantie. Sans parler d'opposition radicale, on peut distinguer deux approches divergentes.

Il y a tout d'abord la position promue par les normes françaises NF Z 42 013 et NF Z 42 020, la plus répandue chez les professionnels français de l'archivage électronique, tant privés que publics : elle consiste à faire porter la charge de la preuve de l'intégrité de données électroniques sur le fonctionnement du SAE qui les contient :

- soit en s'appuyant sur un système ou des supports WORM² ;
- soit en créant, tout au long du fonctionnement du système et du cycle de vie des archives qui y sont conservées, un faisceau de preuves permettant de démontrer, au moment voulu, qu'elles sont intègres³.

Ce dernier principe, le plus communément implémenté dans les solutions logicielles d'archivage électronique du marché français¹, est la journalisation,

¹ BRUNETON (Sophie), « La conversion en PDF/A prise en défaut », *La Gazette des archives*, n° 223, Association des archivistes français, Paris, 2011, p. 85-87 et les études du Service interministériel des Archives de France sur les formats pdf : <http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques/formats-et-supports/>.

² *Write Once, Read Many* : se dit d'un système d'enregistrement de l'information numérique autorisant une seule écriture de l'information et empêchant ensuite toute modification. On distingue le WORM physique (CD-Rom non réinscriptible par exemple) du WORM logique (dispositif logiciel pilotant le support et offrant les mêmes garanties). Voir NF Z 42 013, § 7.3. et 8.

³ NF Z 42 013, § 5.6.

c'est-à-dire l'enregistrement automatique par le système de tous les événements survenus en son sein. Habituelle dans le cadre d'une politique de sécurité des systèmes d'information², la journalisation recommandée par la norme NF Z 42 013 se distingue par la tenue de deux journaux : le journal du cycle de vie des archives, qui liste tout événement survenu sur les archives, et celui des événements, plus commun dans les systèmes d'information, qui conservent la trace des logs techniques, d'accès, d'erreurs, etc. Chaque ligne du journal identifie par une empreinte l'objet archivé touché par l'action enregistrée³. Les journaux sont ensuite horodatés au minimum une fois par jour.

Une autre position apparaît dans plusieurs normes de l'*European Telecommunications Standards Institute* (ETSI)⁴, dont la mise en œuvre pratique semble rester encore rare : il s'agit de faire de tout objet archivé un « artefact auto-porteur » capable de prouver son intégrité seul, moyennant le recours à la cryptographie. L'idée est de signer électroniquement – ou au moins d'horodater – chaque état de l'objet archivé pour attester de son intégrité, que l'objet archivé ait été ou non signé électroniquement au moment de sa validation⁵. Comme toute la charge de la preuve porte sur ce dispositif et non sur un faisceau de preuves, il devient indispensable de procéder au renouvellement régulier des signatures et des horodatages dès que l'algorithme de chiffrement ou de hachage les ayant créés devient obsolète⁶. Enfin, il est recommandé que les signatures électroniques à conserver sur le long terme soient complétées par l'adjonction de métadonnées qui peuvent se révéler assez lourdes, comme la *Certificate Revocation List* de l'autorité de certification⁷. Si le gain de sécurité apporté par une telle solution est réel, la nécessité pour le SAE

¹ On retrouve une approche similaire dans la *Règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC)*, établie en 2014 par l'organisme de normalisation luxembourgeois, l'ILNAS.

² Note d'information DGP/SIAF/2014/005 du 8 juillet 2014 relative à la journalisation des événements et la note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013 portant recommandations de sécurité pour la mise en œuvre d'un système de journalisation.

³ NF Z 42 013, § 5.3.3.

⁴ L'ETSI s'est notamment vu confié la charge de la révision des normes nécessaires à la mise en œuvre du règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui abroge la directive 1999/93/CE relative à la signature électronique sur lequel nous reviendrons.

⁵ ETSI TS 101 533-1, § 6.1. et ETSI TS 102 573, annexe A, § SS 2. et SS 3.2. Le programme allemand TransiDoc initié en 2005 avait abouti à des conclusions similaires.

