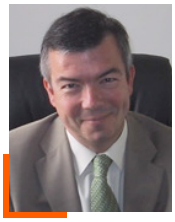
L'ARCHIVAGE ELECTRONIQUE A L'USAGE DU DIRIGEANT

Marie-Anne CHABIN,
Eric CAPRIOLI,
Jean-Marc RIETSCH

FedISA Fédération ILM, Stockage & Archivage

CIGREF

Les Auteurs



Jean-Marc Rietsch

Pilote de l'ouvrage, JM Rietsch est expert des métiers de la confiance et plus particulièrement de l'archivage électronique. Ingénieur Civil des Mines, JM Rietsch a débuté sa carrière professionnelle par le développement logiciel et l'offre de services pour les PME-PMI. En 1993, il oriente sa carrière vers la sécurité et plus particulièrement la sauvegarde des données informatiques et dépose un brevet sur le sujet. En 2001, JM Rietsch participe au lancement du premier tiers archiveur en France. JM Rietsch est Président de FedISA (Fédération de l'ILM du Stockage et de l'Archivage), créée en 2005 afin de pouvoir répondre aux attentes des utilisateurs dans le domaine.

Marie-Anne Chabin

Archiviste de formation, diplômée de l'Ecole nationale des Chartes, MA Chabin a exercé aussi bien dans le public que dans le privé, où elle a acquis une solide expérience de la gestion de l'information papier, électronique ou audiovisuelle. Elle a fondé en 2000 et préside le cabinet d'expertise Archive 17 (www.archive17.fr), spécialisé dans les stratégies d'archivage électronique et dans le Records management. MA Chabin est l'auteur de nombreux articles sur l'archivage et de plusieurs ouvrages dont Le management de l'archive (Hermès, 2000). Elle a coordonné en 2004 le numéro spécial de la revue Document numérique sur « Archivage et pérennisation».

Eric Caprioli

Avocat à la Cour de Paris, Docteur en droit, spécialiste en droit de la propriété intellectuelle et des NTIC, Vice-président de la Fédération Nationale des Tiers de Confiance (FNTC), Expert aux Nations Unies sur les questions de droit du commerce électronique depuis plus de 12 ans, Membre du Comité directeur de la certification près le SGDN depuis 2003 (arrêté du 28 janvier 2003, publié au JO), Président de l'association nationale des professionnels de la propriété incorporelle (ANPPI). Auteur de nombreux articles sur la dématérialisation, la signature, la preuve et l'archivage électronique, conférences et ouvrages sur le droit de l'économie numérique, dont celui sur la Loi pour la Confiance dans l'économie numérique (LCEN), éditions LGDJ publié en 2005. Voir le site du cabinet: www.caprioli-avocats.com. Fondateur du cabinet d'avocats Caprioli &Associés, Paris et Nice.

Remerciements

Avant d'entamer notre développement, je tenais à adresser tous nos remerciements à ceux qui nous ont soutenu et encouragé dans notre démarche. Afin de n'oublier personne le mieux est sans doute de ne pas les citer sachant qu'ils sont nombreux à nous avoir fourni tout ou partie des informations collectées et à nous avoir poussé pour notre travail. Néanmoins je tenais tout particulièrement à remercier deux personnes :

- **Michel Grosbost**, responsable de Terastar et de son pôle évènement ITI FORUMS, par qui tout a commencé, une première conférence « ILM et Archivage Electronique » couronné de succès avec plus de 500 participants, la naissance d'une Fédération « FedISA (Fédération de lILM du Stockage et de l'Archivage) et maintenant cet ouvrage. D'autres manifestations sont d'ores et déjà programmées par ITI FORUMS : Business Continuity, une nouvelle édition de ILM et Archivage Electronique, etc...

- **Jean-François Pépin**, délégué général du CIGREF qui a su nous faire confiance et surtout,de par son expérience, a pris régulièrement sur son temps pourtant bien occupé afin de nous prodiguer de précieux conseils nous ayant finalement permis d'aboutir.

Le code de la propriété intellectuelle du 1er juillet 1992 interdit expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée notamment dans l'enseignement, provoquant une baisse brutale des achats de livres, au point que la possibilité même pour les auteurs de créer des oeuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée. En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation du Centre Français d'Exploitation du Droit de copie, 20, rue des Grands-Augustin 75006 PARIS.

Toute représentation ou reproduction intégrale ou partielle faite sans le consentement des auteurs ou de leurs ayants droit ou ayants cause est illicite selon le Code de la propriété intellectuelle (Art L 122-4) et constitue une contrefaçon réprimée par le Code pénal. Seules sont autorisées (Art L 122-5) les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, ainsi que les analyses et courtes citations justifiées par le caractère critique, pédagogique ou d'information de l'oeuvre à laquelle elles sont incorporées, sous réserve, toutefois, du respect des dispositions des articles L 122-10 à L 122-12 du même Code, relatives à la reproduction par reprographie.

Préface

Le thème de l'archivage électronique devient de plus en plus un sujet d'actualité pour bon nombre d'organisations tant publiques que privées. Ceci s'explique certes par une augmentation extrêmement forte du volume de données électroniques gérées au quotidien mais aussi par une évolution des technologies et surtout des process d'entreprise voire des obligations nées à la suite de différents événements. Les plus récentes évolutions en la matière sont sans doute celles relatives aux réglementations financières qui imposent désormais la conservation d'informations jusque là négligées.

La problématique de l'archivage électronique ne se limite pas à une simple dématérialisation des techniques d'archivage traditionnelles. Outre l'influence des nouvelles obligations, ce nouveau type d'archivage doit être considéré très en amont dans la chaîne de valeur de l'information, d'où la volonté de prendre en compte l'ensemble du cycle de vie de la donnée. En effet, la loi française est très claire sur le sujet, pour que des données électroniques puissent avoir une quelconque valeur juridique, il faut entre autre apporter la preuve de leur intégrité tout au long de leur parcours, de la création à l'archivage.

Compte tenu de l'évolution rapide des nouvelles technologies, il est souvent difficile d'opérer un choix qui engage l'entreprise sur plusieurs années.

Dès lors, pourquoi ne pas profiter de ces évolutions pour donner une nouvelle valeur à la donnée archivée, entre autre en matière d'accessibilité ? En effet, dès que l'information existe sous forme électronique et que son intégrité est garantie, les seules modifications qu'elle puisse subir sont celles relatives à un changement de support, voire un système d'accès plus sophistiqué en matière d'indexation. Dès lors l'information, même archivée, peut rester accessible extrêmement facilement et renforcer d'autant le système d'information de l'entreprise et par là même sa compétitivité en permettant de disposer de la bonne information au bon moment.

En matière d'archivage, les exigences sont les suivantes :

- assurer la traçabilité, l'intégrité, la sécurité et la pérennité des données;
- répondre aux exigences légales de conservation et de communication;
- relever le défi de l'obsolescence technologique récurrente;
- faciliter l'accès à l'information.

Au-delà de la simple technique il est indispensable de considérer d'autres aspects complémentaires de types juridiques, organisationnel voire de normalisation. Sans être compliqué cet environnement devient vite complexe.

Au regard de l'évolution des usages, des contraintes associées et des techniques, il existe aujourd'hui une urgente nécessité d'informer l'ensemble des parties prenantes intéressées aux questions de gestion et de conservation de l'information électronique.

Préface

De cette conviction est née FEDISA, Fédération de l'ILM, du Stockage et de l'Archivage afin de véritablement répondre aux besoins identifiés et qui s'est fixée pour principales missions de :

- sensibiliser les responsables concernés aux nouvelles technologies et aux obligations afférentes (obligation d'archivage, de continuité d'activité, de traçabilité, ...) ;
- informer les utilisateurs sur les nouvelles technologies en effectuant une véritable veille tant technologique que juridique, normative ou encore organisationnelle et ce à un niveau national et international ;
- donner au responsable de tels projets les éléments permettant de pleinement les justifier par rapports aux risques encourus (légaux et financiers) et autres avantages compétitifs comme une meilleure réactivité ;

- former aux nouveaux métiers de l'entreprise comme le « records manager », le « business continuity officer », etc... ;
- définir des « certifications et des référencements », nouveaux process, nouvelles technologies ;
- entretenir des liens avec les organismes oeuvrant dans ces environnements de la sécurisation et de la valorisation de l'information en générale.

Pourquoi un partenariat CIGREF - FEDISA ?

Compte tenu de sa mission « promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise », le CIGREF, association regroupant 120 Grandes Entreprises françaises, est partenaire de cette publication.

Le présent ouvrage s'adresse essentiellement aux dirigeants afin de leur permettre de pouvoir rapidement se faire une opinion de ce qu'il est réellement nécessaire de connaître pour aborder de telles problématiques. Ainsi ce document est destiné avant tout à mieux cerner le périmètre de l'archivage électronique tout en éliminant les idées fausses qui ne manquent pas dans un tel contexte.

Au-delà de la sensibilisation il s'agit également de souligner le rôle essentiel que peut et doit tenir le DSI compte tenu de sa position et de ses responsabilités vis-à-vis de l'information en général et de l'archivage en particulier. Comme évoqué ci-dessus la pluralité des métiers concernés est une des constantes de cette nouvelle problématique et qui, mieux que le DSI, peut permettre d'établir un dialogue entre les différentes fonctions concernées au sein de l'entreprise sans oublier les autres parties prenantes intéressées :

- l'utilisateur qui connaît son secteur d'activité ;
- le responsable informatique qui appréhende cette nouvelle donne technique ;
- l'industriel qui développe des solutions en ce sens ;
- l'archiviste dont c'est le cœur de métier ;
- l'expert technique en archivage qui tient le rôle d'accompagnateur de ces projets ;
- le juriste qui met en lumière les risques juridiques et les encadre ;
- les institutionnels qui identifient des besoins et définissent des normes communes ;
- le tiers archiveur qui se charge de l'hébergement mais aussi de l'organisation de cet archivage.

Faire en sorte que toutes ces compétences puissent travailler efficacement ensemble, telle est l'ambition du présent ouvrage.

Jean-Pierre CORNIOU
Président du CIGREF

Jean-Marc RIETSCH
Président de FEDISA

Introduction

Autrefois simple concept la dématérialisation touche aujourd'hui pratiquement tous les domaines. L'Etat est particulièrement moteur sur ce sujet en proposant au travers de ses différents services et entités représentatives plusieurs dizaines de téléprocédures dont les plus connues sont historiquement téléTVA et téléIR. Depuis janvier 2005 de nombreux appels d'offres publics peuvent se faire de façon dématérialisée. En ce qui concerne plus particulièrement l'entreprise, la dématérialisation des factures est maintenant une réalité bien que réservée, au moins dans un premier temps, aux grandes entreprises compte tenu des volumes nécessaires pour obtenir un bon taux de retour sur investissement. Ce phénomène s'étend même jusqu'au niveau des particuliers ou l'on voit arriver la carte d'identité électronique ou encore la carte de vie citoyenne. Tout cela est rendu possible grâce à l'usage de la signature électronique qui après un démarrage pour le moins chaotique semble enfin avoir trouvé sa voie, entraînant dans son sillage l'horodatage encore en cours de maturation et surtout l'archivage électronique. Ce sont en effet des volumes colossaux d'informations dématérialisées qu'il va falloir maintenant conserver en toute sécurité pendant plusieurs dizaines d'années, voire davantage. Pour preuve la loi sur le dossier médical du patient et plus récemment encore la reconnaissance de l'acte authentique électronique qui nécessite une conservation à vie des documents ainsi traités ! Notons enfin que tous ces services et leurs évolutions sont à prendre en considération à un niveau non pas seulement national mais bien mondial.

Ajoutons à cela que la notion même d'archivage a changé dans la mesure où il faut totalement balayer cette vision ancienne, pourtant bien ancrée dans les esprits, de l'archive conservée dans des cartons poussiéreux. Du fait de la dématérialisation, l'information reste facilement accessible et doit le rester tout au long de son cycle de vie, de sa création à son archivage historique ou à sa destruction. Cela veut dire que même rendue au statut d'archive la donnée doit être récupérable facilement et efficacement, voire disponible en ligne.

Par ailleurs l'archivage est à prendre en compte dès la création de la donnée ce qui provoque certains bouleversements dans les anciennes habitudes comme il est facile de l'imaginer.

Fut un temps l'on pouvait facilement définir la notion de données vivantes ou mortes en résumant cela au type d'accès. Une donnée était réputée vivante si accessible en ligne et encore modifiable alors qu'à l'inverse elle était dite morte si figée et archivée. Cette époque est en train de disparaître et encore une fois l'archivage prend une orientation tout à fait nouvelle dans la mesure où il devient partie intégrante et surtout active du cycle de vie de la donnée. La particularité de la donnée archivée est de ne plus être modifiable tout en demeurant accessible tant qu'elle présente une utilité. C'est le cas par exemple d'un mail qui, autrefois, aurait été considéré comme une donnée morte.

Face à cette profonde mutation le chef d'entreprise se trouve fort démuni, ne sachant pas par quel bout prendre le problème, d'où la tentation fort compréhensible d'attendre ! Pourtant les enjeux sont de taille qu'ils soient, juridiques, réglementaires, organisationnels, sécuritaires, géopolitiques, ...

L'objectif du présent ouvrage est ainsi d'aider le dirigeant face à ce problème posé par la dématérialisation à outrance de la nécessité d'archiver des masses de plus en plus importantes d'informations qu'il va falloir également être capable de retrouver rapidement. Surtout nous essayerons de montrer comment transformer ce qui apparaît a priori comme une contrainte en quelque chose de constructif permettant entre autre une plus grande fluidité et une meilleure accessibilité à l'information et ce quelque soit son état.

Après avoir défini les quelques enjeux qui nous apparaissent comme essentiels, nous fournirons sous forme de fiches les thèmes principaux à connaître permettant de se poser les bonnes questions en matière d'archivage électronique et surtout d'être capable d'y trouver une réponse ou tout au moins un début de réponse.

Les Enjeux

Au niveau de l'entreprise, les enjeux induits par l'archivage électronique sont multiples comme nous allons l'aborder ci-après.

Tout d'abord il s'agit d'un enjeu stratégique pour décider quelles données conserver en dehors des aspects purement obligatoires. En effet, selon son domaine d'activité il est plus ou moins intéressant de conserver ses différents procédés, savoir-faire ou autres afin de pouvoir les réutiliser ultérieurement ou tout simplement d'en garder une trace historique au sens du patrimoine intellectuel de l'entreprise.

