

Politique de numérisation au RSI et archivage légal

Les archives constituent « l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité » (**article L 211-1 du code du patrimoine**).

Archiver c'est conserver des informations, des documents, des objets...pour des raisons identifiées et sur des durées définies, de telle sorte que l'objet archivé ait, le jour où il est extrait, exactement la même valeur que celle qu'il possédait le jour où il a été pris en charge (aucune dégradation à la sortie).

L'archivage électronique a pour finalité la conservation d'objets numériques (contenu informationnel, métadonnées...) en assurant la valeur juridique des documents de leur versement jusqu'au terme du délai de conservation (preuve du contenu d'un fait ou d'un acte juridique, respect d'une exigence de forme, preuve du respect des règles, des procédures internes, du respect d'obligations d'information...etc).

Il permet de faire une dissociation de l'information et de son support, ce dernier n'étant qu'une commodité temporelle.

La nécessité d'archiver implique de se conformer aux obligations légales et réglementaires, se constituer des preuves et préserver le patrimoine de l'organisme.

S'agissant d'archivage électronique, il est nécessaire de prendre en compte les modalités induites par les caractéristiques intrinsèques des objets numériques et celles induites par les technologies de traitement de l'information (réseaux, supports, formats...).

L'article D 253-44 du code de la sécurité sociale (applicable au RSI en vertu de l'article D 611-16 du même code) prévoit la possibilité de conserver les pièces originales sur support électronique.

Il est impératif que les documents ayant une force juridique soient conservés jusqu'à ce qu'ils cessent de produire des effets juridiques, le cas échéant pendant la durée de conservation fixée par les textes.

Cette conservation ne doit pas se limiter aux seuls documents mais doit porter sur l'ensemble des éléments contribuant à la valeur juridique du document.

La conservation garantissant l'intelligibilité et l'intégrité du document constitue une condition essentielle de la valeur juridique du document électronique alors reconnue par le juge.

Au sein du RSI, la préconisation s'oriente vers un processus de dématérialisation notamment en faveur de la numérisation dans un premier temps.

- **Documents numérisés dans le cadre de la GED/GDT RSI**

La Direction des systèmes d'information de la Caisse nationale garantit la sécurité et le suivi de la sauvegarde à long terme des documents numérisés, et tout particulièrement le suivi technologique.

La sauvegarde des documents numérisés est effectuée par chaque caisse RSI de la façon décrite ci-après.

Tous les documents sont gravés simultanément et automatiquement sur deux disques optiques numériques de type WORM. Un support sert de disque courant, l'autre de sauvegarde.

Lorsque le disque de sauvegarde est plein, celui-ci est rangé au coffre de la caisse RSI ou dans un lieu extérieur et est remplacé immédiatement par un disque vierge.

Par ailleurs, les caisses sont invitées à utiliser la procédure de sauvegarde qui est déclenchée manuellement et qui consiste à graver sur un 3^{ème} disque les images numérisées depuis la dernière sauvegarde.

Cette disposition permet de reconstituer un disque si un sinistre survient simultanément sur les disques d'exploitation et de sécurité courants.

Le WORM (Write Once Read Many) est une méthode d'enregistrement dont la propriété intrinsèque est d'empêcher tout effacement, toute réécriture et toute modification.

L'utilisation du disque optique numérique garantit une durée de vie très élevée en raison de l'absence de toute usure mécanique.

L'existence pour les documents numérisés de deux lieux différents de stockage (disque d'exploitation en permanence dans le juke-box et disque de sauvegarde rangé dans un autre lieu) permet une sécurité supérieure à celle de la conservation des documents papier.

- **Documents médicaux numérisés dans le cadre de la fonction de numérisation ARCHSCAN de l'application nationale informatique ARCHIMED**

La fonction de numérisation ARCHSCAN permet depuis l'année 2008 (version V1.16 d'ARCHIMED) la numérisation de pièces médicales et non médicales à joindre aux dossiers médicaux gérés par l'application informatique ARCHIMED. Le rattachement à une décision ou au dossier est effectué dans le dossier ARCHIMED du bénéficiaire. Une base nationale d'images ARCHSCAN a été créée à cet effet, et intégrée à la base ARCHIMED(1). Les pièces jointes numérisées et rattachées à un dossier médical ou à une décision (1) peuvent être ultérieurement appelées et consultées, archivées ou supprimées physiquement. L'exploitation informatique des bases ARCHIMED et ARCHSCAN étant faite sur le site central de Toulouse (CPT), cette application bénéficie de l'ensemble du dispositif de sécurité appliqué aux applications nationales. Il n'existe par ailleurs aucun risque local, si l'on excepte la courte phase de numérisation sur le scanner du service médical. Par ailleurs la fonction ARCHSCAN, comme l'application ARCHIMED, ont fait l'objet d'une autorisation de la CNIL. Enfin la gestion centralisée d'une base unique garantit l'homogénéité et l'évolutivité technique et fonctionnelle du produit(1).