⁶ ETSI TS 101 533-1, § 6.3.2. La re-signature est aussi l'esprit de la norme allemande BSI TR 03 125.

⁷ ETSI TS 101 733, annexe B, § B.3A.

d'avoir recours à une infrastructure de gestion de clés pose question quant à son coût et sa pérennité dans le temps¹.

Les normes de ces deux approches traitent, suivant leurs exigences respectives, de la question de l'intégrité de copies électroniques issues de la numérisation de documents sur support papier².

Enfin, la préservation de l'intégrité de l'information numérique est un domaine dans lequel l'archiviste doit s'attendre à côtoyer des pratiques professionnelles issues de la sécurité des systèmes d'information dont les normes, et notamment la série des ISO 27 000, connaissent un succès grandissant³. Il s'agit certes initialement de normes de management de système, c'est-à-dire créant une organisation censée garantir la qualité des processus, plus que mettant en place telle ou telle fonctionnalité ou technologie. Mais certaines des normes apparentées à cette série sont venues donner des recommandations plus précises, comme la norme ISO/IEC 27 002. En garantissant un système d'information dans lequel n'entrent que des gens autorisés⁴ et qui ne perd pas de données, la sécurité des systèmes d'information est un fondement essentiel de l'archivage électronique que l'archiviste a intérêt à promouvoir tout en sachant expliquer ses limites par rapport à une politique d'archivage électronique.

L'archiviste et les normes

Mieux vaut inciter les archivistes à appréhender ces textes sereinement en rappelant la diversité possible de leurs mises en œuvre. L'idée n'est pas de connaître parfaitement toutes les normes, mais de savoir s'y référer sans se départir de son bon sens et de son esprit critique. À un niveau opérationnel, les

¹ Il est à noter qu'en Allemagne la publication en 2011 de la nouvelle version de la norme BSI TR 03 125 a suscité des débats animés. Voir KAMPPMEYER (Ulrich) et WASNIEWSKI (Agnieszka), *Von TR-03125 über TR-VELS zu TR-ESOR*, note de la société Project consult, 2011.

² NF Z 42 013, § 5.3.1. et 10.2. à 4., et ETSI TS 101 533-1, § 6.5. Abordant ce sujet, les rapports techniques ISO/TR 15 801 et 22 957 s'en tiennent à des conseils trop peu contraignants pour aider à faire émerger le meilleur usage en matière de garantie de la fiabilité d'une copie électronique issue d'un processus de numérisation. Dans ce genre, on préférera l'ISO/TR 13 028 qui intègre des tableaux d'audit d'un projet de numérisation ainsi que des exigences techniques précises.

³ On retrouvera des références à ces normes dans la NF Z 42 013. L'ETSI TS 101 533-1 est quant à elle simplement vue comme un module complémentaire de la norme ISO 27001.

⁴ Voir par exemple la norme ISO/IEC 29 115 sur l'identification des entités pour les transactions entre applications, norme sur laquelle sont fondés les niveaux d'identification du règlement eIDAS.

normes signalées ci-après nous semblent adaptées pour répondre aux usages suivants :

- pour préparer un projet de numérisation de flux quotidiens de documents courants : NF Z 42 013 et ISO 13028¹ ;
- pour penser l'ergonomie et l'usage de son SAE : ICA-Req (pour commencer), MoReq2010 (niveau plus avancé) ;
- pour la pérennisation à long terme : OAIS ;
- pour garantir l'intégrité des documents archivés, en fonction des obligations légales : dans le contexte français, la NF Z 42 013 et la NF Z 42 020 ;
- pour construire un cahier des charges ou une grille d'audit d'un SAE : ICA-Req/MoReq2010 et NF Z 42 013².