A côté de cet aspect existe bien évidemment son pendant obligatoire où l'enjeu est soit légal, destiné au respect des lois en vigueur, soit réglementaire afin de se conformer à des exigences très génériques ou plus spécifiques pour telle ou telle branche d'activité. Quoiqu'il en soit sur ce point il s'agit avant tout de bien connaître ses obligations et l'étendue des sanctions en cas de non respect de ces obligations.

A partir du moment où la décision de mettre en place un système d'archivage a été prise d'autres enjeux interviennent dont le premier est d'ordre purement organisationnel dans la mesure où il faudra autant que faire se peut optimiser la structuration des données afin d'en faciliter la gestion et de maîtriser la redondance de l'information, détruire les données inutiles ou périmées qui alourdissent le système, faciliter l'accès à l'information tout en respectant des droits d'accès établis de façon stricte.

Par rapport à ce dernier point l'enjeu est également sécuritaire et oblige à avoir une cohérence indéniable entre les différentes démarches associées au sein de l'entreprise. En effet pourquoi fermer la porte de son usine si l'on ne bloque pas les accès à l'information, certes immatérielle, avec la même logique.

Intervient ensuite bien évidemment un enjeu d'ordre technologique. La question à laquelle il va falloir répondre consiste à trouver quelle technologie adapter dans un monde en pleine évolution et quelle solution retenir, capable de protéger l'entreprise contre cette obsolescence des technologies tout en lui offrant une garantie de disponibilité des données sur le moyen, long terme. Enfin toujours sous l'aspect technique, le système devra être capable d'absorber une augmentation naturelle des volumes de données à archiver.

L'enjeu juridique concerne essentiellement les données conservées à des fins légales et se situe entre organisation et technique. Il est important de vérifier qu'au besoin, en cas de contentieux par exemple, le système permettra d'une part de retrouver les pièces requises dans les délais impartis et de plus que ces dernières pourront être effectivement retenues comme éléments de preuve. Un autre aspect de cet enjeu consiste à respecter les lois en vigueur par rapport à la conservation de types particuliers de données comme les données personnelles.

Nous pouvons citer également un enjeu géopolitique qui réside dans la capacité pour l'entreprise à conserver son information dans différents lieux pour peu qu'elle puisse y accéder en ligne.

Enfin l'enjeu est éminemment financier et ceci à double titre : le premier au regard des investissements directement liés à la mise en place du système d'archivage et à son exploitation, le second face au risque encouru si l'entreprise se trouve dans l'impossibilité de retrouver et de fournir l'information requise.

Après avoir succinctement listé l'ensemble des enjeux qui nous paraissent essentiels, nous allons pouvoir aborder plus en détail la façon de les traiter efficacement.

Fiches

Chacune des fiches qui suivent a été conçue de façon à pouvoir être lue indépendamment des autres. Ce choix a été dicté par un souci d'efficacité destiné à permettre de trouver rapidement les premiers éléments de réponse aux problèmes que l'on se pose. A contrario, ceci provoque immanquablement certaines répétitions ou renvois le cas échéant à d'autres fiches complémentaires.

Nous avons également préféré mettre directement à l'intérieur du texte les références utiles afin de faire gagner du temps au lecteur qui désirerait approfondir tel ou tel aspect.

Chacune des fiches est organisée de la même manière en trois parties. La première, le contexte est plus particulièrement destinée à bien positionner le problème posé, la deuxième partie précise les enjeux concernés tandis que la troisième énonce les recommandations qui nous semblent fondamentales.

Le détail des fiches est le suivant :

Phase	N° Fiche	Thème
Le cadre	1	Besoins d'archivage
	2	Contraintes légales (droit public)
	3	Contraintes légales (droit privé)
	4	Contraintes spécifiques
	5	Contraintes techniques
	6	Risques et assurances
	7	Stratégie
Les outils	8	Les technologies actuelles
	9	Les logiciels
	10	Les outils méthodologiques
	11	Le tiers archiveur
	12	Les coûts

Contexte

L'on pourrait dire de l'archivage qu'il correspond à l'organisation raisonnée d'une conservation sécurisée de l'information créée aujourd'hui afin de pouvoir la réutiliser demain ou après-demain. De plus en plus ce besoin d'archivage est ressenti comme une nécessité pour les entreprises et devient une obligation.

L'archivage répond en fait à trois besoins distincts :

1. le premier, qui est le plus important, est le besoin pour l'entreprise de prouver ce qu'elle a fait ou ce qu'elle n'a pas fait ; elle doit justifier de son activité vis-à-vis des autorités de tutelle, vis-à-vis de l'Etat, vis-à-vis d'un audit interne ; elle doit en outre, lors d'un contentieux, produire les pièces nécessaires à la défense de ses droits et de ses intérêts ;
2. le second besoin correspond à la réutilisation des données dans la conduite des affaires comme des études déjà réalisées et réutilisables dans le cadre d'un nouveau projet, au lieu de recréer l'information, opération qui peut coûter cher et faire perdre un temps précieux ;
3. le troisième besoin est pour l'entreprise l'intérêt de préserver sa mémoire, tant pour constituer une culture d'entreprise, que pour communiquer envers ses clients, ses partenaires, ses salariés, voire la société.

Les besoins d'archivage sont d'autant plus forts que l'information produite et archivable est toujours plus prolifique ; qu'elle se présente sous des formes multiples (données structurées ou non, images, sans oublier le papier) ; et que l'environnement réglementaire est souvent très contraignant.

Enjeux

Les enjeux de l'archivage ou de l'absence d'un archivage raisonné et efficace sont de cinq types :

1. **juridique :** le principal risque est de ne pas pouvoir produire les données requises par un audit ou un juge dans la forme requise ; non seulement les données doivent avoir été archivées mais elles doivent présenter des caractéristiques d'authenticité, d'intégrité et de non répudiation ;
2. **logistique :** les données ont été bien archivées techniquement mais il est pratiquement impossible d'y accéder car elles n'ont pas été caractérisées pour pouvoir effectuer des recherches et les moteurs de recherche ne produisent que du « bruit » inexploitable ; ou encore, les données existent mais ne sont pas intelligibles (on a perdu le moyen de les décoder et de les interpréter) ;
3. **sécuritaire :** des données confidentielles (données stratégiques, personnelles) risquent d'être divulguées parce qu'elles ne sont pas ou insuffisamment protégées, ou encore parce qu'elles auraient du être détruites ;
4. **technique :** l'enjeu technique est double : dans l'espace avec les problèmes d'interopérabilité entre systèmes, et dans le temps avec le défi de pérennité des données sur le long terme, face à l'obsolescence récurrente des formats, supports et outils de restitution ;
5. **financier :** l'enjeu financier est double également : coût d'une amende ou d'une condamnation judiciaire et dans une moindre mesure, mais à ne pas négliger tout de même, temps perdu à la recherche d'information ou investissement perdu dans des outils non maintenus dans le temps.

Les enjeux de l'archivage peuvent se résumer aux conséquences pour l'entreprise si elle ne peut pas retrouver les informations qu'elle a produites à un moment de son activité, alors qu'elle a besoin de les communiquer ou de les réutiliser.

Recommandations

Quand on parle d'archivage, la première tâche d'une entreprise est d'évaluer ses besoins, c'est-à-dire archiver quoi pourquoi et pour combien de temps ? Pour l'évaluation de ces besoins, il est recommandé de répondre de manière appropriée aux six questions suivantes :

1. Quelles sont les données à archiver parmi l'ensemble des données produites ?	Les données à archiver sont celles qui correspondent à un processus (ou à un sous processus au sein d'un processus) achevé ; elles sont validées et ne doivent plus être modifiées, afin de tracer un événement à une date donnée, et qui sont validées. Les données à archiver représentent en général une minorité de l'ensemble des données produites dans le cadre des activités de l'entreprise. Il faut donc élaborer une cartographie globale des données à archiver, c'est-à-dire des données à identifier et à capturer dans un système d'archivage, par ordre de priorité : • archives vitales pour l'entreprise : en plus des données courantes qui sont sauvegardées régulièrement, d'autres données, plus anciennes, sont elles aussi indispensables à l'entreprise pour redémarrer son activité au lendemain d'un sinistre ; • données à caractère légal et réglementaire : être en règle vis-à-vis du fisc, des organismes sociaux, de la CNIL, etc. ; • données supportant les intérêts de l'entreprise en cas de contentieux ; • information exploitable pour l'activité future ; • mémoire historique.
2. Quelle est la criticité des données ?	Chaque type de données ou de document possède plusieurs caractéristiques qui permettent d'organiser son archivage, notamment : • la sensibilité de l'information : confidentielle, unique et difficile à reconstituer, ou au contraire information de routine ou de confort, etc ; • la fréquence et l'urgence de la consultation selon les types de documents ou de données ; ce critère permet d'optimiser le stockage. A noter que ces caractéristiques évoluent avec le temps.
3. Quelles exigences de conservation ?	Le système d'archivage doit assurer la maintenance des données jusqu'à la fin du cycle de vie de l'information. Cette durée peut aller de quelques mois à plusieurs décennies, voire plus d'un siècle. La durée de conservation est déterminée soit en application des textes réglementaires, soit par analogie avec ces textes en fonction du risque de contentieux, soit par métiers en fonction de la réutilisation prévisible de l'information archivée. Un corollaire de la durée de conservation est la date de destruction. La destruction est réglementaire dans certains cas (données à caractère personnel) ; elle permet plus globalement de fiabiliser les données archivées (suppression des données périmées) et d'éviter des coûts inutiles de stockage et de gestion.
4. Quelles exigences d'intégrité et de sécurité ?	Si les données doivent être restituées dans un environnement juridique ou dans le cadre d'un audit, il est impératif qu'elles soient intègres et que leur utilisation ait été tracée depuis la date de leur archivage voire depuis leur création.
5. Quelle volumétrie à traiter ?	Un type de document (facture, e-mail, comptes rendus du comité de direction, etc.) peut représenter des volumes très variables parmi l'ensemble des données de l'entreprise. La maîtrise des volumes est utile : • pour définir les priorités de gestion (les types de données et de documents les plus volumineux seront prioritaires) ; • pour estimer les besoins en stockage (critère à combiner à la durée de conservation) et donc une partie des coûts.
6. Quel accès ?	La question de l'accès comporte deux volets : a) les droits d'accès, définis en fonction du profil des utilisateurs : accès à tout ou partie des informations, restrictions d'accès, évolution dans le temps (vers une ouverture ou une réduction selon les événements) ; b) la possibilité de recherche d'information via des mots-clés (indexation automatique ou manuelle) ou à l'aide d'un moteur de recherche, assorti ou non d'un thésaurus.

Le Cadre

Fiche 2 - Contraintes légales (droit public)

Contexte

Dans le cadre du régime général des archives, il existe une distinction entre les archives publiques et les archives privées. Les dispositions intéressant les archives publiques sont aujourd'hui codifiées dans le livre II du code du patrimoine dont l'article L. 211-4 indique que « Les archives publiques sont :

- Les documents qui procèdent de l'activité de l'Etat, des collectivités territoriales, des établissements et entreprises publics ;
- Les documents qui procèdent de l'activité des organismes de droit privé chargés de la gestion des services publics ou d'une mission de service public ;
- Les minutes et répertoires des officiers publics ou ministériels. »

Les archives publiques sont imprescriptibles, comme le précise l'article L. 212-1 du code du patrimoine et le législateur a admis les supports électroniques avec l'article 1er de la loi du 3 janvier 1979 : « Les archives sont l'ensembles des documents, quels que soient leur date, leur forme et leur support matériel, (...) ».

Enjeux

L'existence des archives publiques se justifie :

- par la nécessité d'apporter la preuve de ses droits et affirmations pour celui qui conserve;
- par l'obligation de conserver certains documents afin de vérifier qu'une personne physique ou morale a bien respecté les obligations auxquelles elle était soumise.

La problématique de la preuve en droit administratif est très différente de celle du droit civil. En effet, en droit administratif, le juge peut recevoir tous les moyens de preuve qui lui sont présentés par les parties au litige (écrit, témoignage,...). Il n'existe pas de preuve parfaite ou imparfaite. Mais pour convaincre le juge, il faut que cette preuve soit fiable.

En conséquence il sera nécessaire que l'écrit sous forme électronique repose sur un procédé garantissant que ces exigences sont remplies. La conservation électronique des actes dématérialisés ou immatériels doit ainsi garantir leur intelligibilité, leur accessibilité dans le temps, leur imputabilité et leur intégrité.

Par exemple en droit public, la passation de marchés publics par voie électronique implique de recourir à l'archivage électronique. La décision d'archiver et le choix des documents correspondants reviennent à l'autorité publique chargée de la passation et/ou de l'exécution des marchés, en collaboration avec l'Administration des Archives.

La fiabilité des documents archivés réside dans la confiance accordée à la personne publique. Dans le cas d'un marché public dématérialisé, c'est la signature électronique de ce marché par la personne publique qui lui conférera le caractère de seul exemplaire de référence. Les autres pièces relatives aux marchés publics destinées à être archivées devront être attestées ou certifiées par la personne responsable du marché.

Recommandations

Quand on parle d'archivage, la première tâche d'une entreprise est d'évaluer ses besoins, c'est-à-dire archiver quoi pourquoi et pour combien de temps ? Pour l'évaluation de ces besoins, il est recommandé de répondre de manière appropriée aux six questions suivantes :

La preuve en droit administratif est libre	Afin de s'assurer de la recevabilité de la preuve par le juge, il convient de porter une grande attention à la fiabilité de la preuve. Le régime prévu en droit privé semble ainsi pertinent (voir fiche 3).
Apport de dématérialisation des marchés publics	La dématérialisation du marché public peut donner lieu à l'introduction d'un nouvel acteur, à savoir d'un prestataire chargé des aspects techniques informatiques.

Compléments

Une notion importante concerne la durée d'utilité administrative qui représente la durée pendant laquelle les différents services ou organismes détenteurs sont tenus de conserver les documents. Cette durée est généralement définie de façon conjointe entre l'administration concernée et le service des archives, en fonction des obligations juridiques mais également en tenant compte des besoins d'information nécessaires à leur bon fonctionnement.

La CADA (Commission d'Accès aux Documents Administratifs), compétente depuis la loi du 12 avril 2000 pour se prononcer sur l'application des dispositions régissant l'accès aux archives, constate que les demandes de documents portent le plus souvent sur l'urbanisme et les documents sociaux.