(1) => Différence avec GED-GDT

- **Documents numérisés par une société extérieure**

Si la caisse recourt à une société extérieure pour numériser des documents, toutes les garanties quant à leur conservation et à leur utilisation future doivent être prises, notamment :

- choix d'un type de support adapté à l'utilisation souhaitée (le coût doit être mis en relation avec les besoins en termes de pérennité du support, de robustesse, de rapidité d'accès aux documents, de facilité de copie, de volumétrie etc....).
- conservation sur au moins deux supports stockés dans des lieux différents,
- une solution de type WORM doit être impérativement choisie.

Si la conservation est prévue pour du long terme, une procédure interne doit également être mise en place pour garantir le suivi de la solution technologique adoptée. Les techniques évoluent en effet rapidement et il faut s'assurer que les documents pourront être accessibles jusqu'à l'expiration du terme prévu à leur conservation.

Pour mettre en œuvre un projet de dématérialisation, il faut impérativement considérer l'ensemble du cycle de vie du document, en y incluant les échanges avec les partenaires extérieurs (création, acquisition, transmission, traitement, stockage, archivage, destruction) de façon à exploiter une solution offrant une sécurisation des échanges (identification, authentification, horodatage) afin de préserver l'intégrité et la pérennité des documents et des informations, ainsi que la traçabilité des opérations.

Les pièces justificatives sur support électronique qu'elles soient issues, indifféremment, d'un procédé de numérisation de documents « papier » (dématérialisation) ou d'un processus informatique (document natif) jouissent de la même valeur juridique que les documents « papier » correspondants, **sous réserve du respect des conditions évoquées ci-dessus** ; dès lors, elles doivent être acceptées dans les mêmes conditions que les pièces justificatives « papier » par le juge.

La norme NF 42-013 (norme française dédiée à l'archivage intègre, décrivant l'utilisation des procédés techniques au regard des exigences de sécurité), représentative de « l'état de l'art », n'a pas de valeur juridique contraignante mais peut servir de guide aux magistrats. Dans la mesure où elle ne serait suivie qu'en partie, l'organisme devra documenter et expliquer les choix alternatifs opérés dès l'origine.

Un audit préalable relatif aux moyens et solutions informatiques mis en œuvre est conseillé avec un triple angle d'attaque (droit/technique/organisationnel) afin de rédiger un référentiel juridique applicable aux documents archivés par l'entreprise (cadre et contraintes).

La politique d'archivage doit comprendre :

- la description des objets à archiver,
- les procédures de constitution des archives,
- les contrôles prévus pour leur constitution (notamment sur les contenus, l'intégrité ou la conformité technique des objets à archiver),
- la description des opérations à effectuer pour procéder à l'archivage (migrations de support, de format..),
- les modalités d'accès aux archives,
- les audits,
- la réversibilité et l'interopérabilité.

Le législateur n'a donné aucun cadre spécifique à l'archivage ; néanmoins, outre l'archivage papier « traditionnel », seul un archivage électronique sécurisé permettra au juge d'apprécier la valeur juridique du document conservé, lequel devra répondre aux exigences légales et jurisprudentielles conditionnant le fait que cet acte produise des effets juridiques.

Cela impose que l'on s'assure que le document que l'on a conservé puisse être restitué en apportant l'assurance qu'il n'a pu être modifié.

Récemment, la Cour de cassation, édifiant le socle du droit de la preuve pour les documents créés avec des logiciels de bureautique, et dont généralement aucune copie papier n'est conservée, a jugé que :

- lorsqu'une partie n'a pas conservé l'original d'un document, la preuve de son existence peut être rapportée par la présentation d'une copie qui doit en être la reproduction non seulement fidèle mais durable ;
- l'écrit sous forme électronique ne vaut preuve qu'à condition que son auteur puisse être dûment identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité .

Cour de cassation 2ème Chambre Civile / 4 décembre 2008 - Sté Continent France c/ CPAM de la Marne n° pourvoi : 07.17622

La copie se définit comme « *toute reproduction littérale d'un original qui, n'étant pas revêtue des signatures qui en feraient un second original, ne fait foi que lorsque l'original ne subsiste plus et sous les distinctions établies par l'article 1335 du code civil, mais dont la valeur est reconnue à des fins spécifiées (notamment pour les notifications), sous les conditions de la loi (copies établies par des officiers publics compétents...)* » selon l'ouvrage de G.CORNU « Vocabulaire juridique » PUF 2001.

a) **L'archivage « simple »**

L'archivage « simple » est une solution très répandue pour la gestion de documents reçus pour une application métier avec des exigences modérées et des durées de conservation courtes.

- **Pérennité ou durabilité**

Cette notion s'apprécie en considérant la viabilité du support utilisé.

C'est un **élément de sécurité et de qualité destiné à garantir de façon durable la sécurité** (sauvegardes, écritures en miroir, répllication...)

Une directive 2002/68/CE du 23 septembre 2002 a défini le « support durable » comme un instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément pour l'avenir, pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées.

- **Intégrité**

C'est l'état d'une chose qui n'a pas été altérée durant son cycle de vie.

L'intégrité s'appuie sur la pérennité (enregistrement avec altération irréversible du support, calcul et gestion des empreintes, copies multiples...).

C'est l'article 1316-1 du code civil qui évoque expressément ce critère de conservation de l'écrit électronique.

Au plan juridique, l'intégrité peut être définie **comme la caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification.**

La norme NF ISO 15489-1 précise en effet que l'intégrité :

- d'un document d'archives renvoie au caractère complet et non altéré de son état ;
- et que celle d'un système d'archivage est assurée lorsque des mesures de contrôle visant le droit d'accès, l'identité de l'utilisateur, le droit de procéder à des éliminations et la sécurité sont mises en œuvre.

- **Authenticité**

Souvent rapprochée voire confondue avec la notion d'identification (processus de détermination de l'identité d'une personne), elle se définit comme **une opération contemporaine de la rédaction d'un acte consistant à conférer l'authentification à cet acte** ou comme une opération consistant à vérifier a posteriori l'**authenticité** d'un document en établissant de manière formelle et intangible l'identification des parties à un échange ou à une transaction électronique (signature électronique, horodatage, calcul et gestion des empreintes...).

- **Fiabilité, conformité, lisibilité, intelligibilité**

La norme NF ISO 15489-1 définit un document d'archives fiable, comme tout document dont le contenu peut être **considéré comme la représentation complète et exacte des opérations, des activités ou des faits qu'il atteste et sur lequel on peut s'appuyer**.

S'agissant du système d'archivage **fiable**, c'est le système d'organisation et de gestion des documents d'archives qui fonctionne de manière continue et régulière.

L'AFNOR recommande qu'un système d'archivage :

- intègre automatiquement tous les documents d'archives relevant du champ d'activité de l'organisme,
- organise les documents d'une manière telle, qu'elle reflète les opérations du producteur des documents,
- protège les documents contre une altération ou une élimination abusive,
- joue automatiquement le rôle de source première d'information sur les activités décrites dans les documents,
- fournisse un accès immédiat à tous les documents pertinents et à leurs métadonnées.

C'est le critère de qualité de ce qui est fidèlement conforme, c'est-à-dire juridiquement **l'exacte application d'une norme de référence**.

La norme NF ISO 15489-1 précise que la conformité d'un système d'archivage est assurée lorsqu'il est organisé et géré en conformité avec toutes les exigences issues des affaires courantes, de l'environnement réglementaire et des attentes du secteur d'activité concerné.

b) **L'archivage électronique « sécurisé »**

L'archivage sécurisé répond à un besoin de durées de conservation moyennes à longues, comprenant des dispositifs pour garantir l'intégrité des procédures de contrôle d'accès et une journalisation des opérations.

L'intérêt de l'archivage sécurisé est de garantir que le document sera conservé dans le respect des conditions légales, réglementaires et jurisprudentielles afin de produire ses effets juridiques dans le temps.