Il faut aussi oser s'affranchir des normes fonctionnelles, tout en s'en inspirant, et se lancer dans un projet d'archivage en s'appuyant sur sa réflexion issue des expériences et une pratique de terrain. La gestion des archives électroniques est avant tout un projet de gestion documentaire, dont les étapes restent les mêmes :

- analyse des processus métier et recueil des besoins des utilisateurs ;
- définition d'un périmètre documentaire et sélection des métadonnées de contenu, de contexte et de gestion pertinentes et pérennes ;
- étude de faisabilité, soutenabilité et réversibilité du projet ;
- prise en compte de l'environnement réglementaire, permettant de fixer les durées de conservation, les sorts finaux (conservation illimitée ou élimination) et les droits d'accès ;
- élaboration d'une procédure documentaire, fixant les règles de création et le circuit des documents, les points de collecte, les règles de nommage, de référencement et de classement ;
- définition de la responsabilité des acteurs et des règles de sécurité.

¹ Voir également SIAF, *Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision ? Vade-mecum*, 2014.

² Voir les grilles d'audit des SAE réalisées par le Service interministériel des Archives de France (<http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques/plates-formes/> et <http://www.archivesdefrance.culture.gouv.fr/static/7440>).

Enfin, « le SAE est un composant du système d'information de l'entreprise [ou de l'administration], dédié à la gestion des archives électroniques »¹, l'archiviste, comme composante de cet ensemble de ressources humaines, techniques et logicielles, a une carte à jouer dans la coordination des activités de son organisation, à condition de penser l'archivage comme une stratégie et les normes comme des leviers, non comme des contraintes.

En France, cette profusion normative n'a pas encore trouvé d'aboutissement légal ou réglementaire de portée générale. En règle générale, le droit positif français en est resté à définir les exigences techniques nécessaires à la validation d'un acte.

Les normes et le droit

Pour faire son choix parmi les nombreuses exigences portées par les normes en matière d'archivage électronique, un point de repère sûr est le droit en ce qu'il traduit les règles que la société estime nécessaire de s'imposer à elle-même à un moment donné pour fonctionner correctement. Or, sans obligation légale ou réglementaire, l'application des normes ne fait en soi l'objet d'aucune contrainte pour les acteurs.

La validation des documents : un domaine fortement encadré par le droit

Ce que la loi est venue encadrer précisément dans le domaine de la gestion de l'information numérique, ce sont les conditions de sa validation. Et encore, il faut avoir à l'esprit que cet encadrement ne concerne qu'un nombre limité de documents numériques et de technologies.

D'une part, la loi n° 2000-230 du 13 mars 2000 est venue modifier sans ambiguïté le Code civil pour spécifier les conditions de validation d'un acte juridique électronique² pour qu'il soit recevable à titre de preuve devant un tribunal. Cette validation doit passer par un dispositif de signature électronique tel que défini dans l'article 1316-4 du même Code, article dont il faut toutefois souligner les limites :

¹ GA Z 42 019 (guide d'application de la NF Z 42 013), p. 12.

² Un acte juridique est en effet une manifestation intentionnelle qui traduit la volonté d'une personne de réaliser certains effets de droit (vente, legs, don, contrat, etc.).

- les conditions de validation ne concernent que les actes juridiques en droit civil, soumis au régime de la preuve légale, et non les faits juridiques¹, pour lesquels la preuve reste libre, ce qui explique des jurisprudences récentes acceptant à titre de preuve des courriels non signés électroniquement². Dans les domaines du droit autres que civil, la preuve est également libre ;

- les exigences techniques fixées par le décret n° 2001-272 du 30 mars 2001 pris en application de l'article 1316-4 du Code civil n'encadrent que les dispositifs de signature électronique sécurisée tels que définis par le décret précité³.

D'autre part, les dispositions du Code des relations entre le public et l'administration (CRPA) tendent à rendre obligatoire la signature électronique conforme au référentiel général de sécurité (RGS) des actes administratifs⁴. Certes, ces documents relèvent du droit administratif où le régime de la preuve est libre. Néanmoins, l'article L212-1 du CRPA prévoit que « toute décision prise par une administration comporte la signature de son auteur ainsi que la mention, en caractères lisibles, du prénom, du nom et de la qualité de celui-ci ». Il n'est pas dit qu'en contexte électronique cette signature doit être une signature électronique conforme à l'état de l'art, mais le juge peut être amené à le penser⁵. Or, l'article L212-3 du CRPA indique que les autorités administratives peuvent signer électroniquement leurs actes. Si elles le font, cette signature doit être conforme aux préconisations du RGS.