Les budgets ou comptes administratifs des communes, les procès-verbaux des conseils municipaux, les listes électorales, la liste des personnes assujetties à l'impôt sur le revenu ou à l'impôt sur les sociétés ou encore, le registre tenu par les communes dans lesquels figurent toutes les acquisitions réalisées par exercice du droit de préemption sont des exemples des documents qui doivent être archivés par les collectivités territoriales.

A titre d'exemples, doivent être archivés par l'Administration centrale le casier judiciaire, la liste générale des objets mobiliers classés ainsi que les documents nécessaires à l'élaboration de cette liste, l'accès du contribuable à son dossier fiscal.

Contexte

Les contraintes à respecter dans le cadre du recours à un système d'archivage électronique ont essentiellement pour objectif de permettre de se prévaloir du document archivé. Ces contraintes qui ont par conséquent une vocation principalement probatoire se retrouvent tant dans le droit privé national que dans les textes internationaux et particulièrement dans les directives européennes.

En droit privé :

Avant d'envisager les contraintes liées à la vocation probatoire de l'archivage électronique, il convient au préalable d'opérer une distinction entre les actes juridiques et les faits juridiques :

- un acte juridique est une opération juridique consistant en une manifestation de volonté ayant pour objet et pour effet de produire une conséquence juridique (Ex. : un contrat de bail, l'achat d'un voyage sur internet, le contrat d'abonnement auprès d'un opérateur de téléphonie mobile, etc.) ;
- un fait juridique se définit comme un fait quelconque (événement social, phénomène de la nature, fait matériel), auquel la loi attache une conséquence juridique (acquisition d'un droit, création d'une obligation, etc.) et qui n'a pas été nécessairement recherchée par l'auteur du fait. (Ex. : le délit oblige son auteur à réparer le dommage causé ; la possession d'un immeuble pendant 30 ans fait acquérir la propriété ; une force majeure exonère le débiteur ; plus spécifiquement, en matière électronique, les données de connexion qui sont des informations doivent être conservées par l'opérateur ainsi que par toute entreprise ou particulier).

La qualification d'acte juridique ou de fait juridique aura une incidence sur le système de preuve applicable.

Afin de rapporter la preuve d'un acte juridique, il est en principe nécessaire de produire un écrit passé devant notaire ou signé des parties. Une exception existe cependant pour les actes portant sur un montant inférieur à 1500 €.

L'article 1316-1 du Code civil pose certaines exigences à finalité probatoire pour l'établissement et la conservation d'un acte juridique. L'écrit sous forme électronique sera ainsi admis à titre de preuve à la double condition que :

1. l'auteur de l'acte soit identifié (dans les conditions posées par l'article 1316-4 du Code civil) ;
2. l'acte soit conservé dans des conditions de nature à en garantir son intégrité.

L'utilisation de la signature électronique définie à l'article 1316-4 du Code civil comme « un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache » permet de s'assurer que les deux conditions précédentes sont réunies.

Concernant les faits juridiques, rien n'est précisé quant à leur conservation. Leur preuve est libre. Tous les moyens de preuve sont donc recevables par le juge (présomptions, témoignages, aveux, serments, commencement de preuve écrite, etc.). Néanmoins, afin de convaincre le juge, il faudra établir la fiabilité du procédé utilisé pour archiver les moyens de preuve des faits juridiques. Dans un souci de sécurité juridique, il est alors recommandé de s'appuyer sur les modalités d'archivage s'appliquant aux actes juridiques. Les personnes archivant des documents auraient alors la possibilité, au préalable, de s'assurer de la valeur juridique de ceux-ci. Comme en matière de fait juridique, le principe de la liberté de la preuve s'applique entre commerçants. En effet, le Code de commerce prévoit que « les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi».

N'étant pas d'ordre public, les règles déterminant les moyens de preuve ou encore la charge de la preuve peuvent faire l'objet de conventions. Celles-ci sont un gage de sécurité juridique puisqu'elles vont permettre aux parties de régler à l'avance la question de la force probante des contrats qu'elles concluent en ligne. Dans les contrats de consommation, il est possible d'insérer des clauses aménageant le système de preuve sous réserve, pour le professionnel, de respecter la législation en matière de clauses abusives.

Cette qualification pourra en effet être retenue, et la clause susceptible

par voie de conséquence d'être réputée non écrite, dès lors qu'elle aura « pour objet ou pour effet de créer au détriment du consommateur un déséquilibre significatif entre les droits et obligations des parties au contrat ». Sont particulièrement visées les clauses ayant pour objet de limiter les moyens de preuve dont dispose le consommateur ou encore les clauses qui attribueraient la charge de la preuve à ce dernier alors qu'en principe celle-ci devrait peser sur le professionnel.

En l'absence de telles conventions, c'est au juge que reviendra le cas échéant, le soin de régler les conflits de preuve conformément à l'article 1316-2 du Code civil.

En droit international et dans d'autres Etats :

La Commission des Nations Unies pour le Droit Commercial International (CNUDCI) est à l'origine d'une loi type sur le commerce électronique. Cela tient au fait que, dans un certain nombre de pays, la législation encadrant les communications et l'archivage de l'information est inadaptée voire dépassée, celle-ci n'envisageant pas les problématiques relatives au commerce électronique.

Ainsi, la loi type de la CNUDCI sur le commerce électronique adoptée le 6 décembre 1996 a vocation à s'appliquer « à toute information, de quelque nature que ce soit, prenant la forme d'un message de données utilisé dans le contexte d'activités commerciales ». Elle définit le message de données comme « l'information créée, envoyée, reçue, ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie ». Elle précise que « lorsque la loi exige qu'une information soit sous forme écrite, un message de données satisfait à cette exigence si l'information est accessible pour être consultée ultérieurement ».

Il est donc nécessaire de conserver l'information. De plus, lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données peut satisfaire à cette exigence à condition, d'une part, qu'il existe « une garantie fiable quant à l'intégrité de l'information à compter du moment où elle est créée pour la première fois sous sa forme définitive en tant que message de données » et d'autre part, que l'information puisse être présentée à la personne à qui il est exigé qu'elle soit présentée s'il existe une telle exigence.

Dans le cadre de l'Union européenne, bien que le terme « archivage » ne soit pas directement défini, certaines directives européennes posent des exigences (en matière de support, de conditions de stockage, etc.) tenant à la conservation de divers documents.

La directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs a recours à la notion de « support durable » qu'elle définit comme « tout instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément à 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 ». Cette directive impose au fournisseur de communiquer les conditions contractuelles et les informations préalables au consommateur sur un support papier ou sur un support durable qui est mis à sa disposition et « auquel il a accès en temps utile avant d'être lié par un contrat à distance ou par une offre ».

La référence à un support durable se retrouve également dans la directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance.

Par ailleurs, la directive 2001/115/CE du Conseil du 20 décembre 2001 dont le but est de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée, traite du « stockage des factures » et notamment du « stockage électronique des factures» (ou « stockage des factures par voie électronique »). Il s'agit

d'un stockage effectué « au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et en utilisant le fil, la radio, les moyens optiques ou d'autres moyens électromagnétiques ». Aux termes de la directive, l'authenticité de l'origine et l'intégrité du contenu des factures, ainsi que leur lisibilité, doivent être assurées pendant toute la période de stockage.

Les modalités particulières de conservation propres aux différents documents visés par ces directives ont été précisées les textes de transposition. A titre d'exemple, en application de l'article 17 de la loi de finance rectificative de 2002, l'instruction fiscale du 7 août 2003 a précisé les conditions de conservation des factures électroniques.

Enjeux

L'archivage peut concerner de nombreux types de documents électroniques (courriers électroniques, contrats) et les contraintes à prendre en considération sont multiples.

L'archivage des courriers électroniques peut permettre de contrôler les flux entrants et sortants d'une entreprise afin, notamment, d'éviter la divulgation de secrets ou encore d'être informé d'éventuels comportements répréhensibles commis par un salarié. Cependant, ce type d'archivage reste une opération qui se concilie difficilement avec la nécessité de respecter la vie privée des salariés dans l'entreprise. Des limites tenant à la sphère personnelle de ces derniers doivent nécessairement être respectées et cela indépendamment de l'obligation de confidentialité à laquelle est soumis le tiers archiveur lorsqu'il y est fait recours.

L'article L. 134-2 du Code de la consommation impose au professionnel de conserver pendant 10 ans, l'écrit constatant un contrat en ligne portant sur un montant supérieur à 120 ¤ et de le tenir à disposition du consommateur lorsque celui-ci en fait la demande. Le délai de conservation court à compter de la conclusion du contrat « lorsque la livraison du bien ou l'exécution de la prestation est immédiate ». Si tel n'est pas le cas, « le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci». On peut néanmoins s'interroger sur les éléments que le professionnel est tenu d'archiver en pratique (CGV (conditions générales de vente), commande, signature électronique, etc.) ou encore sur les modalités permettant au consommateur d'exercer son droit d'accès.

La loi pose le principe du recours aux factures électroniques signées dès le moment où le destinataire accepte ces factures. Celles-ci doivent être émises et transmises par voie électronique « dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique ». La durée de conservation des factures électronique dépendra de la matière et des délais de prescription qui s'y rattachent. Le C.G.I. prévoit en outre que les factures, la signature électronique à laquelle elles sont liées ainsi que le certificat électronique attaché aux données de vérification de la signature électronique doivent être conservés dans leur contenu originel par l'émetteur et le destinataire. En matière commerciale, la durée de conservation des factures électronique sera de 10 ans, c'est-à-dire la durée à partir de laquelle se prescrivent

les obligations nées entre commerçants à l'occasion de leur commerce.

Le Code de commerce prévoit que les documents comptables et les pièces justificatives doivent être conservés pendant 10 ans et ce sur tout support. Ils doivent obligatoirement être tenus par le commerçant et être « identifiés, numérotés et datés dès leur établissement par des moyens offrant toute garantie en matière de preuve ».

En application de l'article L. 143-3 du Code du travail, l'employeur est tenu de conserver un double des bulletins de paie qu'il remet aux salariés lors du paiement de leur rémunération pendant une durée de 5 ans. Cette conservation peut s'effectuer sur papier ou sur support informatique dès lors que des garanties de contrôle équivalentes sont maintenues.

Recommandations

La phase d'archivage constitue un élément essentiel dans toute stratégie d'entreprise d'où le respect d'un minimum de précautions :

Distinction entre durée de conservation et durée de prescription	En règle générale, il convient d'éviter de confondre délai de conservation et délai de prescription. Trop souvent, les acteurs du domaine omettent cette distinction. Les textes juridiques mettent en exergue les durées de conservation des documents (6, 10 ou 30 ans par exemple). Mais cette durée peut ne pas suffire si les divers délais de prescription légale ne sont pas expirés, c'est-à-dire si certaines actions judiciaires dans lesquelles tel document est requis sont toujours en cours au moment du terme de la durée de conservation. Ce qui compte, c'est l'extinction des effets juridiques liés à l'acte.
Analyse préalable par type de document	A ce titre, il convient d'effectuer une analyse par type de document pour déterminer les modalités juridiques nécessaires à un archivage fiable. Prévoir ce type de précaution doit permettre d'assurer en cas de litige une certaine sécurité juridique quant à la recevabilité des documents à titre probatoire ou de validité d'un acte.
Courrier électronique	Il est conseillé de mettre en place une charte d'utilisation des moyens informatiques, une politique d'archivage des courriers électroniques au sein de l'entreprise et d'informer le comité d'entreprise, les syndicats et les salariés préalablement à la mise en place d'un système d'archivage. Il sera ainsi possible de prévoir la force probante à accorder aux courriers électroniques (simples commencements de preuve par écrit en principe) et d'assurer une certaine sécurité juridique. Par ailleurs, l'archivage des courriers électroniques doit respecter les dispositions de la loi Informatique et Liberté du 6 janvier 1978 et notamment celles relatives à la collecte et au traitement de données à caractère personnel (ce qui peut être le cas d'une adresse électronique). Il faudra en outre déterminer la finalité du traitement ainsi que la durée de conservation des courriers électroniques archivés.

Préambule

Afin de ne pas surcharger le présent ouvrage, nous nous limiterons ci-dessous volontairement aux contraintes relatives au domaine de la finance sachant qu'il en existe également bien d'autres comme celles correspondant au domaine de la santé.

Contexte

Certaines « affaires » récentes (Enron, Worldcom, Vivendi...) ont mis en péril la confiance dans le monde des affaires, coûtant des milliards de dollars aux actionnaires et petits épargnants.

Les Etats-Unis suivis par d'autres Etats dont la France ont alors pris des dispositions législatives pour instaurer une transparence dans le cadre de la vie financière d'une entreprise, synonyme de confiance pour les actionnaires comme pour le reste de l'opinion publique. Les textes impliquent personnellement les dirigeants par une responsabilisation portant notamment sur la situation financière de leur entreprise.

Le contrôle interne a pour objectif de vérifier avec exactitude la santé financière de l'entreprise. L'archivage des données comptables et financières est un des éléments de ce contrôle interne.

Plusieurs textes fixent, de manière plus ou moins explicite, cette exigence d'archivage des documents en matière financière et bancaire.

Enjeux

Textes américains :

Certains textes sont applicables aux sociétés étrangères. De manière schématique, il s'agit des sociétés faisant appel public à l'épargne aux Etats-Unis.

The « Sarbanes-Oxley Act of 2002 » (SOX)

La loi Sarbanes-Oxley, adoptée en réaction aux scandales financiers très médiatisés, est applicable aux sociétés françaises cotées sur les marchés boursiers américains. La section 404 de la SOX intéresse au premier plan les différentes pratiques d'archivage financier. Elle concerne l'auto évaluation des procédures de « reporting » financier. Ainsi, les données financières de l'entreprise doivent être correctement collectées, traitées et stockées.

Ces procédures concernent d'une manière ou d'une autre les services d'information de l'entreprise. A ce titre, la SOX prévoit la traçabilité de tous les mouvements financiers.

Afin de contrôler la pertinence de l'information financière communiquée, l'entreprise doit être en mesure de disposer de moyens d'archivage et de recherche de l'information archivée. En effet, l'archivage doit être un moyen de vérifier les informations comptables, financières et de gestion communiquées aux organes sociaux. Celles-ci doivent refléter avec sincérité l'activité et la situation financière de la société.