- **Tracabilité**

C'est l'historique de l'ensemble des événements et opérations sur les objets numériques (journal des événements...).

- **Sécurité**

C'est la protection des accès (administration et gestion des droits d'accès).

La prise en charge du document doit être sécurisé dès l'origine (scellement, horodatage, signature électronique...).

Si la conservation ne garantit pas les conditions exigées pour la reconnaissance d'un écrit électronique et remplies à la date de son établissement, l'écrit électronique perd sa valeur juridique.

- **Disponibilité et accessibilité**

C'est la possibilité d'accéder facilement au document archivé et garantir l'intelligibilité de l'acte.

A la différence du droit français, le droit communautaire ne soumet pas cette notion à la condition d'irréversibilité du support.

Ainsi, le contenu informationnel doit être maintenu dans son intégrité mais pas forcément dans les mêmes formes et sur les mêmes supports.

Les copies comme les originaux électroniques sont concernés par cette exigence de durabilité. Mais, la facilité d'utilisation et de diffusion des originaux électroniques, qui eux sont intègres, devrait écarter l'utilisation de copies, propres au contexte papier.

L'archivage électronique sécurisé se définit comme un ensemble de modalités de conservation et de gestion des archives électroniques ayant une valeur juridique lors de leur établissement.

Ses fonctions consistent dans :

- le versement
- le stockage
- la gestion des données descriptives
- la consultation et la communication
- l'administration, au sens large.

Il va s'agir de conserver des données sur de longues périodes en s'appuyant sur des technologies en perpétuelle évolution afin de pérenniser l'information, garantir son intelligibilité et protéger son intégrité.

Comme indiqué plus haut, le législateur n'a donné aucun cadre spécifique à l'archivage. Néanmoins, outre l'archivage papier « traditionnel », seul un archivage électronique sécurisé permettra au juge d'apprécier la valeur juridique du document conservé, lequel devra répondre aux exigences légales et jurisprudentielles et conditionnant le fait que cet acte produise des effets juridiques.

Cela impose que l'on s'assure que le document que l'on a conservé puisse être restitué en apportant l'assurance qu'il n'a pu être modifié.

La norme NF 42-013 indique que l'intégrité est la caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification. Le contrôle porte alors sur le document électronique lui-même et donc sur les données stockées.

Les normes ISO (15489-1 et 15489-2) s'attachent à définir les conditions optimum d'une politique d'archivage mais ne privilégient aucune solution technologique et recommandent que soient mises en œuvre des mesures de contrôle visant le droit d'accès, l'identité de l'utilisateur, le droit de procéder à des éliminations et la sécurité.

La technologie WORM (« *write once read many* ») est une référence, reconnue par la norme de l'AFNOR (Association française de normalisation) NF 42-013, à une méthode d'enregistrement dont la propriété intrinsèque est d'être non effaçable, non réinscriptible et non modifiable.

Elle est de 3 types :

- **Type A :**

Principe des disques optiques avec modification du substrat et transformation permanente du support.

- **Type B :**

Principe des disques magnéto - optiques ou des bandes équivalentes et utilisation d'un micro code « worm » inclus dans le support au moment de sa fabrication, reconnu par le lecteur ou le contrôleur et protégé de l'effacement et de la ré écriture dans des conditions d'utilisation normales.

- **Type C :**

Principe des disques magnétiques et génération d'un micro code « worm » enregistré avec l'information et destiné à traiter l'enregistrement comme étant

de type « worm » par le logiciel de gestion de support, le protégeant de l'effacement, de la ré - écriture ou de toute modification.

Le type C est l'avènement du « worm logique » par opposition au « worm physique » ; la grande différence du support optique par rapport au support magnétique semble résider dans sa fiabilité et surtout dans sa pérennité.

C'est en effet une combinaison d'éléments permettant d'assurer une conservation à la fois intègre et pérenne de l'information sur du disque magnétique.

La « worm logique » à base de disques magnétiques présente les avantages suivants :

- rapidité d'accès et de transferts de données
- fiabilité du support (données chiffrées, horodatage)
- migration technologique possible
- possibilité de supprimer un fichier (notamment lorsque la loi prévoit une durée précise ou un droit à l'oubli)

Cette technologie permet au document archivé de conserver toute sa valeur en répondant aux exigences légales de sécurité, d'authenticité, de traçabilité et d'auditabilité.