En outre, même si le régime de la preuve est libre en droit administratif, le juge administratif a tendance à s'appuyer également sur les articles 1316-1 et suivants du Code civil pour étayer sa décision de recevoir un document

¹ Un fait juridique est un événement, volontaire ou non, susceptible de produire des effets juridiques, non du fait d'individus, mais du fait de dispositions légales (accidents, etc.).

² Voir l'arrêt n° 12-16.839 de la Cour de cassation, Chambre civile, 13 février 2014 et l'arrêt n° 11-25.884 de la Cour de cassation, Chambre sociale, 25 septembre 2013.

³ Les autres signatures électroniques, dites parfois « simples », ne sont définies que comme une « donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification » (directive 1999/93/CE, art. 2.1.) ou encore « un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache » (Code civil, art. 1316-4).

⁴ Voir la définition de ce concept donnée par le Code des relations entre le public et l'administration à son art. L200-1.

⁵ Nous avons eu connaissance d'un jugement de ce type concernant un système de gestion des ressources humaines dématérialisé. Les arrêtés de décision individuelle étaient produits sous forme numérique, sans signature électronique. Or le juge a rejeté l'arrêté produit par l'administration en s'appuyant sur l'article 4 de la loi du 12 avril 2000, ancêtre de l'article L212-1 du CRPA.

électronique à titre de preuve, au-delà des décisions des autorités administratives *stricto sensu*. Il peut en venir à considérer que, si le document est électronique et devait être signé d'après une disposition légale ou réglementaire, on ne peut lui présenter à titre de preuve qu'un document revêtu d'une signature électronique conforme à l'état de l'art. Un tel raisonnement empêche notamment toute production en justice d'un document scanné revêtu uniquement de la signature manuscrite de son auteur¹.

L'archivage électronique : un cadre juridique difficile à établir

Mais, passées ces exigences techniques de validation de certains documents, le droit positif français ne dit rien des conditions de conservation des documents. Tout juste est-il dit dans l'article 1316-1 du Code civil qu'un écrit électronique a une valeur probante s'il est conservé « dans des conditions de nature à en garantir l'intégrité² ». En droit administratif, le RGS, au demeurant très précis, n'impose pas de règle d'archivage électronique conforme à l'état de l'art³.

Le livre II du Code du patrimoine est encore le seul texte juridique français à porter un dispositif favorisant de manière large l'archivage électronique conforme à l'état de l'art, au travers de l'agrément des prestataires de conservation externalisée d'archives publiques électroniques⁴. L'arrêté du 4 décembre 2009 qui fixe le cadre technique de cet agrément fait référence aux normes ISO 14 721 et NF Z 42 013. Malgré des dispositions réglementaires prometteuses⁵, l'agrément des hébergeurs de données de santé n'aborde en réalité que des exigences de sécurité des systèmes d'information.

Cela ne signifie pas pour autant que l'archivage électronique n'a, au regard du droit, qu'un intérêt limité aux cas réellement réglementés. Malgré le flou de sa définition, les archivistes peuvent d'ores et déjà valoriser l'utilité de l'archivage

¹ Décision n° 351931 du Conseil d'État, 17 juillet 2013, § 5 et jugement de la Cour d'appel de Fort-de-France n°12/00311 du 14 décembre 2012.

² Des textes catégoriels reviennent sur cette notion de conservation de l'intégrité mais sans jamais en définir techniquement les exigences : Code de la santé publique, art. R2151-11 ; Code du travail, art. L3243-2, D3313-9, D3323-16, D3334-3-1 ; Livre des procédures fiscales, art. A13 F-1, A47 A-3 ; Code de procédure civile, art. 729-1, 456, etc.