La SOX fixe dans sa section 404 les principes qui dirigeront les travaux de la Commission instituée par le « Securities Exchange Act of 1934 » en matière de contrôle interne. Ces règles sont inscrites dans la « Rule 17-CFR 270.17a-4 »

The « Rule 17-CFR 270.17a-4 »

Cette règle pose de nombreuses exigences relatives à l'archivage :

- prévoir des supports pour l'archivage qui ne soient ni réinscriptibles, ni effaçables ;
- vérifier l'enregistrement automatique des fichiers ;
- prévoir que les originaux soient numérotés et datés ;
- télécharger facilement les index et

enregistrements sur n'importe quel autre support prévu par le texte (micrographie ou support électronique) ;
- donner facilement accès aux agents de la Commission (Securities and Exchange Commission) ainsi qu'aux organismes de régulation aux données archivées ;
- disposer d'une copie fidèle des données archivées que pourraient demander les agents de la Commission ;
- conserver les copies séparément des originaux ;
- organiser et indexer clairement toutes les informations conservées à la fois sur les originaux et sur les copies des données archivées ;
- communiquer aux commerçants ou vendeurs les index destinés aux agents de la Commission et aux organismes de régulation auxquels appartiennent lesdits commerçants et vendeurs pour examen ;
- dupliquer et archiver chaque index séparément de l'original ;
- conserver des index originaux et copiés pendant la durée légale ;
- disposer d'un système d'audit permettant d'analyser la conservation des données originales ou dupliquées ;
- les agents de la Commission et les organisations de régulation dont les commerçants ou vendeurs sont membres doivent pouvoir contrôler la méthodologie utilisée pour l'audit de l'entreprise ;
- préserver les résultats de l'audit pendant la période de temps requise ;
- conserver, actualiser et fournir promptement toute information nécessaire pour accéder aux enregistrements et aux index archivés sur support électronique à la requête des membres de la Commission ou des organismes de régulations.

Les accords Bâle II :

Concernant le secteur bancaire, les accords Bâle II, émanation des pays du G10 auxquels s'est associé le Luxembourg, fixent, entre autres, les obligations concernant la conservation des données par les banques de plus de 100 pays, notamment pour la France, et par toutes les organisations qui dépendent du CECEI (Comité des Etablissements de Crédit et des Entreprises d'Investissements).

Les prescriptions relatives à l'archivage des données se trouvent dans la 2ième partie correspondant au premier pilier sur les exigences minimales de fonds propres, troisième chapitre relatif au risque de crédit (Credit Risk, H, 4, (iv) Data maintenance). Aux termes de ce texte, les banques doivent collecter et conserver les données des emprunteurs ainsi que les caractéristiques de l'emprunt de manière exacte et sincère. Les banques doivent aussi conserver les opérations permettant d'apprécier la méthodologie du « scoring » des emprunteurs et de leurs garants.

Cet accord n'est cependant pas encore obligatoire, dans la mesure où les autorités nationales devront veiller à la mise en application de Bâle II d'ici fin 2006.

Les textes nationaux :

La loi sur la sécurité financière du 1er août 2003 (LSF)

Cette loi est applicable à toutes les sociétés anonymes et consacre la notion de contrôle interne. Cette notion implique de nouvelles mesures d'information au profit des actionnaires et du public, et en conséquence, une obligation d'archivage pour les entreprises assujetties. Ces mesures sont développées dans le cadre de l'arrêté du 31 mars 2005.

La loi sur la sécurité financière ne pose pas, à proprement parler, de corpus de règles applicables à l'archivage. Cependant, cette loi est intervenue à la suite de la SOX. On retrouve donc le même souci de transparence dans la gestion financière de l'entreprise, ainsi que dans la gestion des risques de crédit. Mais, contrairement à la SOX, la LSF ne renvoie à aucun texte pour la mise en œuvre pratique de l'archivage. Le contrôle interne mis en place par la LSF concerne, les données financières, et le fonctionnement du contrôle interne. Ce

texte est applicable à toutes les sociétés anonymes, qu'elles soient cotées ou non cotées. Sont ainsi visées tant les sociétés anonymes à Conseil d'Administration que les Sociétés Anonymes à Directoire et à Conseil de Surveillance (Code de commerce articles L.225-37 et L.225-68). La LSF institue le contrôle interne, sans pour autant mettre en place une procédure précise pour l'archivage. L'archivage qu'implique le contrôle interne est cependant précisé par l'arrêté du 31 mars 2005.

L'arrêté du 31 mars 2005

Cet arrêté précise le contenu du contrôle interne qui doit comprendre :

- un système de contrôle des opérations et des procédures internes ;
- une organisation comptable et du traitement de l'information ;
- un système de documentation et d'information.

Dans des conditions optimales de sécurité, de fiabilité et d'exhaustivité, l'entreprise est tenue de vérifier les conditions d'évaluation, d'enregistrement, de conservation et de disponibilité de l'information, ainsi que de vérifier la qualité des systèmes d'information et de communication.

Les entreprises visées par l'arrêté sont nombreuses puisqu'il est applicable tant au niveau national que pour les entreprises possédant des filiales et des succursales à l'étranger.

L'archivage des informations comptables publiées doit permettre de reconstituer dans un ordre chronologique les opérations de comptabilité effectuées.

Les systèmes d'information doivent permettre de protéger les documents ainsi archivés. L'arrêté ne fixe pas le niveau de sécurité des systèmes. Il doit être apprécié périodiquement par l'entreprise, qui doit mettre en place des procédures de secours en cas de défaillances du système.

Les entreprises doivent conserver jusqu'à la date de l'arrêté des comptes suivant, l'ensemble des fichiers nécessaire à la justification des documents du dernier arrêté remis à la Commission bancaire.

La sélection et la mesure des risques de crédit nécessitent de constituer un dossier de crédit destiné à recueillir l'ensemble des informations nécessaire à l'octroi d'un crédit.

L'arrêté précise les mesures d'enregistrement que doivent prendre les entreprises lors des opérations de change et des opérations portant sur leurs portefeuilles de négociation.

Un système de suivi des opérations est exigé par l'arrêté pour :

- enregistrer sans délai les opérations déjà réalisées ;
- enregistrer à la fin de chaque journée et retracer individuellement toutes erreurs dans la prise en charge et l'exécution des ordres. Le prestataire doit en outre s'assurer qu'il est en mesure d'établir la chronologie des opérations et d'évaluer a posteriori les positions prises en cours de journée.

Les entreprises doivent enfin élaborer et tenir à jour des manuels de procédures relatifs et adaptés à leurs différentes activités. Ces documents doivent décrire les modalités d'enregistrement, de traitement et de restitution des informations, les schémas comptables et les procédures d'engagement des opérations. Enfin, les entreprises doivent mettre en place une documentation qui précise les moyens destinés à assurer le bon fonctionnement du contrôle interne.

Recommandations

Les lois américaines décrivent les différentes étapes du processus d'archivage. Les documents financiers, ainsi que les copies des documents archivés, doivent répondre à une procédure rigoureuse. La "Rule 17-CFR 270.17a-4" pose des principes relatifs aux supports destinés à l'archivage et aux méthodes techniques de l'archivage sur ces supports. Elle décrit aussi les différents organismes qui pourront effectuer des contrôles sur l'archivage. Les données archivées – originaux comme copies – doivent être régulièrement mises à jour. Les enregistrements ne doivent être ni réinscriptibles, ni effaçables. Enfin, il serait judicieux d'archiver les messages électroniques (y compris semble-t-il la messagerie instantanée dans la mesure où cette exigence est imposée expressément par la réglementation américaine) et les données permettant de reconstituer un historique financier. Rappelons ici que ces règles sont applicables à un nombre relativement restreint d'entreprises françaises. Toutefois, on peut penser que le respect de ces dispositions peut constituer un état de l'art en matière de contrôle interne.

Au niveau international, les accords Bâle II ont pour objectif de mettre en place une réglementation sur la gestion des risques lors de l'octroi des crédits par les banques et organismes de crédit. Les mesures relatives à l'archivage concernent les méthodes mises en place pour évaluer les crédits accordés ainsi que les informations sur les emprunteurs et les garants. Aux termes de ces accords, toutes les méthodes et données utilisées aux fins de la conclusion ou du refus d'un crédit doivent être conservées. Cette conservation de données est très vaste, dans la mesure où son analyse doit permettre d'apprécier dans sa globalité les raisons de l'accord ou du refus du crédit. Cette norme n'est cependant pas obligatoire avant fin 2006.

Les mesures nécessaires à la réalisation du contrôle interne mis en place par la loi sur la sécurité financière de 2003 sont nombreuses. Les entreprises concernées le sont aussi puisque sont visées toutes les sociétés anonymes, cotés ou non. Dans des conditions optimales de sécurité, de fiabilité et d'exhaustivité, l'entreprise est tenue de vérifier l'évaluation, l'enregistrement, la conservation et la disponibilité de l'information, ainsi que la qualité des systèmes d'information et de communication. Ces exigences concernent avant tout les documents comptables, dans la mesure où ils sont les premiers indicateurs de la réalité financière de l'entreprise.

Contexte

Les objectifs auxquels doit répondre l'archivage sont multiples. Ces objectifs ne pourront être atteints qu'avec le respect d'un ensemble de mesures dont une grande partie repose sur des aspects purement techniques. Il en est ainsi de l'intégrité, de la sécurité et de la pérennité des données pour lesquelles il faudra savoir gérer et anticiper le principe de l'obsolescence technologique récurrente tout en facilitant leur accès.

Les différentes contraintes peuvent se résumer ainsi :

- retenir un format logique de document par rapport à différents types (image, vectoriel, traitement de texte, éditique, ...) en fonction de divers critères de choix (pérennité, conversion, coût) ;
- choisir un format physique ou type de support (magnétique ou optique) selon différents critères (pérennité, conversion, coût) ;
- analyser les possibilités de migrations tant du point de vue des formats logiques que des supports physiques ;
- prendre en compte certaines spécificités comme celles liées à la signature électronique ;
- avoir en permanence à l'esprit les aspects de performance.

Les contraintes technologiques sont d'autant plus importantes qu'une fois en place, un système d'archivage inefficace aura beaucoup de mal à être corrigé compte tenu du volume d'information à traiter.

Enjeux

Le fait de savoir répondre aux contraintes techniques posées par l'archivage électronique est déterminant afin d'obtenir un système efficace permettant de disposer de la bonne information au moment opportun.
Les enjeux à prendre en considération se retrouvent à différents niveaux :

- technique : si par exemple le système d'accès n'a pas été suffisamment bien étudié tant en termes de définition des index que des outils mis en place, l'information archivée se retrouvera ainsi pratiquement inexploitable car difficilement accessible. Cette difficulté d'accès pourra se trouver au niveau de la recherche proprement dite ainsi qu'au niveau de temps de réponse beaucoup trop longs ;
- juridique : que faire si le format logique utilisé pour conserver l'information a été mal choisi et qu'il ne permet pas l'intelligibilité de l'information lorsqu'on en a besoin ou ne peut garantir son intégrité ?
- réglementaire : face par exemple aux exigences de la CNIL et compte tenu des moyens d'accès mis en place il faudra bien mesurer le respect de la confidentialité des données concernées ;
- sécuritaire : au-delà de la simple réglementation il est évident que les informations archivées ne devront être accessibles que sous certaines conditions pour tout ou partie en fonction des personnes qui interrogent et surtout elle devront être bien protégées grâce à un système de sauvegarde adapté ou tout autre système de redondance de l'information ;
- financier : du fait de l'obsolescence d'un matériel comment effectuer la migration rapide de volumes importants de données à moindre coût et surtout dans des délais raisonnables et sans perturber le fonctionnement au quotidien ?

Face à ces enjeux, la prise en compte des différentes contraintes techniques doit ainsi contribuer à la mise en place d'un système d'archivage efficace répondant aux attentes et, entre autres, à celle de pouvoir évoluer sans pour autant remettre en cause l'existant, grâce à une bonne anticipation des besoins.

Recommandations

Devant l'ensemble des ces contraintes nous donnons ci-dessous les éléments qu'il nous parait primordial de respecter :

Choix du format logique	Sans entrer dans le détail des différents formats disponibles, nous recommandons d'utiliser un format qui permette l'intelligibilité, soit en lecture directe (exemple du TXT), soit par utilisation d'un interpréteur relativement facile à écrire en cas de besoin (cas du PDF). On aura par contre soin d'éliminer tous types de formats propriétaires issus de traitements ou de logiciels dont la pérennité ne peut être assurée.
Choix des supports	Même si dans l'absolu le support idéal existait, ce qui est loin d'être le cas, encore ne faudrait-il pas oublier de prendre en considération les aspects économiques de façon globale. En effet sur ce dernier point il est nécessaire de raisonner non pas sur l'achat ponctuel de tel ou tel support ou technologie mais sur une exploitation simulée de plusieurs années afin d'être bien sûr de prendre en compte l'ensemble des paramètres : administration, maintenance, remplacement, ... Quoiqu'il en soit, le type de support sera avant tout choisi en fonction de critères précis comme la durée de conservation, la criticité des données à conserver, l'accessibilité, la volumétrie et le coût.
Migration	Pour diverses raisons il peut être néanmoins nécessaire de prévoir des migrations au niveau du format logique et des supports physiques. Dans ce cas il faudra particulièrement veiller au type de migration concernée afin d'en évaluer aussi précisément que possible les tenants et les aboutissants tant en matière de coûts qu'en matière du temps nécessaire et de l'indisponibilité éventuelle de l'information.
Système d'accès	Dans la mesure où il s'agit de la mise en place du système destiné à retrouver une information de façon efficace, l'on devra être particulièrement vigilant. En effet dans le cas d'un système d'indexation classique rappelons qu'une base de données, si performante soit-elle, pourra se trouver vite limitée en termes de performance. De plus si certains critères de recherche ont été oubliés il est toujours délicat voire très difficile de les ajouter ensuite. De même un moteur de recherche peut se révéler totalement inefficace à cause du phénomène de bruits parasites renvoyant systématiquement une multitude de réponses inexploitables à chaque recherche. Dans les deux cas qui précèdent, l'information archivée deviendrait ainsi quasi inaccessible et serait pour ainsi dire perdue.
Sécurité /sauvegarde	Sans oublier que le système d'accès doit également être vu comme un contrôle au niveau des droits à l'information archivée, encore faudra t-il mettre en place les systèmes et procédures ad hoc destinés à garantir tant la confidentialité que l'intégrité des données. Afin de renforcer la notion de preuve il est également nécessaire de prévoir un système de traçabilité permettant de garder la trace de l'ensemble des interrogations effectuées. Enfin, au-delà des éléments de sécurité évoqués précédemment, il ne faut surtout pas oublier un élément fondamental de sécurité qui est celui relatif à la sauvegarde de l'information ou tout autre système de redondance des données qui doit permettre en cas de sinistre de ne pas perdre l'information.
Evolutivité	Dans la mise en place de tout système d'archivage il est important de prévoir l'évolution de la volumétrie des données à conserver afin d'anticiper les augmentations de capacité des différents matériels et plates formes, voire d'envisager certaines migrations. La prise en compte de cette évolutivité est en effet fondamentale quant au choix des technologies à utiliser.
Anticipation	Enfin le fait de pouvoir anticiper suffisamment certains types de problèmes est également important pour éviter toute rupture dans le service d'archivage mis en place. Ainsi la signature électronique impose en fonction des procédures retenues, de re-signer les documents tous les trois ans ou tout au moins de les horodater à nouveau afin de profiter des dernières technologies en matière de cryptographie et d'éviter ainsi tout risque de falsification. Il est clair qu'il est préférable d'avoir prévu ce type de traitement dès le départ si l'on veut s'éviter de fortes déconvenues comme la remise en cause d'une information quant à son identification ou son intégrité, lui retirant du même coup toute sa valeur de preuve.

Contexte

La question de l'assurance est essentielle à tout système d'archivage. En effet, un dysfonctionnement du système peut déclencher de graves préjudices pour l'entreprise utilisatrice. La perte d'informations constitue un risque vraisemblable et souvent peu pris en compte dans le cadre de systèmes d'information (exemple : pertes des adresses mail des clients ou de l'ensemble des données clients). Le système d'archivage devra donc être analysé pour déterminer l'impact d'un dysfonctionnement en terme de risques.

Il est aujourd'hui possible de s'assurer contre les atteintes aux informations (couverture de l'information elle-même et des pertes résultant de cette altération). Une assurance des supports des données et de la reconstitution en cas de dommages aux supports ou une assurance de la reconstitution des données altérées ou perdues pour une raison quelconque semble indispensable dans le cadre de l'archivage.

Les risques peuvent également être constitués par les dommages immatériels, relatifs aux valeurs incorporelles, tels que la destruction volontaire ou involontaire des données, la divulgation d'informations, la mauvaise qualité des programmes, du fait d'une altération volontaire ou par simple négligence, l'exploitation ou l'utilisation anormale des données archivées.

Il est donc indispensable d'avoir une évaluation précise des risques, effectuée à partir d'un « audit des risques informatiques ». Il existe plusieurs méthodes dont les plus connues et les plus pratiquées sont les suivantes :

- MEHARI (MEthode Harmonisée d'Analyse de RIsques), mise au point par le CLUSIF (Club de la sécurité des systèmes d'information français). Elle succède en quelque sorte, quatorze ans après, à la méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux). La caractéristique intrinsèque de la méthode MEHARI est de permettre, non seulement l'évaluation réaliste des risques mais également le contrôle et la gestion de la sécurité de l'entreprise sur court, moyen et long termes, quelle que soit la répartition géographique du système d'information. https://www.clusif.asso.fr/

- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), conçue par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), placée sous l'autorité du SGDN (Secrétariat Général de la Défense Nationale), qui dépend lui-même du Premier ministre. EBIOS est une méthode d'appréciation et de traitement des risques relatifs à la sécurité des systèmes d'information. http://www.ssi.gouv.fr/

- COBIT (Control Objectives for Information and related Technology), créée en 1996 par l'ISACA (Information System Audit & Control Association), diffusée en France par l'AFAI (Association Française de l'Audit et du Conseil Informatique). La méthode décompose tout système informatique en 34 processus regroupés en 4 grands domaines. http://www.isaca.org/, http://www.afai.fr/

- FISCAM (Federal Information System Controls Audit Manual), rédigé en 1999 par l'AIMD (Accounting and Information Management Division) dépendant du GAO (General Accounting Office). http://www.gao.gov/

- CISA (Certified Information Systems Auditor), reconnu par l'ISACA (voir COBIT).

Signalons que certains courtiers ou compagnies d'assurance proposent également leur propre système d'évaluation des risques comme par exemple le « Netscoring » mis en place par MARSH.

Enjeux

Dans le cadre de l'entreprise, il se peut qu'une perte d'information se produise, due à des erreurs de saisie, de transmission, d'utilisation des informations, des erreurs d'exploitation, de manipulation du système ou des supports. Se pose ainsi la question de savoir dans quelle mesure les polices d'assurances couvrent ce type de dommages immatériels indirects.

Ces derniers sont garantis par un contrat connu sous le nom d'« extension des risques informatiques ». Une simple « assurance bureautique », visant à couvrir les pertes matérielles directes (destruction, détérioration, incendie, explosion, dégât des eaux...) subies par l'assuré ne jouera pas dans le cadre d'une perte de données.

En effet, les juges ont une conception très précise de la perte de données. Ainsi a-t-il été jugé qu'une police d'assurance ayant pour objet de ne réparer que les dommages matériels directs n'avait pas vocation à couvrir les pertes de données (CA Paris, Sté CPP c/ Compagnie Zurich Assurances, 2 nov. 2003).

Il convient donc de faire particulièrement attention au choix de la police d'assurance, en prenant garde de bien préciser dans quelle mesure les dommages immatériels indirects sont pris en compte dans le contrat.

Dans le domaine des prestations informatiques de tiers archivage, deux assurances semblent particulièrement adaptées :

- l'assurance responsabilité civile professionnelle couvre les dommages que peut subir le client dans le cadre de l'exécution d'un contrat de prestations de services à la suite d'une faute commise par le tiers archiveur, sur deux plan :
  - délictuel ou quasi délictuel, lorsque les dommages causés sont le fait des préposés, des matériels ou de l'installation ;
  - contractuel, lorsque les dommages sont la conséquence d'un manquement à une obligation contractuelle.

Elle a pour objet de couvrir la responsabilité de l'assuré à l'égard des tiers victimes. Dans ce sens, une assurance contre les risques professionnels permet au prestataire, dans le cadre d'un contrat de prestations informatiques, d'être couvert dans les limites prévues par la police des conséquences des dommages causés à l'occasion de l'exercice de cette activité de tiers archivage. Ainsi, les polices de type responsabilité civile d'exploitation, relatives aux dommages causés du fait du personnel ou du fait des locaux semblent appropriées pour couvrir ce type de risque.

- l'assurance de responsabilité du Syntec informatique (Chambre syndicale des SSII et des éditeurs de logiciels) est destinée aux sociétés de services informatiques adhérentes. Il s'agit d'une police de type coopératif. Elle permet de garantir les conséquences financières supportées par un client de l'assuré à la suite de dommages dont il serait responsable.

Cette assurance est adaptée à la problématique de l'archivage dans la mesure où elle prend en compte les dommages causés aux matériels et documents divers nécessaires à l'activité de l'assuré qui lui sont confiés pour exercer son activité professionnelle. Sont notamment garantis les dommages qui sont la conséquence directe d'une faute de manipulation des préposés de l'assuré.

Les dommages couverts peuvent être matériels ou immatériels. Les dommages matériels résultent de la destruction ou de l'endommagement des matériels informatiques ou de l'atteinte corporelle subie par une personne physique. Les dommages immatériels peuvent consister en des pertes de résultat d'exploitation consécutives à une perte du chiffre d'affaires, de client ou de déficit d'image, par exemple. Pour l'archivage, la perte de données relative à la comptabilité pourrait causer d'une part, la perte d'une preuve amenée à être utilisée en justice, d'autre part, un fort coup financier dans le cadre d'un redressement fiscal par exemple.

Recommandations

Audit indispensable	Un audit des risques informatiques est incontournable aux fins de choisir la police d'assurance la mieux adaptée.
Assurance interne de perte de données	La perte de données en interne doit faire l'objet d'une assurance particulière, car elle n'a pas vocation à être couverte par les polices généralistes.
Assurance du tiers	La responsabilité vis-à-vis des tiers, enjeu particulièrement important dans le cadre de l'archivage, doit être, elle aussi, couverte par une police d'assurance spéciale.
Valeur de l'information	Il faudra également être attentif au fait que dans le cadre d'un service de tiers archivage, le client voudra connaître au préalable le montant de son indemnisation en cas de sinistre de son prestataire. Savoir à ce niveau que des assurances spécifiques existent permettant de couvrir la valeur désirée par le client.

Contexte

Les données archivées dans l'entreprise constituent un ensemble complexe dont le volume ne cesse de croître. Cet ensemble se présente sous des formes et des supports variés (y compris papier), selon des flux très divers doit pouvoir être restitué dans un contexte juridique ou utilisé par les équipes métiers pendant une durée parfois longue et enfin se voit rapidement confronté à l'obsolescence technologique.

Bien sûr, l'archivage vise plutôt la fin du cycle de vie des données mais il s'avère que la maintenance des données tout au long du cycle de vie dépend aussi bien de la gestion après la capture dans le système d'archivage que de la qualité des données archivées au moment de cette capture.

Un bon archivage fait intervenir des choix à plusieurs niveaux : critères de sélection des données, choix des formats et supports, règles et mesures de sécurité, mise à disposition et droits d'accès, outils de recherche, matériels et logiciels de stockage, gestion interne ou externalisée, règles et procédures de destruction, compétences et coûts de gestion.

On peut donc véritablement parler de « stratégie d'archivage » car la direction de l'entreprise doit arbitrer plusieurs options de gestion, selon les risques et les coûts identifiés.

Enjeux

La stratégie d'archivage de l'entreprise doit anticiper les conséquences de la non disponibilité de l'information, aussi bien dans un environnement réglementaire ou juridique, que dans le cadre d'une gestion saine du patrimoine informationnel de l'entreprise.

La stratégie d'archivage doit ainsi être globale et :

- adaptée aux besoins de l'entreprise : si elle est sous-dimensionnée, les besoins fondamentaux de restitution de l'information risquent de ne pas être satisfaits ; si elle est surdimensionnée, elle sera trop contraignante pour les utilisateurs et trop coûteuse ; de même les enjeux sont différents selon les activités de l'entreprise, son ancienneté, la taille et le flux des données et leur criticité ;
- cohérente avec la politique générale de l'entreprise : une politique de sécurité très rigoureuse ou une démarche qualité très poussée ne peuvent donner tous leurs fruits sans une politique d'archivage de même niveau ; si l'entreprise a un système de gestion des connaissances très développé, il est logique d'avoir un système d'archivage en conséquence pour pérenniser ces connaissances.

Recommandations

Pour définir et promouvoir une stratégie globale d'archivage dans l'entreprise, on peut énoncer les recommandations suivantes :

Elaboration et diffusion d'un document stratégique	Il est important que les grands principes d'organisation de l'archivage soit mis par écrit et validés par la direction générale. Il est même souhaitable que ce document soit opposable aux collaborateurs de l'entreprise. Ce document sera préparé par un groupe de travail qui étudiera et proposera à la direction générale des choix sur les aspects présentés dans la suite du tableau. Ce document s'intitulera de préférence « politique d'archivage », mais pourrait également s'appeler « charte d'archivage », etc.
Groupe de travail pluridisciplinaire	L'archivage concerne plusieurs acteurs dans l'entreprise. En conséquence la définition d'une stratégie cohérente d'archivage suggère de solliciter les différents acteurs en présence : • direction de systèmes d'information ; • juriste ; • équipes métiers ; • archiviste, responsable documentaire ou records manager. Ce groupe de travail tiendra compte des documents de référence déjà existant sur la sécurité, la qualité, les contraintes juridiques, l'accès à l'information, les règles de conservation, etc. pour élaborer le document à soumettre à la direction générale.
Risques	Après avoir identifié les contraintes réglementaires en vigueur, au plan national et le cas échéant international il s'agira d'évaluer les risques qu'il y a à archiver ou à ne pas archiver. Il sera également utile d'analyser les incidents qui ont pu avoir lieu en lien avec des dysfonctionnements d'archivage : données perdues, données indûment détruites, données confidentielles divulguées, document introuvable car non indexé ou mal décrit, données anciennes illisibles, etc.
Archives papier	Même si l'archivage électronique se développe, il reste qu'un certain nombre de documents continuent d'être produits, archivés et conservés sous forme papier. Or il convient bien évidemment de gérer les stocks d'archives papier pour les durées requises, parfois pluri décennales sachant que le support n'est pas discriminant pour la définition de la valeur d'archive dans la mesure où les données de l'entreprise, quel que soit leur support, forment un tout. La stratégie d'archivage doit être globale. Il est ainsi recommandé que les principes définis pour l'archivage électronique s'appliquent aux archives papier dans le sens où il est important pour l'entreprise d'avoir une visibilité globale de toute son information archivée.
Qualité des données	Les données et documents à archiver doivent être créés de manière à ce qu'ils soient archivables : informations complètes, référencées, validées et datées. Il faut par ailleurs veiller à ne pas créer des informations confuses, fausses ou non autorisées, notamment en poliçant l'utilisation de la messagerie électronique. La qualité touche aussi le problème de la fiabilité des données et de la redondance. Ainsi pour les données produites en interne, le principe de l'archivage effectué par l'émetteur peut être avantageusement retenu.
Responsabilités	Plusieurs niveaux de responsabilité existent dans la gestion du cycle de vie de l'information archivée et ils doivent être identifiés et décrits : • producteur de l'information ; • propriétaire (qui a la maîtrise du contenu et valide la durée de conservation) ; • gestionnaire de l'information ; • utilisateur ; • administrateur du système d'archivage.
Externalisation	La question de l'externalisation de l'archivage se pose pour l'archivage électronique comme pour l'archivage papier. Les principaux critères de l'externalisation sont la qualité du service (compétences et systèmes spécifiques disponibles ou non en interne), le coût global de l'archivage, le rôle joué par un tiers dans le dispositif (voir la fiche « tiers archiveur »)
Réorganisation de l'entreprise	La politique d'archivage doit être suffisamment générale pour ne pas être remise en cause lors des inévitables réorganisations de l'entreprise : restructuration, fusion, rachat, suppression d'entités. Le devenir des données archivées des entités qui changent de statut doit être anticipé, notamment la responsabilité du stockage et les incompatibilités éventuelles des systèmes d'archivage électronique des différentes entités.
Procédures	La stratégie d'archivage doit être déclinée par un certain nombre de procédures d'organisation comme celles de la sélection des données, de la maintenance au plan technique, de l'accès et de la destruction (voir outils méthodologiques, fiche n°10)

Contexte

Dans un environnement où les technologies ne cessent d'évoluer et de gagner en performance extrêmement rapidement, il semble tout à fait paradoxal de rechercher un système destiné essentiellement au moyen et au long terme, rôle pourtant assigné à l'archivage. A l'inverse le fait que les technologies évoluent laisse à penser que l'on devrait être capable de trouver la réponse aux besoins des entreprises qui sont pour le moins variés quant aux différents types de données à conserver, sur quelle durée et avec des volumétries très variables.
Sur ce dernier point nous sommes aujourd'hui largement familiarisé avec la notion de gigaoctets (Go) et les mégaoctets (Mo) sont pratiquement oubliés ; rappelons tout de même que 100 mégaoctets (Mo) représentent le contenu d'une pile de livres de 1 mètre de haut. On parle même de plus en plus de téraoctets (To 1012 octets), voire de pétaoctets (Po 1015 octets) et pourquoi pas bientôt d'hexaoctets (Ho 1018 octets) et autre zettaoctets (Zo 1021 octets) ou yottaoctets (Yo 1024 octets). A titre indicatif 2 téraoctets (To) correspondent à tous les ouvrages d'une bibliothèque universitaire et 2 pétaoctets (Po) aux fonds de toutes les bibliothèques universitaires des EtatsUnis !
En ce qui concerne les différentes technologies disponibles à ce jour disons qu'il existe en fait deux grands types de supports : magnétiques et optiques. Pour ce qui est de l'utilisation des hologrammes ou des nano technologies il faudra encore attendre un peu avant de pouvoir disposer de supports véritablement exploitables et présentant une nette amélioration tant en capacité qu'en temps d'accès par rapport à ceux existants.