³ Des travaux sur l'archivage électronique sécurisé ont néanmoins été menés en 2006 par les Archives de France et l'ANSSI, mais il s'agit de simples recommandations : <http://www.ssi.gouv.fr/administration/guide/archivage-electronique-comment-le-securiser/>.

⁴ Code du patrimoine, art. L212-4 et R212-19 à 31, arrêté du 4 décembre 2009 précisant les normes relatives aux prestations en archivage et gestion externalisée.

⁵ Code de la santé publique, art. R1111-14, 3°.

électronique pour constituer un faisceau de preuves à même d'emporter la conviction du juge dans tous les cas où le régime de la preuve est libre, notamment pour prouver la conservation de l'intégrité du document conformément aux exigences de l'article 1316-1 du Code civil¹. Pour fonder son jugement et apprécier la fiabilité d'un système, le magistrat pourra s'appuyer sur des normes techniques qui, même si elles ne sont pas obligatoires, peuvent constituer un indice dans la mesure où elles reflètent un certain « état de l'art »². Sans faire de référence à l'archivage électronique, une jurisprudence du Conseil d'État en date du 31 mars 2008 met en exergue l'importance de l'analyse de processus et de la traçabilité dans l'administration de la preuve, en l'absence de toute signature électronique³.

La fin des années 2010 : la maturité juridique de l'archivage électronique ?

On sent monter aujourd'hui le besoin juridique de définir plus clairement l'archivage électronique en droit. L'évolution se fait sans portée générale, compte-tenu des difficultés énoncées plus haut, mais en s'appuyant sur des besoins précis.

En premier lieu, le besoin juridique d'archivage électronique s'affirme en lien avec la question du maintien de l'intégrité d'un document sur le long terme, en particulier quand il est signé. Successeur de la directive n° 1999/93/CE du 13 décembre 1999 à l'origine de la loi du 13 mars 2000, le règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit « eIDAS », introduit, dans son article 34, l'enjeu de la pérennisation de la signature électronique, notamment au-delà de la durée de validité du certificat du signataire. Un acte d'exécution fixant des exigences techniques est envisagé à son second alinéa, mais reste facultatif. Compte-tenu des différences de points de vue en matière de conservation de l'intégrité des documents électroniques, l'enjeu est fort pour savoir vers quel principe normatif l'Union européenne va se tourner.

Un deuxième enjeu pousse les acteurs publics comme privés à s'intéresser à l'archivage électronique : il s'agit de définir les conditions dans lesquelles une

¹ Arrêt de la Cour de cassation, Chambre civile, du 4 décembre 2008, n° 07-17.622.

² Une jurisprudence récente est venue reconnaître la pertinence d'un archivage électronique conforme à la NF Z 42013 pour ce faire (jugement de la Cour d'appel de Lyon n°13/09407 du 3 septembre 2015).

³ Décision n° 311095 du Conseil d'État, 31 mars 2008.

copie numérique d'un document papier peut avoir la même force probante que l'original. Le Service interministériel des Archives de France a évalué ce qu'il était possible de faire à droit constant, mais l'évaluation du risque juridique reste complexe dans le cadre actuel. La fixation en droit de ces conditions est attendue : elle a déjà fait l'objet d'un rapport de l'APROGED¹, tandis que la CN171 de l'AFNOR mène des travaux autour de la notion de « copie fidèle ». La volonté de progresser rapidement sur ce sujet s'est déjà traduite dans la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Son article 204 habilite le gouvernement à légiférer par ordonnance pour fixer les conditions de destruction anticipée des dossiers de patient après leur numérisation. Comme la demande dépasse le secteur de la santé et que le cadre technique, pour cet usage précis, devrait être identique dans tous les domaines d'activités, il existe un besoin fort de coordination qu'une modification du Code civil devrait porter².

Enfin, certains secteurs d'activité à fort enjeu de pérennisation et d'intégrité des données voient dans l'archivage électronique un moyen de sécuriser la dématérialisation en marche. Le ministère de la Justice avait ainsi fixé les normes ISO 14 721 et NF Z 42 013 comme cadre de référence réglementaire de l'archivage électronique des documents électroniques signés de la procédure pénale les normes ISO 14 721 et NF Z 42 013³. La réalisation concrète est encore en attente de la dématérialisation complète de la chaîne pénale.