Les supports magnétiques : d'un point de vue technique, s'agissant d'informatique et donc d'un environnement binaire, il faut être capable de repérer deux états représentants respectivement le 0 et le 1. Ceci est obtenu sous l'effet d'un champ magnétique, par polarisation dans un sens ou dans l'autre des particules d'oxyde de fer présentes à la surface du support. L'on distingue essentiellement deux grandes familles de supports magnétiques, les bandes magnétiques et les disques.

Les bandes se présentent sous plusieurs formats DAT (Digital Audio Tape), DLT (Digital Linear Tape), LTO (Linear Tape-Open), AIT (Advanced Intelligent Tape) pour ne citer que les plus connus. Les différences sont directement fonction des capacités, des débits ainsi que de la longévité annoncée par les fabricants. Une bande au format ultrium LTO3 permet par exemple d'atteindre des capacités de quelque 400 Go. Quoiqu'il en soit l'usage de juke box est néanmoins indispensable lorsqu'il s'agit d'archivage afin de pouvoir atteindre des capacités de l'ordre du To.
En ce qui concerne les disques plusieurs technologies existent qui sont plus particulièrement dédiées à l'archivage du fait de la conjonction de deux phénomènes. Le premier est incontestablement une réduction drastique des coûts grâce à l'utilisation de la norme SATA (Serial Advanced Technology Attachment) disposant d'une connectique simplifiée.
Le second phénomène résulte de l'évolution de la notion même de WORM (Write Once Read Many) initialement purement physique, vers un aspect plus logique. Sans vouloir être exhaustif nous pouvons citer différents constructeurs et technologies associées : EMC (Centera), HP (RISS pour Reference Information Storage System), HITACHI (Data Retention Utility), IBM (TotalStorage DataRetention x50), Network Appliance (Snap Lock). Ces technologies à base de disques permettent d'atteindre des capacités de l'ordre du Po.

Les supports optiques : par rapport à la technologie magnétique la différence entre le 1 et le 0 se fait en réalité sur la présenceou l'absence d'un « trou » dans le support. Au moment de la lecture le rayon laser traverse donc plus ou moins de matière et génère du même coup un courant plus ou moins fort. Tout comme pour les supports magnétiques l'on distingue deux grandes familles de supports optiques, celle des CD et DVD et la famille des disques magnéto optiques (MO) et UDO (Ultra Density Optical).

La différence entre ces supports réside dans le fait qu'ils sont ou non réinscriptibles et dans leur capacité de 700 Mo pour un simple CD à plus de 30 Go pour un disque UDO. Cette dernière technologie offre la performance du disque magnéto optique de 5,25", la longévité des disques non réinscriptibles de 12" et la rentabilité du DVD. Tout comme pour les bandes il existe des juke-box destinés essentiellement

aux MO et UDO pouvant atteindre plusieurs To lorsqu'ils sont utilisés avec des disques UDO.

Enjeux

Le choix d'une solution technique d'archivage comporte essentiellement deux enjeux:

1. le premier des enjeux consiste à trouver la technologie la mieux adaptée à ses besoins. En effet, ainsi que nous l'avons évoqué précédemment les entreprises sont loin d'avoir toutes les mêmes besoins en matière de volumétrie, d'accessibilité et de durée de conservation des données archivées.

2. le second des enjeux sera essentiellement d'ordre économique afin de bien prendre en compte les aspects opérationnels du système sous l'angle de son exploitation. En effet à quoi servirait de retenir par exemple une technologie sur bandes, a priori la moins chère au gigaoctet stocké, si cela nécessite par ailleurs et compte tenu de la durée envisagée, de nombreuses opérations en matière de tests de relecture, voire de migrations qui auront pour principal mérite d'augmenter très fortement le coût global de l'archivage.

Recommandations

Pour choisir une technologie d'archivage, plusieurs points devront être étudiés :

Evaluer les besoins d'archivage identifiés	La première chose à faire consiste à bien définir ses besoins : • volumes de données ; • types de données (entre autres données à valeur légale ou non) ; • durée de conservation des données ; • fonctionnalités de gestion et de consultation, exigences de traçabilité et de destruction ; • etc.
Evaluation des systèmes existants	A partir des besoins, il est important d'évaluer en quoi les systèmes existants y répondent ou n'y répondent pas. Il est recommandé de prendre en considération le fait que très souvent existent des pratiques d'archivage sur des systèmes parallèles (disques partagés, disques personnels).
Interopérabilité et partage de ressources	La question de l'interopérabilité est fondamentale afin de ne pas s'enfermer dans un système « propriétaire », si performant soit-il d'autant que le plus souvent, l'outil devra pouvoir communiquer avec les autres composantes du système d'information ou partager des ressources.
Mutualisation	Il peut être intéressant dans le cadre d'une première implémentation d'un système d'archivage électronique de le considérer comme un véritable backbone d'archivage destiné à être mutualisé avec d'autres besoins déjà identifiés ou à venir et de prévoir ainsi son évolutivité.
Temps d'accès	Le temps d'accès à l'information est un critère important qui dépend largement du besoin de chaque entreprise : soit l'accès à l'information archivée est toujours urgent de l'ordre de la seconde, soit il peut attendre plusieurs minutes voire davantage. D'où l'importance de bien définir ses besoins avant d'entamer la recherche de la solution la mieux adaptée.
Montée en charge et volumétrie	C'est un point difficile à évaluer réellement lors d'une simple présentation. Dans la mesure où la question de la volumétrie est importante et doit être assortie de performances constantes en matière d'accès, il faudra obtenir des garanties du fournisseur. La visite d'un site en exploitation chez un de ses clients est également fortement conseillée.
Stockage	Vérifier si les modalités de stockage correspondent aux besoins et aux souhaits de l'entreprise, à savoir en ligne (on line), en différé (off line) ou en léger différé (near line).
Coûts directs et coûts associés	Plutôt que de considérer un simple prix d'achat de matériel et des supports il est recommandé de faire une simulation d'exploitation sur au moins trois ans sans oublier d'y inclure les coûts associés comme celui de la maintenance.
Autres coûts	Afin d'éviter toute surprise il est également prudent de prendre en compte d'autres coûts comme : • administration du système ; • migration des données et améliorations du matériel ; • besoin d'entretien et manutention des supports ; • copie de sécurité ; • autres facteurs propres à l'installation.
Pérennité du constructeur/éditeur	La pérennité du constructeur est à prendre en considération même si effectivement rien ne peut la garantir à 100 %. Ainsi la reprise ou le transfert des données, doivent être précisément envisagés (modalités et coût).
Réorganisations de l'entreprise	Les réorganisations (y compris les fusions et acquisitions) font partie des événements courants de la vie des entreprises. Il est ainsi préférable que les systèmes d'archivage soient compatibles ou du moins qu'on puisse mutualiser les outils de recherche.

Contexte

Le marché propose aujourd'hui un panel assez large et diversifié de solutions d'archivage qui se précise et se complète d'année en année. La typologie des produits va du coffre-fort à la solution générale qui englobe l'archivage dans la gestion du cycle de vie complet des données (ILM). Les produits du marché mettent tantôt l'accent sur la gestion de contenu, tantôt sur l'archivage légal (l'expression est répandue mais il serait plus exact de dire « archivage à des fins de preuve »). Ils visent tantôt l'ensemble des données de l'entreprise (incluant parfois les données sur les archives papier), tantôt un type d'information ou un format de document bien spécifique, tel que les messages électroniques.

De même, les entreprises clientes ont des besoins et des attentes variés :

- données à archiver essentiellement sur le court ou moyen terme, ou au contraire sur le long terme ;
- petaoctets (Po) de données scientifiques ou gigaoctets (Go)de documents à valeur probante ;
- entreprise régionale ou internationale avec de nombreuses filiales ;
- etc.

La recherche d'un logiciel correspond à la meilleure relation entre son besoin et l'offre du marché. Toutefois tous les besoins identifiés n'ont pas encore trouvé leur solution d'archivage idéale. Par exemple, l'extraction de données des ERP pour les archiver en fonction de leur durée de conservation respectives reste un problème non résolu.

Enjeux

On peut dire que le choix d'une solution d'archivage comporte deux enjeux principaux :

1. le premier est de sélectionner l'outil le mieux adapté à sa situation. En effet, les entreprises n'ont pas les mêmes besoins du fait d'un certain nombre de caractéristiques : taille et ancienneté de l'entreprise, types de données et de processus, volumes en cause, avantages et inconvénients des systèmes existants, exigences particulières de sécurité, fréquence des consultations, part réciproque de la gestion de la traçabilité (intégrité, suivi des modifications, pérennité) et de la gestion des connaissances (exploitations des contenus), etc ;

2. le second est de ne pas minimiser les aspects organisationnels de l'archivage, avant et à côté des aspects techniques. Il arrive que des processus bien rôdés trouvent facilement un logiciel d'archivage ; dans d'autres cas, ce ne sont pas tant les logiciels qui ne sont pas adaptés aux processus et aux données que l'inverse ! Il n'est pas rare en effet que les processus doivent être repensés pour que la solution technique procure toute son efficacité. En amont, le processus et les données doivent être « lissés » pour éviter de complexifier inutilement les fonctionnalités de l'outil. Par exemple, le fait de conserver un raisonnement « papier » en choisissant un outil, ou le fait de faire des développements en dehors des besoins réels des utilisateurs, peuvent conduire à des lourdeurs dommageables qui ne sont pas le fait de l'outil au départ. En aval, il ne faudra pas négliger l'accompagnement du changement pour les utilisateurs, de façon à ce que des systèmes parallèles ne subsistent pas, ou pire, ne se créent pas, sous prétexte que le logiciel ne répondrait pas à certains besoins des utilisateurs, ou que ceux-ci croiraient qu'il n'y répond pas.

Recommandations

Pour l'acquisition d'un logiciel d'archivage, plusieurs points devront être étudiés :

Chiffrer les besoins d'archivage	La première étape est de définir ses besoins : • gestion du cycle de vie des données y compris la phase d'archivage, gestion du cycle d'archivage dès la création (à partir du moment où les données ne sont plus modifiées) ou archivage secondaire (après une phase d'archivage actif) ; • volumes et types de données ; • fonctionnalités de gestion et consultation, exigences de traçabilité et de destruction ; • etc.

Evaluation des systèmes existants	Le besoin une fois défini, il est important d'évaluer en quoi les systèmes existants y répondent ou n'y répondent pas. Il est recommandé de prendre en considération le fait que très souvent, à côté des systèmes « officiels » gérés par la direction des systèmes d'information, il existe des pratiques d'archivage sur des systèmes parallèles (disques partagés, disques personnels, gravage de CD, etc.).
Solution du marché, logiciel libre ou développement spécifique ?	Chacune de ces approches a ses partisans. L'essentiel est de bien prendre la mesure de ses choix, étant entendu que les changements de politique auront un coût qu'il vaut mieux connaître et si possible éviter. On trouve dans la presse spécialisée un certain nombre de témoignages d'abandon du marché vers le libre et du libre pour revenir au marché. Dans les deux cas, il est souhaitable de prendre en compte les questions techniques de récupération des données et de maintenance. Il est recommandé de limiter le développement spécifique à des projets eux-mêmes très spécifiques pour lesquels, même après reconfiguration des processus (cf ci-dessus enjeu n° 2), le marché ou le libre n'offre aucune solution satisfaisante.
Interopérabilité et partage de ressources	La question de l'interopérabilité est fondamentale sauf dans les cas particuliers où la communauté d'utilisateurs serait par définition limitée et fermée. Le plus souvent, l'outil devra pouvoir communiquer avec les autres composantes du système d'information ou partager des ressources telles qu'une base de données ou un thésaurus avec d'autres applications. L'interopérabilité avec l'extérieur, même pour un outil d'archivage, peut être un besoin fort et doit être étudiée.
Facilités d'indexation	Vérifier les facilités d'indexation automatique et d'indexation par mots-clés et surtout la complémentarité ou la co-existence des deux systèmes, en fonction des besoins exprimés par les utilisateurs. Garder à l'esprit le fait que l'offre technologique accroît les besoins des utilisateurs. Vérifier éventuellement que l'outil permet de hiérarchiser les résultats de recherche et de faire des recherches en cascade.
Accès (temps)	Le temps d'accès à l'information est un critère de choix mais qui dépend largement du besoin de chaque entreprise : soit l'accès à l'information archivée est toujours urgent (besoins de chercheurs ou de juristes par exemple), soit il peut attendre plusieurs minutes voire davantage. Là encore, il est préférable d'avoir défini ses besoins avant la recherche de la solution satisfaisante.
Accès (sécurité)	De la même façon, les données archivées peuvent être hautement confidentielles (données commerciales) ou en partie publiques (certaines données administratives ou documentaires). Cet aspect devra être évalué en fonction du besoin identifié.
Montée en charge et volumétrie	C'est un point qui ne peut être évalué lors d'une simple démonstration. Si la question de la volumétrie est importante, il faut obtenir des garanties de l'éditeur et une démonstration grandeur réelle sur site de l'éditeur ou chez un de ses clients.
Stockage	Vérifier si les modalités de stockage correspondent aux besoins et aux souhaits de l'entreprise : en ligne (on line), en différé (off line) ou en léger différé (near line).
Coût du logiciel	Analyser l'ensemble des éléments de facturation : serveur, client, microprocesseur. Il est fortement recommandé de faire une simulation d'exploitation sur trois ans.
Coûts associés	Dans cette simulation d'exploitation, il ne faudra pas oublier d'inclure les coûts associés de maintenance (évolutive ou corrective) voire d'autres types de coûts.
Pérennité du fournisseur/éditeur	La pérennité du fournisseur est à prendre en compte même si rien ne peut la garantir à 100 %. Ainsi la reprise ou le transfert des données, la récupération des codes sources doivent être précisément envisagés (modalités et coût).
Réorganisations de l'entreprise	Les réorganisations (y compris les fusions et acquisitions) font partie des événements courants de la vie des entreprises. Il est préférable que les systèmes d'archivage soient compatibles ou du moins qu'on puisse mutualiser les outils de recherche. Ceci plaide aussi pour des solutions modérément sophistiquées et des procédures unifiées.
Unicité du logiciel d'archivage	L'unicité du logiciel d'archivage pour l'ensemble de l'entreprise ou du groupe n'est pas systématiquement l'idéal. Plusieurs logiciels peuvent ainsi cohabiter si cela est justifié par un partage des périmètres et des fonctionnalités (dans l'espace ou dans le temps) d'où l'importance de l'interopérabilité.

Contexte

Les solutions techniques ne suffisent pas à gérer l'archivage. Une part non négligeable du processus d'archivage s'appuie sur des outils méthodologiques qui aident à clarifier les besoins, à organiser le périmètre documentaire et à accompagner le cycle de vie des informations archivées.

On connaît les problèmes posés par l'accroissement exponentiel du volume des données (notamment pour la messagerie électronique) de même que les problèmes posés par l'obsolescence des formats, des supports et des outils de lecture. Mais l'hétérogénéité des données est un défi tout aussi difficile à relever.

En effet, on constate que l'information est variée, pléthorique, redondante (recopie des données ou recouvrement de l'information), pas toujours finalisée ni validée ou, du moins, pas tracée comme elle le devrait. De fait, les questions que posent de plus en plus les décideurs et les utilisateurs sont :
quelles données et quels documents archiver ? à quel moment ? pendant combien de temps ? comment les retrouver quand j'en aurai besoin ? feront-ils foi face un à audit ou lors d'un contentieux ?

Il n'est pas possible de transposer dans le monde numérique des processus élaborés naguère dans un environnement contraint par la matérialité du papier. L'informatique permet plus et exige plus. Il faut donner plus d'attention à la granularité de la donnée et à la traçabilité de l'information.

Diverses initiatives ont été prises au niveau national et international pour répondre à ces nouveaux défis. Des normes existent dont il est utile de s'inspirer pour gagner du temps, fiabiliser l'archivage et optimiser la gestion de l'information.

Enjeux

L'enjeu de l'archivage « méthodique » est de maîtriser non seulement la forme mais aussi le contenu de ce que l'on archive. Si on ne peut retrouver l'information ou que cette information n'est pas fiable, l'archivage n'a tout bonnement servi à rien.

On le voit bien pour la messagerie électronique : archiver des messages incomplets ou incompréhensibles parce que rédigés en style télégraphique avec des allusions équivoques, présente un intérêt limité. Ainsi stocker pendant des années des giga ou teraoctets de mails dont on sait pertinemment que plus de 90 % sont périmés et ne produisent que du bruit dans les requêtes est inutilement coûteux. Et pourtant, les quelques pourcents de mails « archivables » doivent pouvoir être traités pendant leur durée d'utilité, qui peut atteindre 10 ans ou plus. Il est vrai que si la création des messages était soumise à des règles de gestion plus rigoureuses, les mails sensibles seraient plus faciles à identifier et leur archivage plus facile à automatiser.

Recommandations

On peut distinguer trois outils méthodologiques majeurs pour un bon système d'archivage :

1. l'énoncé par la direction générale des principes directeurs ou politique d'archivage (policy) au niveau global de l'entreprise : définition des données documents de l'entreprise (par opposition aux documents de caractère privé), énoncé des responsabilités de chacun dans la création, la conservation et la destruction des données. Un tel document est parfois appelé « charte d'archivage » ;

2. un référentiel de conservation, le plus souvent sous forme de tableau, qui indique pour chaque type ou catégorie de données/documents, les règles de classement et d'archivage : quelle durée de conservation (motivée), quel support d'archivage, quels droits d'accès ;

3. des procédures : comment opérer concrètement, qui fait quoi, quand et où ?

L'outil référentiel de conservation consiste à structurer les données et les documents et à les qualifier de manière à permettre leur maintenance et leur exploitation pendant toute la période requise. Le plan de classement le plus efficace est celui qui s'appuie sur les activités pérennes de l'entreprise plutôt que sur l'organigramme dans la mesure où celui-ci n'est pas stable.

Pour chaque activité ou processus, on décrit les données résultant de cette activité ou de ce processus, constituées en séries ou en dossiers, eux-mêmes constitués de documents auxquels sont attachés des pièces justificatives ou des informations temporaires.

Chaque catégorie de données est ensuite qualifiée par rapport à :

- sa durée de conservation et le motif de cette durée (référence légale, évaluation d'un risque de non disponibilité, utilité documentaire interne) ;
- son degré de confidentialité ;
- son support d'archivage.

Quelques pages suffisent généralement à décrire, de façon à la fois synthétique et efficiente, l'ensemble de l'information archivable de l'entreprise. Il est indispensable de réviser le référentiel de conservation chaque année, afin d'y intégrer les évolutions réglementaires, organisationnelles et technologiques impactant la production de l'information : nouvelles durées de conservation, nouveaux types de données, changements des outils de production des données.

Les éléments à archiver sont en général constitués de leur contenu auquel on associe des données complémentaires relatives au contexte (descriptives : origine, auteur,... ou administratives : droits, durée,...), à la structuration de l'information, voire à la présentation de la donnée. L'ensemble de ces données complémentaires constitue les métadonnées en général représentées grâce au langage XML. XML ou eXtensible Markup Language est donc un langage à balises qui permet de mettre en forme un document et de définir ses propres balises contrairement au HTML (HyperText Mark-Up Language). Afin de vérifier qu'un document XML est conforme à une syntaxe donnée on peut utiliser un document type ou Document Type Definition (DTD).

L'archivage exige par ailleurs des procédures pour que créateurs, gestionnaires et utilisateurs connaissent leurs responsabilités et les tâches concrètes qui leur incombent.

Les processus d'archivage, déclinés en procédures plus détaillées sont au nombre de trois :

1. identification et capture :
   - identifier les données et les documents à archiver par rapport à l'ensemble des données et documents produits ;
   - éviter l'archivage en multiples exemplaires en désignant un responsable de l'archivage (souvent l'émetteur pour les documents produits mais pas nécessairement) ;
   - faciliter la capture automatique des données par des règles de nommage et de classement ;
   - vérifier la qualité des données archivées (information complète, cohérente et ré-exploitable) ;
   - définir les métadonnées nécessaires et suffisantes pour gérer chaque catégorie de données : provenance (activité, auteur, destinataire, contexte), mots-clés, rattachement à un dossier, documents liés, format, application d'origine, support, indice de sécurité, droits d'accès ;

- assurer l'intégrité et donc la traçabilité, dès la validation du document, c'est-à-dire depuis le moment où il acquiert sa valeur de preuve et de témoignage.

2. Conservation et destruction :
- assurer la pérennisation des données pendant leur cycle de vie ; détecter la dégradation des formats et des supports. Le cas échéant, programmer et effectuer les migrations ;
- tracer tous les éléments qui affectent la vie de l'archive : consultation, modifications de métadonnées, re-signature, migration, etc. ;
- organiser la destruction des données périmées, pour des raisons de bonne gestion (coût et risque du stockage inutile), d'obligation légale (cas des données personnelles) et de fiabilité du fonds d'archives (toutes les informations stockées doivent être pertinentes).

3. Accès :
- permettre de savoir rapidement et avec certitude si l'information recherchée existe, est archivée et où elle se trouve ;
- fournir l'information à l'utilisateur dans les délais demandés ;
- ne donner accès qu'aux personnes habilitées mais s'assurer que les habilitations sont à jour (à voir avec l'annuaire d'entreprise et éventuellement d'autres applications).

Bien évidemment, il est préférable de disposer de l'ensemble de ces outils méthodologiques avant de choisir un logiciel d'archivage (voir fiche 9)

On peut citer un quatrième outil, réservé à l'administrateur général de l'archivage (records manager), qui est un tableau de bord des données archivées, afin de pouvoir dire à tout moment si tel type de données ou de documents existe, si tout ce qui devait être archivé l'a été, qui en est le responsable juridique, qui en est le gestionnaire, avec quel outil, où se trouvent les données, si elles ont été détruites,... Les entreprises ont de plus en plus besoin d'un tel outil qui procure une visibilité globale sur une question souvent elle-même globale.

Les principales normes ou guides pour l'archivage :
- guide de l'archivage électronique sécurisé, Association Ialta France, 2000 : recommandations pour la mise en œuvre d'un système d'archivage interne ou externe utilisant des techniques de scellement aux fins de garantir l'intégrité, la pérennité et la restitution des informations, ouvrage collectif sous la direction de Michel Lesourd, juillet 2000 ;
- norme française NF Z42-013 : recommandations 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, 2001 ;
- norme internationale ISO 19005-1 sur le format PDF/A ("A" comme "archive"), approuvée de façon unanime en juin 2005, devrait être publiée en septembre 2005 ;
- ISO 15489 associée à la méthodologie DIRKS (Design and Implementation of Recordkeeping Systems) d'implémentation en 8 étapes d'un système global d'archivage :

1. enquête préliminaire ;
2. analyse des activités ;
3. identification des exigences archivistiques ;
4. évaluation des systèmes existants ;
5. identification de la stratégie pour la satisfaction des exigences ;
6. conception d'un système d'archivage ;
7. mise en œuvre ;
8. contrôle.

- le modèle MoReq (Model Requirements for the Management of Electronic Records / Modèle d'exigences pour l'organisation de l'archivage électronique), publié par la Commission Européenne en 2001 : http://www.cornwell.co.uk/moreq.html et http://www.archive17.fr/MoReq_en_francais.pdf, en cours de révision MoReq2 ;
- modèle OAIS (système ouvert d'archivage d'informations), devenu la norme internationale ISO 14721 : description de l'organisation et du fonctionnement d'un centre d'archivage pour la pérennisation des données numériques : http://vds.cnes.fr/pin/documents/projet_norme_oais_version_francaise.pdf.

Contexte

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

Il existe quelques risques afférents à l'archivage interne (effectué au sein même de l'entreprise) en matière de preuve. L'archivage externe est ainsi préférable pour deux raisons :

- la mutualisation et donc le partage des coûts ;
- le professionnalisme de la solution, gage supplémentaire de la force probante des éléments archivés.

Toutefois, un archivage interne est parfois obligatoire par exemple pour les collectivités territoriales.

Le tiers archiveur est une personne physique ou morale qui est en charge, pour le compte du client, de la réception, de la conservation et de la restitution de documents électroniques (écrit, signature, certificat, jetons d'horodatage, données de connexion, etc.) et des données qui y sont jointes.

Dans un environnement informatique, on a fréquemment recours à un prestataire ASP (Application Service Provider), en français FAH. (Fournisseur d'Applications Hébergées). Le concept ASP prend la forme d'une mise à disposition de programmes informatiques et de services auxquels l'entreprise peut accéder à distance (internet, VPN ou réseaux privés), moyennant le versement d'une redevance. Ce modèle ASP est amené à se développer en matière d'archivage.

Le Contrat d'archivage externe (ASP) est un contrat par lequel un client passe par un tiers disposant d'une plate-forme informatique pour effectuer les prestations d'archivage auxquelles il est légalement tenu ou non. Le tiers archiveur agit pour le compte du client et en son nom (article 1984 Code civil). On est donc en présence d'un contrat de mandat. En matière d'archivage électronique, le tiers archiveur a la possibilité de changer le support ou le format physique de l'archive. C'est d'ailleurs un des intérêts de passer par un prestataire de services d'archivage externe qui utilise des moyens permettant de garantir l'intégrité du document archivé et ainsi sa force probante voire sa validité.

Enjeux

Il est nécessaire de mettre en place un contrat reprenant les fonctionnalités attendues du service d'archivage externe. Les obligations et les responsabilités du tiers archiveur devront être précisées. A titre indicatif nous citerons les obligations suivantes auxquelles est soumis le tiers archiveur :

- obligations de fiabilité : un archivage à vocation probatoire doit être fiable et sécurisé ;
- obligation d'intégrité et de préservation des données : le tiers archiveur doit ainsi garantir le maintien des données intactes et les préserver de toute altération, modification ou destruction (prise en compte du partage de responsabilité en cas de virus informatiques, par exemple) ;
- respecter les conditions tenant à la réversibilité : hypothèse du changement de prestataire ou de l'arrêt de l'activité ;
- assurer la sauvegarde des données qui lui sont confiées : sur un autre site d'archivage par exemple ;
- permettre la restitution des documents archivés : sur tout type de support, de format, etc. défini avec le client ;
- obligation d'information : le tiers archiveur informera le client à chaque modification du service d'archivage.

Il en sera ainsi notamment pour :

- L'ajout d'une nouvelle application informatique ;
- La modification substantielle d'une de ses applications ;
- Le changement de système d'exploitation ou de système de gestion des bases de données ;
- Le changement de prestataire d'exploitation informatique. Même avec l'autorisation du client, le tiers archiveur est alors tenu d'une obligation de surveillance du prestataire substitué (Bulletin des arrêts Cour de Cassation,

Chambre civile 1, n°163, audience du 29/5/1980).