¹ Groupe de travail ElimDoc, *Proposition pour l'évolution du cadre réglementaire*, APROGED, décembre 2014.

² L'article 1348 du Code civil, communément cité dans le contexte de la dématérialisation, affirme qu'est recevable à titre de preuve, en cas de perte de l'acte original, « une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support ». Cet article ne concernait pas initialement l'électronique, mais la micrographie (voir Sénat, *Rapport sur le projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique*, Charles Jolibois (rapporteur), rapport n° 203, Commission des lois, 1999-2000 [en ligne : <http://www.senat.fr/rap/199-203/199-2035.html#toc32>]). Mais l'ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations va modifier cet article à partir du 1^{er} octobre 2016 pour reconnaître clairement la valeur probante de toute copie fiable dans un nouvel article 1379.

³ Code de procédure pénale, art. A53-6.

Conclusion

L'archiviste a la chance de bénéficier d'un *corpus* important de normes qui peuvent lui faire gagner du temps dans un projet d'archivage électronique en lui permettant de s'approprier l'expérience de ses pairs. Cependant, il ne doit pas considérer qu'il lui est indispensable d'en maîtriser toutes les arcanes avant de se lancer dans un projet et ce, d'autant plus que les normes fonctionnelles dans ce domaine ont eu des approches diverses et qu'aucune n'a couvert complètement l'étendue des fonctions théoriques d'un SAE. Le droit s'en ressent et avance prudemment dans la définition d'exigences réglementaires fondées sur des normes fonctionnelles d'archivage électronique.

L'archiviste doit donc garder un esprit critique face aux normes fonctionnelles¹. La norme est un idéal ; le SAE, une réalité technique et fonctionnelle. En fin de compte, ce qui comptera sera l'ergonomie de l'outil, son adéquation avec les besoins de l'organisation, sa soutenabilité et sa réversibilité. La question pour l'archiviste n'est donc pas de catégoriser *a priori* les logiciels suivant leur dénomination et leur prétendu respect de telle ou telle norme, mais d'examiner leurs fonctionnalités. Il ne doit pas se désespérer de s'être vu refuser l'installation d'un système d'archivage électronique conforme à MoReq ou encore à la NF Z 42013 : des actions peuvent toujours être entreprises dans l'esprit général de la définition que nous donnions en introduction de l'archivage électronique (plan de classement, plan de nommage, travail sur les formats, amélioration de la sécurité des systèmes d'information, etc.).

Le pire pour l'archiviste serait de se complaire dans un rôle de Cassandra s'arcbutant avec raideur sur ses normes pour annoncer la catastrophe imminente : malgré des pertes régulières de données, le désastre annoncé de la « page blanche » s'éloigne des consciences à mesure que le numérique pénètre notre société et semble en mesurer les moindres détails. Que l'archiviste soit plutôt Ulysse : qu'il se glisse avec ruse au sein des organisations en répondant au mieux aux besoins pressants de ces dernières pour mieux imposer des dispositifs techniques fiables et performants.

¹ Concernant les normes techniques (standards d'échange, formats de métadonnées, formats de fichier, etc.), le choix est différent : on a en général le choix entre plusieurs normes qui sont autant de produits différents. Il s'agit donc de déterminer celles qui répondent à nos besoins et ensuite de les respecter afin de garantir la pérennité des informations et l'interopérabilité des systèmes.