D'autres obligations à la charge du tiers archiveur sont liées à l'exécution de la prestation. Le tiers archiveur doit notamment :

- disposer d'une capacité de stockage suffisante pour pouvoir assurer sans discontinuité la prise en charge des documents ;
- mettre en place un niveau de sécurité physique et logique suffisant. Les mesures de sécurité étant établies et documentées en fonction des besoins ;
- conserver l'intégralité des éléments qui lui ont été confiés ;
- ne communiquer les documents archivés qu'aux destinataires désignés dans le contrat, et cela même après que le contrat ait pris fin ;
- permettre un accès direct et sécurisé au client pour consulter les archives ;
- documenter et permettre l'audit des procédures d'archivage, de migration de support et de restitution ;
- prendre une assurance couvrant les risques liés à l'exécution du contrat ;
- détruire les éléments reçus à la demande du client et fournir à celui-ci une attestation de destruction.

L'obligation qui pèse sur le tiers archiveur est en général une obligation de moyens mais elle peut être plus lourde en fonction de la qualification prévue pour celle-ci dans le contrat. L'intérêt de connaître la nature des obligations prévues au contrat tient au régime de preuve qu'il faudra respecter en cas de litige.

Ainsi dans le cadre d'une obligation de moyens, la charge de la preuve repose sur le client qui doit démontrer l'existence d'une faute, d'un préjudice et d'un lien de causalité. Alors que dans le cadre d'une obligation de résultat, la faute est présumée par la seule non réalisation des objectifs. La charge de la preuve repose par conséquent sur le tiers archiveur qui doit démontrer l'absence de faute de sa part.

A côté de ses obligations contractuelles, le tiers archiveur est également soumis à des obligations de nature légale relatives au contenu des archives. Celles-ci dépendent des données faisant l'objet de l'archivage. Ainsi, le tiers archiveur est notamment tenu de respecter :

- les formalités préalables nécessaires à la mise en place de traitements automatisés d'informations nominatives ;
- l'obligation de confidentialité et de protection des données à caractère personnel qu'il traite.

En revanche, le tiers archiveur n'est soumis à aucune obligation générale de surveiller les informations qu'il héberge quant à leur contenu.

Le tiers archiveur est susceptible de voir sa responsabilité engagée tant sur le plan civil que sur le plan pénal. Pour engager la responsabilité civile contractuelle de l'archiveur, le client doit prouver l'existence des trois éléments suivants :

- une faute : il s'agit d'un manquement à une des obligations contractuelles ;
- un préjudice : celui-ci pourra être constitué par la perte ou encore l'altération d'un document. Les dommages dits « indirects » (les pertes d'exploitation par exemple) sont en général exclus ;
- un lien de causalité entre la faute et le préjudice sachant que le tiers archiveur n'est pas responsable du contenu des documents archivés et notamment de leur authenticité.

La responsabilité pénale du tiers archiveur pourra notamment être engagée en raison d'un manquement aux obligations relatives à la mise en place de traitements informatiques. Le tiers archiveur encourt alors de nombreuses sanctions pénales. On peut citer à titre d'exemple les infractions suivantes :

- le non respect des formalités préalables nécessaires à la mise en place de traitements automatisés d'informations est puni de 3 ans d'emprisonnement et de 45 000 € d'amende (article 226-16 du Code pénal) ;
- un manquement à l'obligation de sécurité des informations ou de détournement de la finalité du traitement est puni de 5 ans d'emprisonnement et de 300 000 € d'amende (article 226-17 et suivants du Code pénal) ;
- la divulgation intentionnelle d'informations à des tiers est punie d'un an d'emprisonnement et de 15 000 € d'amende (article 226-22 du Code pénal).

Les personnes morales peuvent être déclarées responsables pénalement de ces infractions (article 226-24 du Code pénal) dans les conditions le l'article 121-2 du Code pénal. Les peines encourues sont

les suivantes (articles 131-38 et 131-39 du Code pénal) :

- une amende d'un montant jusqu'à 5 fois supérieur à celui prévu pour les personnes physiques ;
- la dissolution, le placement sous surveillance judiciaire, la fermeture d'établissements, l'exclusion des marchés publics, l'interdiction de faire appel public à l'épargne, etc.

Recommandations

Les obligations encadrant le contrat d'archivage externe sont nombreuses et il faudra prendre un soin particulier à la rédaction des clauses. Cette rédaction aura, dans l'hypothèse de la survenance d'un litige, une influence déterminante sur les moyens probatoires (exemple : charge de la preuve, contenu de l'obligation, etc.) qui selon les cas reposeront sur le client (obligation de moyens) ou sur le tiers archiveur (obligation de résultat).

Contexte

Le coût de l'archivage électronique dans une entreprise n'est pas simple à évaluer dans la mesure où il se compose de plusieurs éléments. Les principaux postes de coûts directs sont :

- les matériels et logiciels d'archivage et plus globalement tous les équipements nécessaires au stockage (acquisition et maintenance) ;
- les ressources humaines nécessaires pour préparer l'archivage, gérer les données archivées et restituer l'information aux utilisateurs ; le constat a été fait que le coût humain est toujours plus important que le coût matériel.

Ces coûts sont à comparer aux coûts indirects du non-archivage :

- temps perdu à rechercher des informations mal archivées ;
- coût des solutions techniques mal adaptées qui provoquent des systèmes parallèles ou imposent un renouvellement prématuré des matériels ;
- les amendes, sanctions et éventuels redressements, conséquences de l'impossibilité pour l'entreprise de produire le document exigé par les autorités ou de prouver son authenticité, ou encore par suite de la conservation de données personnelles dont la destruction est réglementaire. On a vu plus d'un cas où le coût d'un seul procès aurait financé une magnifique solution d'archivage gérée par une équipe de techniciens et d'archivistes professionnels.

Tout ceci est également valable pour l'archivage papier mais avec l'archivage électronique, les coûts sont beaucoup plus élevés et les processus plus complexes. L'archivage électronique et son coût sont conditionnés par la qualité initiale des données : on ne peut archiver valablement des données mal documentées car on ne pourra pas les exploiter ; pareillement, si l'intégrité des documents n'a pas été vérifiée en amont (l'archivage ne pourra que pérenniser le défaut d'intégrité).

L'archivage apparaît donc comme un métier à part entière qui nécessite des compétences spécifiques dès que l'on atteint un seuil critique en volume de données mais surtout en hétérogénéité des données, des contraintes et des usages.

Enjeux

Deux objectifs sont prioritaires dans l'approche du coût de l'archivage électronique :

1. trouver le bon rapport coût / efficacité : des solutions techniques et des outils méthodologiques trop sophistiqués feront de l'archivage une contrainte trop lourde pour les utilisateurs qui seront tentés de contourner le système. De même, des outils sous-dimensionnés en termes de volumes, de fonctionnalités ou de points de contrôle produiront un archivage qui ne sera pas fiable et qui présentera donc des risques plus ou moins élevés pour l'entreprise ;
2. identifier et hiérarchiser les risques financiers du non archivage afin de définir les données ou services prioritaires et de programmer les dépenses en fonction de ces risques.

Recommandations

En matière de coût d'archivage électronique, il n'y a pas de recommandations absolues. Il est important que chaque entreprise analyse ses coûts par rapport à ses besoins de consultation de l'information archivée et par rapport à ses risques potentiels.

En revanche, une étude des coûts doit prendre en compte tous les aspects de la démarche d'archivage et nous ne saurions que trop recommander une simulation d'exploitation complète sur au moins trois ans afin d'être sûr de ne rien oublier.

Coût de l'investissement de base	Les coûts directs concernent d'abord les matériels informatiques et télécoms, les logiciels, et les prestations de mise en place. L'amortissement de ces coûts se fait en général sur trois ans.
Coût d'exploitation	L'exploitation regroupe des postes de coût assez variés : locaux sécurisés, personnel affecté à la gestion de l'archivage, maintenance des matériels et logiciels, télécommunications.
Autres coûts	D'autres coûts ponctuels viennent s'ajouter à l'investissement initial et au budget d'exploitation : investissement complémentaire pour augmenter la capacité de base, coût de migration (pérennisation), coût de restitution, coût de l'assurance, reprise des données, sauvegarde.
Coûts amont induits	On ne peut exclure de l'archivage les coûts d'implémentation et de fonctionnement des systèmes de production des données dans la mesure où ceux-ci conditionnent la qualité et « l'archivabilité » des données. Par exemple, la capture automatique des métadonnées allégera d'autant le travail du personnel d'archivage. De même, l'interopérabilité des différents systèmes en place réduira le coût des flux de données.
Coûts d'accompagnement d'une politique d'archivage	Enfin, le coût de l'archivage comprend aussi le coût de la gestion d'un projet autour de la définition d'une politique d'archivage au niveau de l'entreprise : • communication sur le sens et les conséquences de l'archivage ou du non archivage au niveau global de l'entreprise ; • prise en compte des exigences d'archivage par l'ensemble des métiers et fonctions de l'entreprise ; • actions de sensibilisation et de formation de l'ensemble des collaborateurs, moins pour « bien archiver » que pour « créer une bonne information ». Ces opérations constituent un véritable investissement (prévenir plutôt que guérir) dont l'entreprise récoltera les premiers fruits en un ou deux ans.
Mutualisation des coûts	Un bon archivage exige des équipements qui ne seront pas nécessairement rentabilisés, ou des compétences spécifiques qui seront sous-employées. Afin d'y remédier, on peut par exemple : • regrouper l'organisation de l'archivage électronique, l'archivage papier et la documentation pour mutualiser les compétences méthodologiques : expertise des documents, techniques de recherche documentaire, logistique de l'information ; • partager un équipement ou sous-traiter ponctuellement une tâche particulière dans l'ensemble de la démarche d'archivage, par exemple la migration de données.
Risque financier et valeur de l'information	Les coûts sont liés au volume de données archivées et à la fréquence de consultation mais aussi aux exigences de sécurité et à la finesse du traitement de l'information (indexation, métadonnées). Il est recommandé d'attribuer une valeur à l'information en fonction des risques financiers encourus par la non disponibilité des données. En fonction de cette valeur, on pourra définir des niveaux d'archivage plus ou moins élaborés donc plus ou moins onéreux. Ainsi la gestion des archives vitales (voir fiche 1) coûtera légitimement plus cher que celle de données de moindre valeur.
Mesurer l'archivage	Il n'existe pas à ce jour d'indicateurs de référence pour l'évaluation de la performance de l'archivage. Il est recommandé à chaque entreprise de mesurer son propre archivage en sélectionnant un jeu de documents ou de données représentatifs et en calculant le coût annuel d'archivage comprenant la création, l'identification, la capture, la gestion, la maintenance, l'accès et la destruction, ainsi que l'évolution de ce coût au fil des ans. On pourra ainsi évaluer et suivre par exemple le coût moyen annuel : d'une facture, d'un e-mail, d'un contrat, d'un dossier de personnel, d'une étude, etc. Attention à prendre en compte, dans le calcul des coûts, la gestion des copies.
Faire ou faire faire	Comme on l'a déjà vu, la réponse à la question de l'externalisation n'est pas absolue mais relative à une situation d'entreprise. Elle n'est pas non plus monolithique, c'est-à-dire que la meilleure solution peut s'avérer un panachage de plusieurs solutions articulées en fonction de la nature des données et des classes de services recherchés. Chaque entreprise doit bâtir et chiffrer deux ou trois scenarii en fonction des outils existants, des compétences internes, des risques, de sa politique vis-à-vis de son cœur de métier, des avantages et garanties apportés respectivement par la solution interne et la solution externe. Dans tous les cas de figure, l'important reste d'avoir une vision globale des solutions, outils et équipes d'archivage pour connaître le coût global de l'archivage pour l'entreprise.

Index

L'ensemble des mots-clés de l'archivage utilisé dans l'ouvrage est repris ici dans l'ordre alphabétique. Les références indiquées renvoient aux numéros des fiches, suivi le cas échéant de la lettre C pour la partie « Contexte », E pour « Enjeux » ou R pour « Recommandations ».

ti Forums
Les conférences
Enrichir ses connaissances - Partager ses expériences

OFFRE SPECIALE

Valable jusqu'au 31 Décembre 2005

2 Conférences et 5 Cahiers/livres blancs pour 250€HT

UN Pass 2 jours à la conférence :
« Nouvelles Technologies pour les Data Centers »
Mardi 28 Février et Mercredi 1er Mars 2006
(Palais des Congrès – Porte Maillot)
Les thèmes : ILM , Archivage Réglementaire, Consolidation, Virtualisation, Provisioning, CDP,Linux, Dématérialisation, etc.... pour offrir une amélioration de la qualité de service, une réduction des couts et des risques lors des changements et être conforme avec la réglementation. Les thèmes sont traités sous l'angle légal, système d'information, organisationnel, budgétaire comme dans toutes les conférences ITIFORUMS.
www.itiforums.com

UN Pass 2 jours à la conférence :
« Business Continuity et Telecom »
les 24 et 25 Octobre 2006
(Palais des Congrès – Porte Maillot)
Les thèmes sont traités sous l'angle légal, système d'information, organisationnel, budgétaire comme dans toutes les conférences ITIFORUMS
www.itiforums.com

LE Cahier thématique de :
la Conférence Business Continuity 2005
Le cahier est un résumé écrit de toutes les présentations de la conférence - Business Continuity 2005

LE Livre Blanc :
L'archivage électronique à l'usage du dirigeant
Le livre blanc de la Fedisa (Fédération pour l'ILM, le stockage et l'Archivage) publie un livre blanc sous forme de fiche écrit par Marie-Anne Chabin, Eric Caprioli et Jean-Marc Rietsch de la FEDisa (Fédération de l'ILM , du stockage et de l'Archivage) www.fedisa.org
Adhésion à la FEDisa

LE Cahier thématique :
ILM et Archivage Electronique 2005
Le cahier est un résumé écrit de toutes les présentations de la conférence - ILM et Archivage 2005

LE Cahier thématique de :
la Conférence Nouvelles Technologies 2006
Le cahier est un résumé écrit de toutes les présentations de la conférence - Business Continuity 2006

LE Cahier thématique de :
la Conférence Business Continuity 2006
Le cahier est un résumé écrit de toutes les présentations de la conférence - Business Continuity 2006

Pour profiter de cette offre et en savoir plus www.itiforums.com

Ou merci de retourner le coupon au dos et de le renvoyer au numéro indiqué

Pour toute question complémentaire : info@itiforums.com