Antoine MEISSONNIER

Adjoint au chef de bureau du contrôle et de la collecte des archives publiques
Service interministériel des Archives de France
antoine.meissonnier@culture.gouv.fr

Rémy ROQUES

Responsable du département Déploiement de l'archivage et de la collecte
Direction des archives du Groupe La Poste
remy.roques@laposte.fr

ANNEXE

Normes citées dans l'article

Rappel : les normes sont des documents élaborés à partir d'un consensus plus ou moins large d'experts réunis par des organismes mandatés par les États pour ce faire. Les normes ISO, de portée mondiale, émanent de l'Organisation internationale de normalisation. L'Union européenne dispose de plusieurs organismes de normalisation, dont l'*European Telecommunications Standards Institute* (ETSI). Les normes de portée française sont essentiellement l'œuvre de l'Association française de normalisation (AFNOR - normes NF).

BSI TR 03 125 : *Preservation of Evidence of Cryptographically Signed Document*, 2011.

DOMEA-Concept : État fédéral allemand, *Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang*, 2005. Ce standard allemand est en cours de remplacement par un nouveau *corpus* de règles : l'*Organisationskonzept elektronische Verwaltungsarbeit*.

ETSI TS 101 533-1 : *Electronic Signatures and Infrastructures (ESI), Data Preservation Systems Security; Part 1: Requirements for implementation and Management*, V1.2.1., 2011.

ETSI TS 102 573 : *Electronic Signatures and Infrastructures (ESI), Policy requirements for trust service providers signing and/ or storing data for digital accounting*, V2.1.1., 2012.

ICA-Req : *Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique, modules 1 à 3*, 2008. Ce standard a fait l'objet d'une normalisation en 2011 à l'ISO sous la référence ISO 16 175-2.

ISO 13 008 : *Information and documentation - Digital records conversion and migration process*, 2012.

ISO 14 721 : *Space data and information transfer systems - Open archival information system (OAIS) - Reference model*, 2012. Cette norme est à l'origine un guide du CCSDS, disponible actuellement en anglais sous la référence 650.0-M-2.

ISO 15 489-1 et 2 : *Information et documentation - « Records management » - Partie 1 : Principes directeurs et Partie 2 : Guide pratique*, 2001.

ISO 16 363 : *Space data and information transfer systems - Audit and certification of trustworthy digital repositories*, 2012.

ISO 19 005-1 : *Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)*, 2005.

ISO 20 652 : *Space data and information transfer systems - Producer-archive interface - Methodology abstract standard (PAIMAS)*, 2006.

ISO 23 081-1 à 3 : *Information et documentation - Processus de gestion des enregistrements - Métadonnées pour les enregistrements - Partie 1 : Principes, Partie 2 : Concepts et mise en œuvre et Partie 3 : Méthode d'auto-évaluation*, 2006 à 2011.

ISO 30 300 et ISO 30 301 : *Information et documentation - Systèmes de gestion des documents d'activité - Principes essentiels et vocabulaire et Exigences*, 2011.

ISO/IEC 27 002 : *Information technology - Security techniques - Code of practice for information security controls*, 2013.

ISO/IEC 29 115 : *Information technology - Security techniques - Entity authentication assurance framework*, 2013.

ISO/TR 13 028 : *Information et documentation - Mise en œuvre des lignes directrices pour la numérisation des enregistrements*, 2010.

ISO/TR 15 801 : *Document management - Information stored electronically - Recommendations for trustworthiness and reliability*, 2009.

ISO/TR 22 957 : *Document management - Analysis, selection and implementation of electronic document management systems*, 2009.

ISO/TR 26122 : *Information et documentation - Analyse des processus pour la gestion des informations et documents d'activité*, 2008.

MoReq2010 : DLM-Forum, *Modular Requirements for Records Systems*, 2010.

NF Z 42 013 : *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*, 2009. La première version de cette norme date de 1999, mais elle a été révisée en 2009. En mars 2012, elle est devenue une norme internationale publiée sous la référence ISO 14641-1. Depuis novembre 2012, l'AFNOR propose une certification pour cette norme (NF 461 - Système d'Archivage électronique).

NF Z 42 020 : *Spécifications fonctionnelles d'un composant Coffre-fort numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps*, 2012. Publiée en juillet 2012, cette norme complète la NF Z 42 013 en détaillant les fonctionnalités d'un composant Coffre-fort numérique destiné, au sein d'un SAE ou non, à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps.