LES MEMBRES DU BUREAU 2006 DE LA CHAMBRE MONÉGASQUE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Monsieur Christian HANEUSE, *Président*

Monsieur Jean-Paul GALLY, *Vice-Président*

Monsieur Jean-Charles ALLAVENA, *Secrétaire Général*

Monsieur Vincenzo GUGLIERI, *Trésorier*

CHAMBRE MONÉGASQUE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

MICROTEK
Monsieur O. MERLIN
2, boulevard Rainier III - MC 98000 MONACO

TEKWORLD
Monsieur C. HANEUSE
2, boulevard Rainier III - MC 98000 MONACO

BLUE WAWE SOFTWARE
Monsieur C. HANEUSE - Monsieur M. DAURE
15, avenue de Grande-Bretagne
MC 98000 MONACO

LA TÉLÉPHONIE PRIVÉE
Monsieur M. MANIVET
L'Aigue Marine - 24, avenue de Fontvieille
MC 98000 MONACO

SO.NE.MA.
Monsieur G. DATRIER
7, avenue d'Ostende - Les Princes
MC 98000 MONACO

DISTRICOMMUNICATION
Monsieur G. DATRIER
7, avenue d'Ostende - Les Princes
MC 98000 MONACO

SAMIC
Monsieur JOLLY - Monsieur J.P. GALLY
24, avenue de Fontvieille - MC 98000 MONACO

LOGICAL
Monsieur V. GUGLIERI
51, avenue Hector-Otto - MC 98000 MONACO

RIVIERA TELECOM
Monsieur A. GARCIA
Le Continental - place des Moulins
MC 98000 MONACO

MEDIA COMPUTERS
Monsieur E. PERODEAU
Le Soleil d'Or - 9, rue Aureglia
MC 98000 MONACO

MONTE CARLO SYSTEMS
Monsieur A. GUILLET - Monsieur M. VAREILLE
Buckingham Palace - 11, avenue Saint-Michel
MC 98000 MONACO

MONACO INFORMATIQUE SYSTEMS
Monsieur Thierry AIGLON
13 avenue des Castelans - MC 98000 MONACO

TELIS S.A.M.
Monsieur T. LERAY
14, avenue de Grande Bretagne MC 98000 MONACO

KJT COMPUTER
Monsieur A. ARNOUX
41, avenue Hector Otto
MC 98000 MONACO

GLOBAL SITE POSITION
Monsieur C. BENNIER
20, boulevard de Suisse - MC 98000 MONACO

MONACO INTERACTIVE
Monsieur T. POYET
25, boulevard de Suisse - B.P. 14
MC 98000 MONACO

SYCAMORE SERVICES
Monsieur A. VEREVIS
31, avenue Hector Otto - MC 98000 MONACO

FUTUR CYB
Monsieur Gilles RENAULT
S.C.S. MINELLONO & Cie
45, avenue de Grande Bretagne
MC 98000 MONACO

NETBAY SAM
Monsieur J.L. COUTAREL - Monsieur Franck YVORET
30 boulevard Princesse Charlotte
MC 98000 MONACO

NAMEBAY SAM
Monsieur BOUTINET
27, boulevard des Moulins - MC 98000 MONACO

JCA CONSEILS
Monsieur J.C. ALLAVENA
17, boulevard de Suisse - MC 98000 MONACO

CEDEMO SAM
Monsieur F. PAPAZIAN
2, rue du Gabian - MC 98000 MONACO

SOCIÉTÉ TEK LINE
Monsieur A. DELUERMOZ
2, boulevard Rainier III - MC 98000 MONACO

CMT MONACO / E-MEDIA CORP
Monsieur C. PISTERMAN
Le Victoria - 13, boulevard Princesse Charlotte
MC 98000 MONACO

ENAMAX STUDIO
Monsieur M. SPINETTA - Monsieur J. RICHMOND
20, boulevard Rainier III - MC 98000 MONACO

M.M.S.
Monsieur A. TOMASINI
18, rue Grimaldi - MC 98000 MONACO

MC TEL / MONACO TELEMATIQUE
Monsieur D. MAVRAKIS - Monsieur F. JULIEN
Le Patio Palace - 41, avenue Hector Otto
MC 98000 MONACO

BUSINESS PROCESS
Monsieur L. BAUMGARTNER - Monsieur J. Vazquez
Le Monte Carlo Sun - 74, boulevard d'Italie
MC 98000 MONACO

BG COMMUNICATION (MAP TELECOM)
Monsieur R. RAMY - Monsieur N. JABRE
7, rue du Gabian - Gildo Pastor Center
MC 98000 MONACO

ALBERTSEN INFORMATIQUE
Monsieur S. ALBERTSEN
14 ter, boulevard Rainier III - MC 98000 MONACO

NOVENCI MONACO
Monsieur J. BRESCIANO
2, boulevard Rainier III - MC 98000 MONACO

TERRE DE RECHERCHE
Monsieur T. DANA
Le Patio Palace - 41, avenue Hector Otto
MC 98000 MONACO

INFORCA MONACO
Monsieur J.P. CLARET
2, avenue de la Madone - MC 98000 MONACO

Palais de Monaco

Le 21 novembre 2006

Cher Christian,

C'est avec grand intérêt que j'ai pris connaissance de votre plan d'action destiné à favoriser l'accueil d'entreprises en Principauté, à développer autour de nouvelles technologies une synergie des entreprises locales ainsi qu'une dynamique de projets.

Je vous félicite de cette initiative qui contribuera, j'en suis sûr, au développement harmonieux et rapide de la Principauté dans un domaine stratégique.

Vous remerciant, ainsi que l'ensemble des entreprises associées à cette dynamique, de votre implication à cet égard, je vous assure, Cher Christian,
de mes sentiments les meilleurs.

Albert de Monaco

Monsieur Christian Haneuse
Président
Chambre Monégasque des Nouvelles Technologies
de l'information et de la Communication

Un des axes prioritaires définis par notre Souverain est de développer les pôles d'excellence.
Notre association mène des réflexions et actions concrètes destinées à promouvoir le secteur des technologies et participer à la potentielle émergence de ce pôle :
- livres blancs et petits déjeuners de vulgarisation des technologies pour les entreprises,
- opérations plus ambitieuses : festival des effets spéciaux, implantation d'entreprises de technologie, travaux sur les modes de financement des technos,"centrale de services".

Notre démarche pour 2007 continuera dans cette lignée en se concentrant sur tous les points qui intéressent surtout les entreprises et nos adhérents.
Les livres blancs 2007 étudieront depuis l'archivage de tout type de données, tous les process "dématérialisation, tiers certificateur, hébergement sécurisé" jusqu'aux offres associées, plan de reprise d'activité, infogestion, supervision à distance et sécurité.
Seront traités tous les aspects juridiques relatifs à la valeur d'un document "archivé".

En avant première sera présentée une démarche destinée à offrir à nos entreprises une plate-forme technique "ASP" opérationnelle de ces solutions.
Distribuée par un réseau de partenaires, la "centrale de services" est le nom de code de lancement de l'opération.
Son 1er composant, l'archivage de document, sera annonçé le 18 janvier.

Nous sommes donc particulièrement heureux de ce lancement du 3e livre blanc, car il inaugure une dynamique forte où la Principauté sera une ambitieuse vitrine.
Cette vitrine mèlange les technologies et les nouveaux modèles de mise en œuvre (ASP), des partenariats entreprise/État/fournisseurs et le respect de l'environnement, en commençant par nous-mêmes. Ce 3e livre blanc a été conçu sur du papier recyclable, nous inscrivant ainsi dans une démarche écologique de base.

Alors, commençons par définir succinctement notre thème majeur et découvrir l'homme de l'art de ce 3e livre blanc, le Président de la FedISA, Jean-Marc Rietsch.

L'archivage électronique consiste à conserver sur des supports informatiques adaptés et spécifiques des données provenant de la scannérisation de documents papier ou d'origine numériques. Les supports utilisés évoluant très vite technologiquement, nous insisterons sur ce véritable paradoxe à devoir conserver des informations sur de longues périodes voire ad vitam eternam en utilisant des technologies rapidement obsolètes.

Toutes les organisations publiques et privées sont aujourd' hui concernées par l'archivage électronique. Ceci s'explique par l'addition de différents facteurs tels que l'augmentation extrêmement forte du volume de données informatiques gérées au quotidien, par l'évolution des technologies et des processus d'entreprise ainsi que par les nouvelles obligations légales et réglementaires.

Au-delà des aspects techniques qui lui sont propres, l'archivage électronique nécessite également la prise en compte d'autres domaines de compétence tels que les aspects juridiques, organisationnels et normatifs. Le présent livre blanc met en lumière l'ensemble de ces aspects et trouve ainsi tout son intérêt à avertir, sensibiliser et informer les utilisateurs potentiellement concernés.
Aussi ne faut-il pas se limiter à considérer la problématique de l'archivage électronique comme une simple dématérialisation des techniques traditionnelles d'archivage.
Outre l'influence des nouvelles obligations, ce nouveau type d'archivage doit être considéré très en amont dans la chaîne de l'information, et c'est en fait l'ensemble du cycle de vie des données qu'il faut prendre en considération. Il est ainsi indispensable de repenser tous les processus d'entreprise en matière de gestion et de suivi des données.

De fait par rapport à cette évolution des besoins, des contraintes associées et des techniques, est née FedISA, Fédération de l'ILM, du Stockage et de l'Archivage. Cette Fédération a ainsi pour principal objectif de pouvoir répondre aux véritables préoccupations des utilisateurs en matière de gestion et de conservation de l'information électronique.

Dès sa création en 2005, FedISA s'est ainsi fixée pour principales missions de :

- sensibiliser les responsables concernés aux nouvelles technologies et aux obligations afférentes (obligation de conservation, 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 tels que "records manager" ou encore "compliance officer",
- définir "des certifications et des référencements", nouveaux processus, nouvelles technologies,
- entretenir des liens avec les organismes œuvrant dans les environnements de la sécurisation et de la valorisation de l'information en générale.

Par rapport à ce qui précède et compte tenu de la finalité de la Chambre Monégasque des NTIC de promouvoir les nouvelles technologies, la complémentarité entre ces deux organisations devenait évidente pour la réalisation du présent document.
N'oublions pas également que l'archivage consiste également à conserver au-delà du patrimoine informationnel des différentes organisations existantes, notre patrimoine historique à transmettre aux générations futures.
Gageons que cet ouvrage sera ainsi la première pierre d'une nouvelle construction immatérielle au sein de la Principauté.

Christian HANEUSE
Président de la Chambre Monégasque des NTIC

Jean-Marc RIETSCH
Président de FedISA

Jean-Marc Rietsch

À la fois instigateur, coordinateur et coauteur de l'ouvrage, Jean-Marc Rietsch est expert en archivage électronique, plus particulièrement pour les aspects conformité, économie et risque. Ingénieur Civil des Mines et titulaire d'un DEA de gestion industrielle, Jean-Marc Rietsch a débuté sa carrière professionnelle par le développement logiciel et l'offre de services pour les PME-PMI. En 1993, il s'oriente vers la sécurité et plus particulièrement la sauvegarde des données numériques et dépose un brevet sur la télé sauvegarde. En 2001, Jean-Marc Rietsch participe au lancement du premier tiers archiveur en France .Il est l'auteur de nombreux articles dans le domaine de l'archivage électronique et d'un premier livre blanc "L'archivage électronique à l'usage du dirigeant". Il participe également à de fréquentes conférences, séminaires ou groupes de travail sur le sujet. Jean-Marc Rietsch est Président de FedISA (Fédération européenne de l'ILM du Stockage et l'Archivage) (www.fedisa.eu), créée en 2005 afin de pouvoir répondre aux attentes des utilisateurs dans le domaine.

Marie-Anne Chabin

Expert dans le domaine des archives et de l'archivage, Marie-Anne Chabin a fondé et dirige depuis 2000 le cabinet d'expertise Archive 17, (www.archive17.fr), spécialisé dans les stratégies globales d'archivage, le records management et la formation aux méthodes d'archivage. Diplômée de l'École nationale des chartes, elle a été successivement directeur des Archives départementales de l'Essonne, consultant en gestion électronique de documents et responsable de la vidéothèque d'actualités de l'Institut national de l'audiovisuel (INA). Elle est l'auteur de "Je pense donc j'archive", "L'archive dans la société de l'information" (L'Harmattan, 1999) et de "Le management de l'archive, traité des sciences de l'information" (Hermès, 2000) ainsi que de nombreux articles. Elle a coordonné en 2004 le numéro spécial de Document numérique intitulé "Archivage et pérennisation". Marie-Anne Chabin est membre de FedISA.

Éric Caprioli

Expert juridique dans le domaine des technologies de l'information et de la communication et de la sécurité des système d'information. Spécialiste des questions juridiques liées aux nouvelles technologies et plus particulièrement au cycle de vie des documents électroniques tant dans l'entreprise que dans la sphère publique : preuve, validité, horodatage, confidentialité, archivage, gestion des accès. Il est membre de la délégation française aux Nations Unies depuis 1993 (CNUDCI) pour les travaux touchant au commerce électronique.

Auteur de nombreux articles, conférences et ouvrages juridiques dans la matière. Docteur en droit, Avocat à la Cour de Paris, Spécialiste en droit de la propriété intellectuelle, il est le fondateur du cabinet d'avocats "Caprioli & Associés", basé à Paris et Nice (www.caprioli-avocats.com). Éric Caprioli est en outre membre du Conseil d'administration de Fedisa et de la Fédération Nationale des Tiers de Confiance (FNTC).

Les trois auteurs viennent également de publier chez Dunod en novembre 2006 dans la collection management des systèmes d'information : "Dématérialisation et archivage électronique. Mise en œuvre de l'ILM (Information Lifecycle Management)", préfacé par Didier Lambert, Président du CIGREF.

Autrefois simple concept, la dématérialisation touche aujourd'hui pratiquement tous les domaines de l'entreprise. Ainsi 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'archivage électronique. Ce sont en effet des volumes colossaux d'information numérique qu'il va falloir maintenant conserver en toute sécurité pendant plusieurs dizaines d'années, voire davantage sachant 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 à priori comme une contrainte en quelque chose de constructif permettant entre autres 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.

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.

À 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.

À 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 détails la façon de les traiter efficacement.

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. À 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.

PHASE	N° FICHE	THÈME
LE CADRE	1	Besoins d'archivage
	2	Contraintes légales
	3	Contraintes spécifiques
	4	Contraintes techniques
	5	Risques et assurances
	6	Stratégie
LES OUTILS	7	Les technologies actuelles
	8	Les logiciels
	9	Les outils méthodologiques
	10	Le tiers archiveur
	11	Les coûts

LES BESOINS D'ARCHIVAGE

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'État, 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.
À 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.

LES CONTRAINTES LÉGALES

CONTEXTE

Les contraintes juridiques à respecter dans le cadre du recours à un système d'archivage électronique ont essentiellement pour objectif de permettre de se prévaloir en justice ou lors d'un contrôle de l'administration d'un document archivé. Cette vocation probatoire se retrouve dans le droit privé monégasque mais aussi dans les textes internationaux et particulièrement dans les directives européennes.

Il convient de rappeler en cet endroit que les délais de prescription applicables en matière probatoire peuvent être interrompus (ex : une procédure), contrairement aux obligations de conservation imposées par les administrations fiscales ou de sécurité sociale dont les délais sont pré-fixés. Cette distinction revêt une importance considérable pour les délais qu'il faudra respecter dans l'archivage électronique.

La mise en place d'un système d'archivage doit s'appuyer avant tout sur les objets informatiques à archiver. Il s'agira le plus souvent d'actes juridiques. C'est pourquoi, il est important de préciser la distinction entre acte juridique et fait juridique.

EN DROIT PRIVÉ

L'acte juridique se définit comme une opération juridique consistant en une manifestation de volonté ayant pour objet et pour effet de produire une conséquence juridique (ex. : contrat de bail, contrat de voyage sur internet, 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.

La qualification d'acte ou de fait juridique aura une incidence sur le système de preuve applicable. L'étendue du champ d'application du système d'archivage se limite, le plus souvent, aux actes juridiques. Mais des faits juridiques peuvent aussi faire l'objet d'un archivage, par exemple dans le cadre de la traçabilité des échanges et de la cybersurveillance mise en place par l'entreprise (log de connexion, jeton d'horodatage, signature électronique, authentification, …). Notre propos portera donc essentiellement sur la preuve des actes juridiques.

La preuve des actes juridiques

Les règles probatoires diffèrent selon le domaine du droit en cause.
En droit commercial, l'article 74 du Code de commerce de la Principauté pose le principe de liberté de la preuve. Liberté de la preuve ne signifie pas absence de preuve. En réalité, cela signifie que tous les moyens de preuve seront recevables par le juge (présomptions, témoignages, aveux, serments, commencement de preuve écrite, …). On peut donc prouver par tous moyens.

Rappelons qu'à l'heure actuelle (décembre 2006), aucune disposition n'est intervenue pour consacrer la valeur juridique et l'admission de l'écrit et de la signature électroniques au titre de la preuve et de la validité des actes juridiques en droit civil monégasque.

Ces questions juridiques ont été prises en compte dans l'Union européenne. En France, la loi du 13 mars 2000, la loi pour la confiance dans l'économie numérique du 21 juin 2004 et l'ordonnance du 16 juin 2005 ont réglé ces aspects fondamentaux pour la sécurité juridiques des échanges électroniques en intégrant dans le code civil les règles relevant du formalisme juridique exigé ad probationem et ad validitatem pour les contrats conclus par voie électronique, ainsi que les lettres et les envois recommandés électroniques.

Pourtant, un projet de loi avait été déposé à l'aube du XXI^{e} siècle au Parlement, il est resté lettre morte. Et c'est sans doute mieux comme cela, car de nombreuses évolutions ont permis de vérifier qu'il "était urgent d'attendre". En 2007, pour la sécurité juridique des transactions, le marché a besoin que les autorités de la Principauté adoptent un texte sur ces sujets cruciaux pour l'avenir du pays.

Les actes juridiques dont l'objet est supérieur à 1 140 euros (article 1 188 du Code civil) ne peuvent être prouvés que par certains moyens de preuve, seuls admissibles, tels que l'écrit, l'aveu (articles 1 201 et suivants du

Code civil) ou le serment (articles 1 204 et suivants du Code civil), voire par une accumulation d'éléments probants (on parle de "commencements de preuve par écrit" tels que des copies, contenus non signés, …).

Nous nous intéresserons exclusivement à la hiérarchie des écrits entendus comme preuves et clairement spécifiée dans un chapitre VI intitulé "De la preuve des obligations et de celle du paiement". Au sommet de l'édifice, se situe l'acte authentique prévu à l'article 1164 du Code civil, à savoir "celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises". [Définition de mai 1999]. Puis suivent par valeur probatoire décroissante les actes sous seing privé, actes établis par les parties elles-mêmes sous leur seule signature sans l'intervention d'un officier public (articles 1 169 et suivants du Code civil), les tailles (article 1 180 du Code civil), les copies de titres (articles 1 181 et suivants du Code civil) et les actes récognitifs et confirmatifs (articles 1 184 et suivants du Code civil). Or, l'archivage électronique s'intéresse exclusivement à deux types de preuves, toutes deux écrites : l'une parfaite, l'écrit original et l'autre imparfaite, la copie numérique.

L'admission de l'écrit sous forme électronique pose problème

Les articles 1 169 et 1 170 du Code civil mettent en avant l'importance de la signature pour qualifier un écrit d'acte sous seing privé. Ainsi, l'article 1 170 du Code civil énonce "celui auquel on oppose un acte sous seing privé est obligé d'avouer ou de désavouer formellement son écriture ou sa signature". On peut déduire de cette disposition deux fonctions de l'écrit :

• l'identification de l'auteur de l'acte (qui reconnaît ou ne reconnaît pas sa signature),
• l'intégrité du contenu de l'acte (l'auteur peut désavouer son écriture).

Mais de ce constat, il ne découle aucune reconnaissance de l'acte sous seing privé passé sous forme électronique.

Ces deux fonctions sont les fonctions cardinales de l'écrit sous forme électronique. On peut penser que, par analogie avec le droit français, qu'il faut que le code civil prévoit que l'écrit sous forme électronique sera admis en tant que preuve dès lors qu'il existe une certitude que l'écrit émane bien de celui auquel il pourrait être opposé et que ni son origine, ni son contenu n'ont été modifiés ou falsifiés dans le temps, c'est à dire depuis le moment de son établissement. L'écrit sous forme électronique devrait également s'appuyer sur une signature électronique qui, sous réserve du respect des exigences de fiabilité requises, peut permettre d'identifier l'auteur de l'acte, de manifester son consentement au contenu et de garantir l'intégrité du contenu. La fiabilité de l'écrit et de la signature électroniques peut dépendre uniquement des procédures mises en place par un prestataire technique : le Prestataire de Service de Certification Électronique (P.S.C.E.).

La fiabilité et les éléments de sécurité (signature électronique et certificat électronique d'identité) nécessaires pendant la phase de conclusion de l'écrit sous forme électronique doivent perdurer pendant toute la période d'archivage. L'accès aux documents devra être sécurisé et leur restitution intègre assurée.

La copie électronique

Le droit civil monégasque intègre de nombreuses dispositions relatives à la copie de titre.
Par principe et selon l'article 1188 du Code, tout acte excédant la somme de 1 140 euros doit être passé devant notaire (acte authentique) ou sous seing privé. Seul un tel écrit sera considéré comme recevable à titre de preuve dans ce cas. Par exception, l'article 1 194 mentionne "Les règles ci-dessus reçoivent exception lorsqu'il existe un commencement de preuve par écrit. On appelle ainsi tout acte par écrit qui est émané de celui contre lequel la demande est formée ou de celui qu'il représente, et qui rend vraisemblable le fait allégué".

On en déduit donc qu'à titre de preuve, une copie constitue un commencement de preuve par écrit. L'article 1 181 du Code précise que "les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée". Le principe, pour attester de la valeur juridique d'un acte, est donc de disposer du titre original, un écrit papier, signé de façon manuscrite.

Toutefois, plus cette copie rendra vraisemblable le fait allégué, plus il y aura de chance d'emporter la conviction du juge quant à la force probante de celle-ci.

De plus, l'article 1 195 du Code civil, dans sa rédaction issue de la loi du 6 novembre 2001, pose une exception permettant la preuve autre que par un écrit original.

Cette exception s'applique lorsqu' "(…) une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction, non seulement fidèle, mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support. La preuve de la destruction de l'original est présumée en cas d'archivage". Cette disposition est fondamentale et elle peut légitimer l'utilisation d'un procédé de numérisation dûment documenté (il faut pouvoir tracer la vie d'un document de son origine à sa destruction "physique"). La traçabilité constitue, en effet, un élément important de la fiabilité du dispositif de numérisation et de destruction mis en place et par là même de la force probante des copies archivées. Le juge sera sans doute moins enclin à demander la production de l'original lorsqu'un procédé d'archivage fiable apporte des garanties.

Il est vivement recommandé de s'appuyer sur une politique d'archivage qui fixe d'une part, les principes généraux et les objectifs et d'autre part, les règles et les exigences de sécurité à respecter. Ce document contient une dimension juridique forte, qu'il ne faut pas négliger. De plus, des procédures doivent préciser comment la politique est mise en œuvre en fonction des applications visées. Ainsi, des documents juridiques et techniques établissent le cadre et les obligations et responsabilités en fonction du rôle de chacune des composantes du système d'archivage électronique.

Une intervention du législateur précisant que la destruction des documents papier de façon volontaire est autorisée, sous réserve qu'un système d'archivage électronique soit mis en place et qu'une procédure de destruction soit adoptée et contrôlée. L'objectif est que le système d'archivage puisse garantir la fidélité et la durabilité du document dans le temps, et son accès intègre jusqu'à la fin des durées de conservation (au sens juridique s'entend).

La preuve des faits juridiques

Pour les faits juridiques (par exemple, la preuve d'une date ou d'un évènement), la preuve est libre. Néanmoins, pour emporter la conviction du juge, il faut établir la fiabilité du procédé utilisé pour archiver les moyens de preuve des faits juridiques. Dans un souci de sécurité juridique, il est recommandé de s'appuyer sur les modalités d'archivage s'appliquant aux actes juridiques.

Les conventions de preuve

Enfin, il est possible de prévoir des conventions de preuve entre les parties, mais qui n'auront pas d'effets juridiques à l'égard des tiers. Ce procédé est souvent utilisé en matière bancaire (ex : les cartes de crédit et de débit). Avec ces conventions sur la preuve, chaque partie reconnaît la valeur et la force probante des éléments informatiques ou des copies issues des originaux numérisés et archivés par la banque. La rédaction de cette convention doit être précise et rigoureuse, afin d'être reconnue comme étant valable en cas de litige.

En tout état de cause, le juge pourra toujours demander l'original aux risques et périls de celui qui doit produire la pièce. L'entité doit donc mesurer le risque économique encouru dans ce cas, et la probabilité qu'un juge puisse être conduit à demander la production d'un original papier. Ainsi, les procédés de numérisation, de destruction et d'archivage mis en place devront être documentés et suffisamment fiables pour emporter la conviction du juge.

EN DROIT INTERNATIONAL ET D'AUTRES ÉTATS

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 électroniques et l'archivage de l'information était 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".

De nombreux pays ont suivi et repris les dispositions contenues dans la loi-type.

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. La conservation est implicite, mais l'article 10 de la loi-type prévoit les conditions de la conservation : "1. Lorsqu'une règle de droit exige que certains documents, enregistrements ou informations soient conservés, cette exigence est satisfaite si ce sont des messages de données qui sont conservés, sous réserve des conditions suivantes :
a) L'information que contient le message de données doit être accessible pour être consultée ultérieurement,
b) Le message de données doit être conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues,
c) Les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, doivent être conservées si elles existent.
2. L'obligation de conserver des documents, enregistrements ou informations conformément au paragraphe 1 ci-dessus ne s'étend pas aux informations qui n'ont d'autre objet que de permettre l'envoi ou la réception du message de données.
3. L'exigence visée au paragraphe 1 ci-dessus peut être satisfaite par recours aux services d'une autre personne, sous réserve que soient remplies les conditions fixées aux alinéas a, b et c de ce paragraphe".

De plus, l'Assemblée générale de la CNUDCI a adopté une Convention sur l'utilisation des communications électroniques dans les contrats internationaux le 23 novembre 2005. Ce nouveau texte a pour objectif de renforcer la sécurité juridique et la prévisibilité commerciale lorsque les communications en matière de contrats internationaux se font par le biais de messages de données. La Convention est ouverte à la signature depuis le 16 janvier 2006 jusqu'au 16 janvier 2008. En septembre 2006, plusieurs pays avaient signé la Convention : République centrafricaine, Liban, Madagascar, Sénégal, la Chine, Sierra Leone, Singapour et Sri Lanka.

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.

En outre, il ne faut pas négliger l'importance juridique de l'archivage dans le cadre des directives du 13 décembre 1999 sur les signatures électronique et du 8 juin 2000 sur le commerce électronique relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

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.

ENJEUX

L'archivage concerne de nombreux types de documents électroniques. Il peut s'agir de contrats bien évidemment, mais aussi de courriers électroniques ou d'autres documents plus spécifiques comme la facture.

Ainsi, le droit monégasque est venu préciser les contours juridiques de la facture dématérialisée. Le régime juridique fait référence directement aux directives communautaires applicables en la matière. L'ordonnance souveraine du 13 septembre 2004 relative à la taxe sur la valeur ajoutée est venue préciser le régime juridique de la facture électronique.

Toutefois, il ne faut pas oublier que la facture est également un document de la vie des affaires et qu'à ce titre, son régime juridique est protéiforme : il comprend, outre le droit fiscal les droits commercial, civil, douanier, financier. Les délais et les modalités de conservation sont susceptibles de varier et le respect des exigences juridique applicables à la TVA peut s'avérer insuffisant : par exemple, une conservation minimale de 10 ans sera souvent à retenir.

L'ordonnance prévoit la transmission de la facture selon deux normes sécurisées : la signature électronique et l'échange de données informatisées. Il convient d'aborder ces deux modalités de transmission des factures :

LE CADRE JURIDIQUE DE LA FACTURE ÉLECTRONIQUE SIGNÉE

Conformément à l'article 71 IV du Code des taxes de la Principauté, les factures électroniques signées doivent "sous réserve de l'acceptation des destinataires, être transmises par voie électronique dès lors que l'authenticité de leur origine et l'intégralité de leur contenu sont garanties au moyen d'une signature électronique".
Cet article précise que la facture électronique sécurisée au moyen d'une signature électronique tient lieu de facture d'origine pour l'application des articles 66 et 71 du Code des taxes.

La signature électronique se définit comme "une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthodes d'authentification du signataire et de l'origine des informations" conformément à l'article A-153 ter du Code des taxes. Le signataire peut être une personne morale ou une personne physique. Dans le premier cas, la signature électronique va être produite automatiquement lors de l'établissement des factures ce qui implique la mise en place d'un serveur capable de signer automatiquement les factures avec un certificat (de serveur). Dans le second cas, la personne physique va émettre la facture après l'avoir signée en son nom et pour le compte de l'entreprise. Les factures reçues par les destinataires pourront ainsi être vérifiées à l'aide du certificat électronique correspondant à la signature.

La signature électronique doit être propre au signataire et doit permettre une identification de celui-ci. Elle doit être créée par des moyens que le signataire puisse garder sous son contrôle exclusif. Enfin, la signature électronique doit garantir le lien avec les factures auxquelles elle s'attache et ainsi de permettre de détecter toute modification ultérieure de ces factures. À cet effet, la signature électronique devra reposer sur des technologies de cryptographie asymétrique.

Le nouveau texte consacre l'auto facturation (Article 71 I du Code des taxes) ainsi que le recours à un tiers mandaté (plate-forme de facturation) pour effectuer l'émission et éventuellement l'archivage des factures électroniques (Article 71 I du Code des taxes).

En tout état de cause, le système de facturation électronique devra garantir l'authenticité de l'origine des factures ainsi que l'intégralité de leur contenu. L'acceptation préalable de ce système par le destinataire est requise et doit faire l'objet d'un contrat (Article 71 IV du Code des taxes). Juridiquement, au minimum, il est nécessaire de prévoir la signature d'un contrat préalable, mais si l'entreprise a recours à une plate-forme de facturation, ou si elle pratique l'auto facturation, elle devra également prévoir des mandats de facturation, voire si elle utilise les services d'un tiers archiveur un (ou plusieurs) mandat(s) d'archivage.

La Direction des Services Fiscaux doit être préalablement informée de l'utilisation d'un tel système (Article 71 bis

II al. 2 du Code des taxes).

Les factures électroniques doivent ensuite être conservées dans leur format original pendant une durée au moins égale au délai prévu à l'article 118 du Code des taxes. Le Code des taxes prévoit que les factures, la signature électronique à laquelle elles sont liées et le certificat électronique attaché aux données de vérification de la signature électronique doivent être conservés dans leur contenu originel pour constituer une facture d'origine.

Enfin, l'accès aux factures par l'administration fiscale à des fins de contrôle doit toujours être assurée. Ainsi, l'administration doit pouvoir accéder en ligne aux factures et aux données jointes dans les meilleurs délais et quels que soient leur lieu de stockage pour effectuer son contrôle.

En cas d'impossibilité pour l'entreprise de dématérialiser elle-même ses factures, celle-ci peut faire appel à un prestataire de service de facturation électronique qui émettra, signera et recevra les factures en son nom. La négociation du contrat de prestations de services avec ce prestataire revêt une grande importance.

LE CADRE JURIDIQUE DE LA FACTURE TRANSMISE PAR VOIE TÉLÉMATIQUE (EDI)

L'article 71 du Code des taxes prévoit qu'une facture peut être transmise par voie électronique dès lors que l'authenticité de son origine et l'intégralité de son contenu sont garanties au moyen d'une signature électronique. En cas d'acceptation par le destinataire de la transmission par cette voie, la facture tient lieu de facture d'origine. Ici, l'acceptation se manifestera par la signature d'une convention d'interchange (EDI) contenant notamment une convention de preuve qui se fonde sur l'article 2 de la recommandation 1994/820/CE du 19 octobre 1994 de la Commission concernant les aspects juridiques de l'échange de données informatisées.

Selon l'article 71 bis I du Code des taxes, constituent des documents tenant lieu de factures d'origine, "les factures se présentant sous la forme d'un message structuré selon une norme convenue entre les parties, permettant une lecture par ordinateur et pouvant être traité automatiquement et de manière univoque constituent des factures d'origine". Par conséquent, les entreprises qui veulent transmettre les factures par Échange de Données Informatisées (EDI) doivent recourir à un système de télétransmission répondant à certaines normes techniques et à certaines caractéristiques :

• Tout d'abord "les informations émises et reçues doivent être identiques". Les mentions obligatoires contenues dans le message doivent figurer dans des zones du message facture que le logiciel doit rendre obligatoires. Une vérification de la conformité de la structure du message aux mentions obligatoires doit être effectuée à l'émission et à la réception du message. Aucune altération ne doit être constatée après la constitution, l'archivage et l'émission par le fournisseur.

• Ensuite, la tenue d'une "liste récapitulative et fichier des partenaires". Il s'agit d'une liste récapitulative de tous les messages émis et reçus qui doit être établie au fur et à mesure, quel que soit le support, et comporter un certain nombre de mentions obligatoires ainsi que les anomalies éventuelles intervenues lors de chaque transmission. L'entreprise qui émet ou reçoit des factures transmises par EDI, quelle que soit la personne qui a matériellement émis ou reçu les messages, en son nom et pour son compte, doit s'assurer qu'une telle liste est tenue et conservée sur support papier ou électronique dans les délais prescrits par les textes. Lorsque la liste est conservée sur support électronique, le fichier doit être constitué et alimenté au fur et à mesure de l'émission ou de la réception des messages et ne doit pas être modifiable. Lorsqu'elle est conservée sur support papier, elle doit être éditée séquentiellement dans l'ordre d'arrivée ou d'émission des messages et au minimum une fois par jour.

En cas d'impossibilité pour l'entreprise de dématérialiser elle-même ses factures, celle-ci peut faire appel à un prestataire de service qui émettra et recevra les factures en son nom et qui établira une liste récapitulative pour chaque entreprise.

Les informations émises ou reçues doivent être conservées dans leur contenu originel et durant les délais prescrits par les textes. L'obligation de conservation porte sur l'intégralité du message reçu, y compris sur les mentions non obligatoires. S'il s'agit d'un prestataire agissant au nom et pour le compte de plusieurs entreprises, il doit assurer une conservation des factures dématérialisées bien distincte pour chaque société.

Sur demande, l'intégralité des informations, facultatives ou obligatoires, des messages factures doit être restituée en langage clair à la Direction des Services Fiscaux en vue d'un contrôle par la personne chargée de s'assurer

qu'une facture est délivrée (même si ce n'est pas elle qui l'a matériellement émise) et par la personne destinataire (quelle que soit la personne qui les a reçues en son nom et pour son compte). Sur demande de la Direction des Services Fiscaux, la restitution peut être effectuée sous support papier. Le défaut de conservation total ou partiel constaté par les agents de l'administration pourra être sanctionné par la remise en cause de la déduction de la TVA.

Les agents de la Direction des Services Fiscaux peuvent procéder à des contrôles inopinés de la conformité du fonctionnement du système de télétransmission (Article 71 bis IV du Code des taxes). Si le système n'est pas conforme ou s'il y a eu une opposition au contrôle, une régularisation devra être effectuée dans les trente jours suivant la date de réception du procès-verbal. À défaut, l'administration interdira la transmission des factures par ce système, les factures ne seront plus considérées comme des factures d'origine et la TVA sur ces factures ne sera pas déductible.

Que l'on soit dans l'un ou l'autre des systèmes consacrés par l'Ordonnance souveraine de 2004 (ou dans une situation où les deux procédés sont combinés), au préalable, il est recommandé de procéder à un audit de conformité légale et réglementaire du projet de système de facturation et d'archivage électronique. Des actions juridiques peuvent en découler.

RECOMMANDATIONS

La phase d'archivage constitue un élément essentiel dans toute stratégie d'entreprise d'où le respect d'un minimum de précautions d'ordre juridique, souvent imbriquées aux dimensions organisationnelle et technique. Les règles de droit énoncent les fonctionnalités à prendre en compte.

Distinction entre durée de conservation et délai 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 (actions judiciaires en cours ou qui ont interrompu le délai). Ce qui compte, c'est l'extinction des effets juridiques liés à l'acte.

Analyse juridique préalable par type de document

À ce titre, il convient d'effectuer une analyse juridique 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 ou d'un contrôle de l'administration.

Audit de conformité légale et réglementaire

- En matière d'archivage électronique (originaux et copies),
- En matière de procédure dématérialisée (ex : la facture électronique, y compris son archivage spécifique).

LES CONTRAINTES SPÉCIFIQUES

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 États-Unis suivis par d'autres États, 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 États-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. À 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 Établissements de Crédit et des Entreprises d'Investissements).

Les prescriptions relatives à l'archivage des données se trouvent dans la 2e 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 FRANÇAIS

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

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.

LES CONTRAINTES TECHNIQUES

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 elles 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-après 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.

Évolutivité

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.

LES RISQUES ET ASSURANCES

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 plans :
- 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.

LA STRATÉGIE

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 :

Élaboration 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).

LES TECHNOLOGIES ACTUELLES

CONTEXTE

Dans un environnement où les technologies ne cessent d'évoluer, il semble tout à fait paradoxal de rechercher un système destiné au long terme, rôle pourtant assigné à l'archivage. À l'inverse, cette progression des technologies laisse à penser que l'on trouvera la réponse aux besoins très variés des entreprises quant aux différents types de données à conserver, aux durées et aux volumétries.
Sur ce dernier point, nous sommes déjà familiarisés 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 m de haut. On parle même de plus en plus de téraoctets (To 1 012 octets), voire de pétaoctets (Po 1 015 octets). À titre indicatif 2 téraoctets correspondent à tous les ouvrages d'une bibliothèque universitaire et 2 pétaoctets aux fonds de toutes les bibliothèques universitaires des États-Unis !
Au niveau des technologies, il existe 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.

LES SUPPORTS MAGNÉTIQUES

D'un point de vue technique, les deux états représentant respectivement le 0 et le 1 sont obtenus 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 et les disques.

Les bandes se présentent sous plusieurs formats DAT (Digital Audio Tape), DLT (Digital Linear Tape), LTO (Linear TapeOpen), 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 quelques 400 Go. 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, plus particulièrement dédiées à l'archivage du fait de la conjonction de deux phénomènes. Le premier consiste en une réduction drastique des coûts grâce à la norme SATA (Serial Advanced Technology Attachment) utilisant une connectique simplifiée. Le second phénomène résulte de l'évolution de la notion même de WORM (Write Once Read Many) passée d'un aspect purement physique (modification irréversible du substrat) à un aspect plus logique (contrôle logiciel).
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 Data-Retention 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 au magnétique, la différence entre le 1 et le 0 se fait sur la présence ou 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. L'on distingue deux grandes familles de supports optiques, celle des CD et DVD et celle 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. Là encore, les juke-box permettant d'atteindre plusieurs To de données.

ENJEUX

Le choix d'une solution technique d'archivage comporte essentiellement deux enjeux :
1. le premier consiste à trouver la technologie la mieux adaptée à ses besoins. En effet, les entreprises ont des besoins très variés en matière de volumétrie, d'accessibilité et de durée de conservation des données archivées.
2. le second enjeux est d'ordre économique afin de bien prendre en compte les aspects liés à l'exploitation du système. En effet, pourquoi par exemple utiliser une technologie sur bandes, a priori la moins chère au gigaoctet stocké, si sur la durée cela nécessite de nombreuses opérations en matière de tests de relecture, voire de migrations qui augmenteront très fortement le coût initial.

RECOMMANDATIONS

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

Évaluation des 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.

Évaluation des systèmes existants

À 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. 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

Il s'agit d'un point difficile à évaluer au cours 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.

LES LOGICIELS

CONTEXTE

Le marché propose aujourd'hui un panel assez diversifié de solutions d'archivage qui se précise et se complète régulièrement. La typologie des produits va du coffre-fort à la solution globale qui inclue 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 à des fins de preuve (abusivement appelé archivage "légal"). 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 revient à bien 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.

Évaluation des systèmes existants

Il est important d'évaluer l'adéquation des systèmes existants aux besoins identifiés et de recenser l'ensemble des systèmes parallèles.

Solution du marché, logiciel libre ou développement spécifique ?

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 des 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 particuliers 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. Le plus souvent, l'outil devra pouvoir communiquer avec les autres composantes du système d'information ou partager des ressources telles qu'un thésaurus avec d'autres applications. L'interopérabilité avec l'extérieur peut être un besoin fort et doit être étudiée.

Facilités d'indexation

Vérifier les facilités d'indexation automatique ou par mots-clés et surtout la complémentarité ou la co-existence des deux systèmes, en fonction des besoins des utilisateurs. Garder à l'esprit le fait que l'offre technologique accroît les demandes des utilisateurs. Vérifier éventuellement que l'outil permet de hiérarchiser les résultats de recherche et de faire des interrogations 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 forcément 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.

LES OUTILS MÉTHODOLOGIQUES

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.

LE TIERS ARCHIVEUR

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. À 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.

À côté de ses obligations contractuelles, le tiers archiveur est également soumis à des obligations de nature légal, 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 du droit français 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).

LES COÛTS DE L'ARCHIVAGE

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.

Le Coffre-fort électronique Communicant

PROTECTION DES DONNÉES

ARCHIVAGE

TRAÇABILITÉ

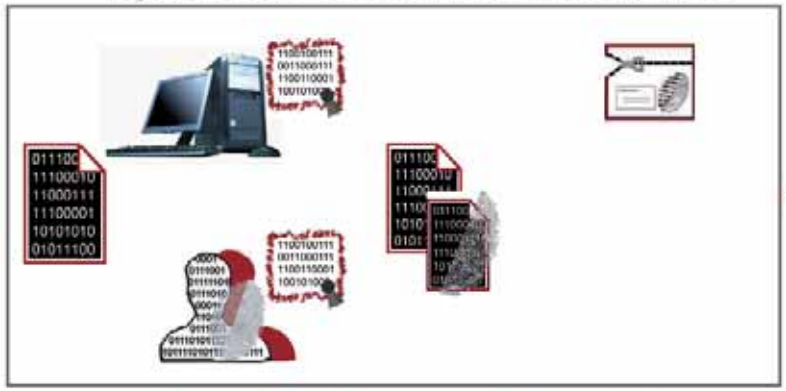
20 Juin 2006

Conservation sécurisée dans le Coffre-fort électronique Communicant

Conforme aux normes et standards

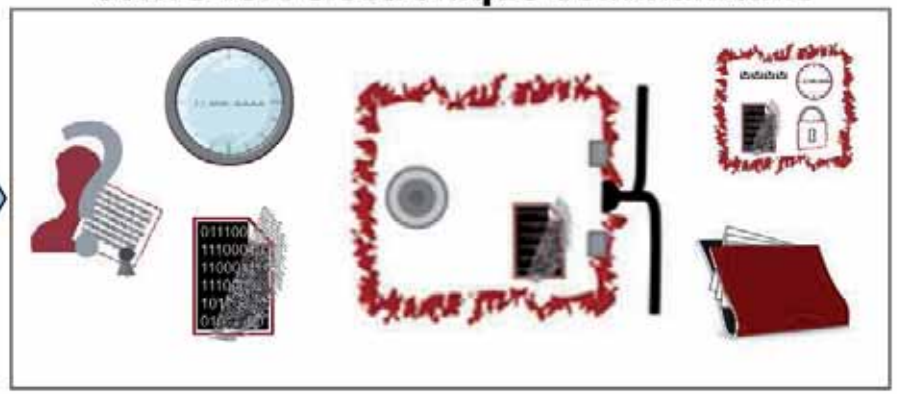
Conservation garantissant la valeur probante des pièces déposées

Système d' Information du client



SSL

Coffre-fort électronique Communicant



❶ Authentification certificat électronique
(Captation du Certificat et gestion des habilitations)

❷ Production d'une empreinte intégrité

❸ Production enveloppe et acheminement sécurisé

❹ Contrôle identité numérique

❺ Contrôle intégrité du fichier reçu

❻ Horodatage des pièces et des actions

❼ Scellement par Signature électronique

❽ Constitution de l'objet archive

❾ Notification au déposant

❿ Réception du compte-rendu XML

Notarisation - Traçabilité des opérations

Actis

<Objet archive/> XML signé et réversible

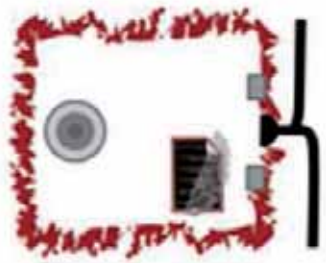
Dépôt Agence pour la Protection des Programmes n°IDDN.FR.001.060050.000.S.P.2005.000.10300

<En-tête/>	En-tête Cecurity.com
<Données de sécurité/>	Adresse CFEC Identifiant unique de l'archive
<Date/>	Date et heure de dépôt *ou* jeton d'horodatage
<Transaction/>	Identifiant session Certificat électronique du déposant
<Document/>	Nom du document **Document originel** Empreinte du document Taille du document *(option)*
<Signature/>	**Signature** Nom du document Date & heure Certificat Empreinte du document Identifiant de l'archive

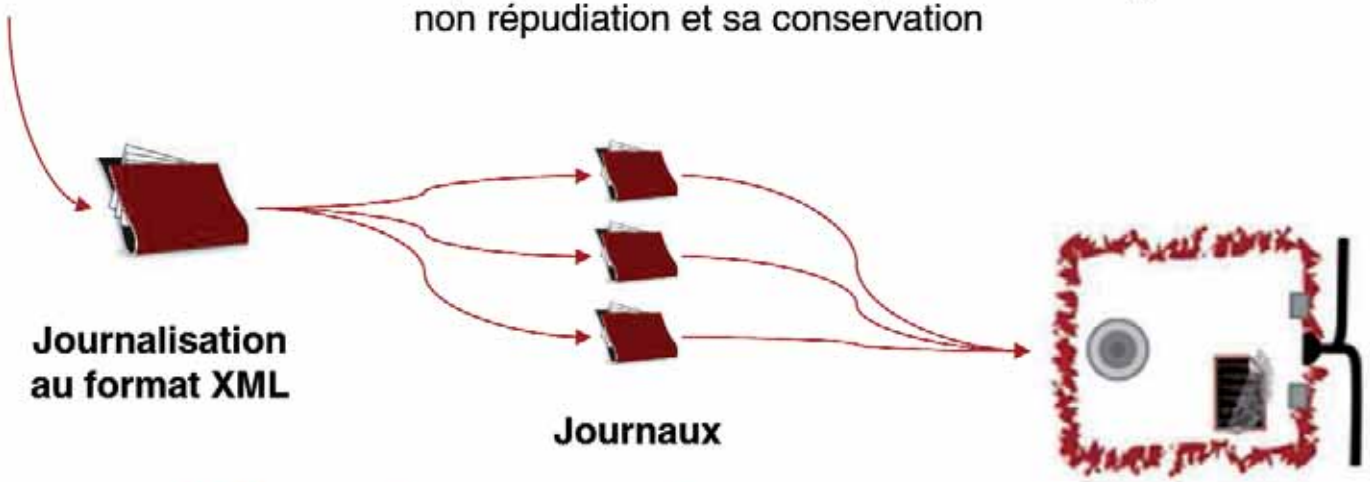
Actis

Traçabilité sécurisée des données archivées dans un Coffre-fort électronique

CFEC



- Journaux générés selon une **fréquence paramétrable** (*n* opérations, plage de temps…)
- Chaque journal généré est clôturé et **chainé** au suivant et au précédent.
- Chaque journal est **scellé électroniquement** par dépôt dans un CFE afin de garantir son intégrité et sa non répudiation et sa conservation



Journal à valeur probante inaltérable et inviolable

Archivage du journal dans un CFE (même CFEC ou autre CFEC

Actis

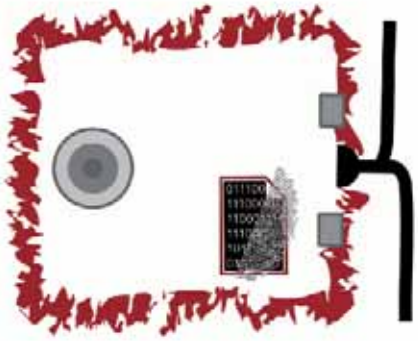
Quelques usages du Coffre-fort électronique

Coffre-fort : intégrité, traçabilité, confidentialité, valeur probante

Documents bancaires financiers

Ressources Humaines

Factures électroniques



Rapports électroniques

Actifs immatériels

Marchés Publics

Délibérés

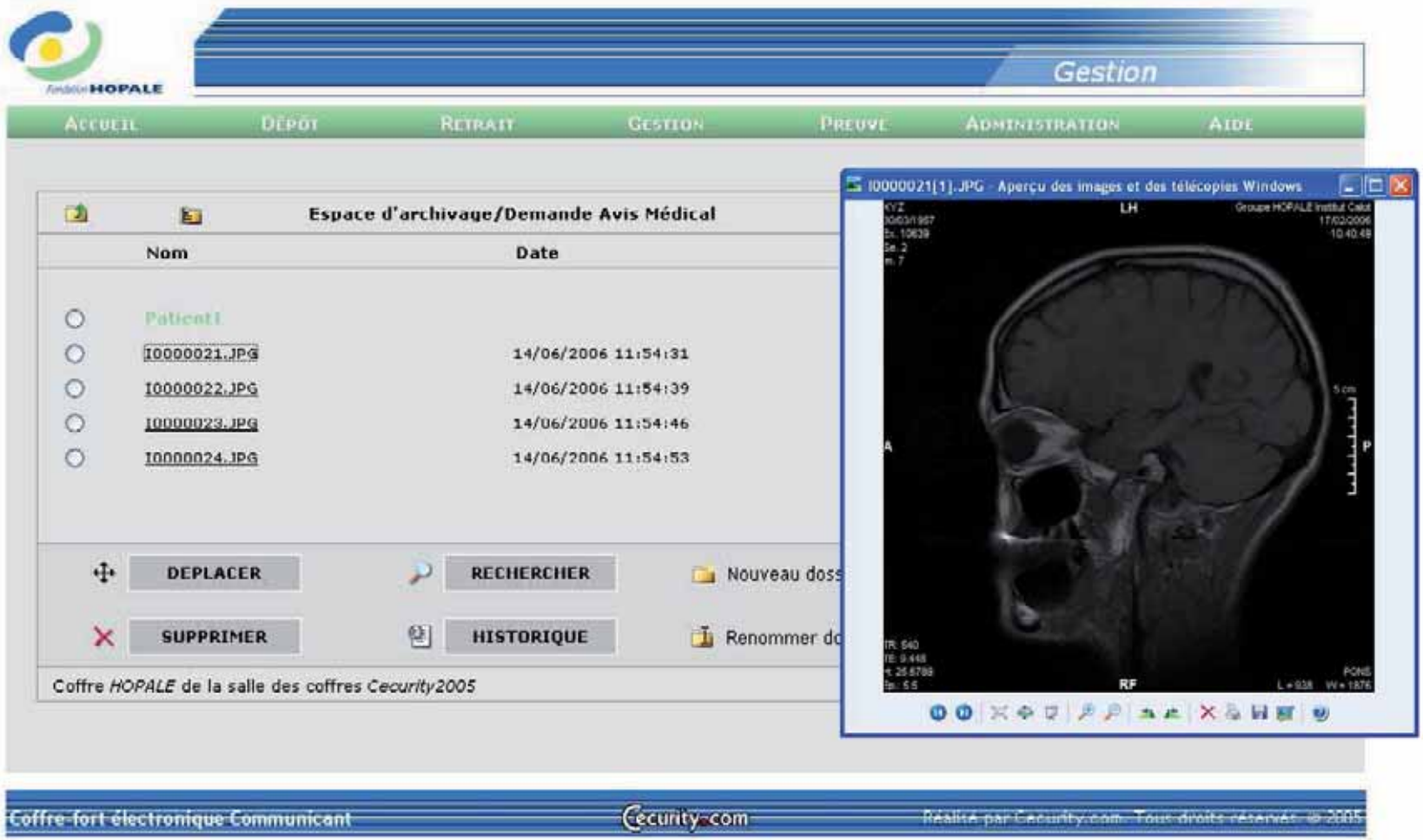
Registres sensibles

Dossier médical personnel

Contrats électroniques

Actis

Visualisation à partir du Coffre-fort d'Images pour Diagnostic et Avis en vue d'une IRM



Actis

Centre Officiel Européen
Business Continuity Recovery Services

IBM

Actis

Assurez la continuité de vos activités... en toutes circonstances

- Plan de continuité et de reprise d'activité
- Secours système informatique, salle de Marché
- Réseaux et téléphonie
- Secours utilisateurs
- Logiciel de gestion de crise
- Télé-Sauvegardes ...
- Archivage légal

Des solutions sur mesure...

Accès au centre de secours ACTIS.
Possibilité de recourir à des centres de secours IBM de second niveau en Europe : France, Belgique, Luxembourg, etc.

...Complètes

ACTIS et IBM accompagnent leurs clients à chaque étape de leur Plan de Continuité :

- Mise en place logiciel gestion de crise
- Audit et analyse des risques/vulnérabilités
- Évaluation des impacts sur les processus critiques
- Définition des besoins en continuité
- Mise en place de l'organisation de crise
- Rédaction des procédures de reprise et de continuité.

...et Évolutives

ACTIS et IBM sont au côté de leurs clients pour maintenir le Plan de Continuité et organiser des tests réguliers. Les dispositifs en place sont validés et les manuels de procédures mis à jour.

Infrastructure et équipement

- 300 m² au centre de Monaco
- Salle informatique de back-up sécurisée
- Sécurité et confidentialité des données
- Environnements multiplateformes
- Surveillance intrusion et incendie
- Multiples installations réseaux
- 30+30 positions de travail équipées et modulables : pc, téléphone
- Salle de marché de secours ETRALI
- Accès aux principaux flux d'informations financiers
- Centre d'accès au réseau bancaire international reliant les principales places financières.
- Secours courant par groupe électrogène.

ACTIS SAM (capital de 150 000 €)
Le George V - 14, avenue de Grande-Bretagne
Monte-Carlo - 98000 Monaco
Tél. +377 97 98 18 18 - Fax +377 97 98 18 19

Actis

www.actis.mc

Président : **Thierry Leray**
Administrateur Délégué : **Jean-Pierre Ballet**

... INFORCA MONACO ...

L'ENGAGEMENT ET LA PUISSANCE DU 1ER PARTENAIRE EMC EN FRANCE

EMC²
where information lives

STOCKAGE

EMC SYMMETRIX DMX-3

PROFESSIONAL

EMC CLARIION AX150

ARCHIVAG

EMC CLARIION CX3-10

LE MONTAIGNE 2 AVENUE DE LA MADONE MONTÉ CARLO 98000 MONACO - HTTP://WWW.INFORCA.FR

INFORCA Monaco

HTTP://WWW.INFORCA.FR

TEL: 00.377.93.50.64.25

GROUPE

ASCOMA

Courtage d'Assurances et de Réassurances

www.ascoma.com

ASCOMA
24 bd Princesse Charlotte
98000 Monaco
Tel +377 97 97 22 04
Fax +377 97 97 22 05
E-mail : info@ascoma.com

cybersquatting ?

phishing ?

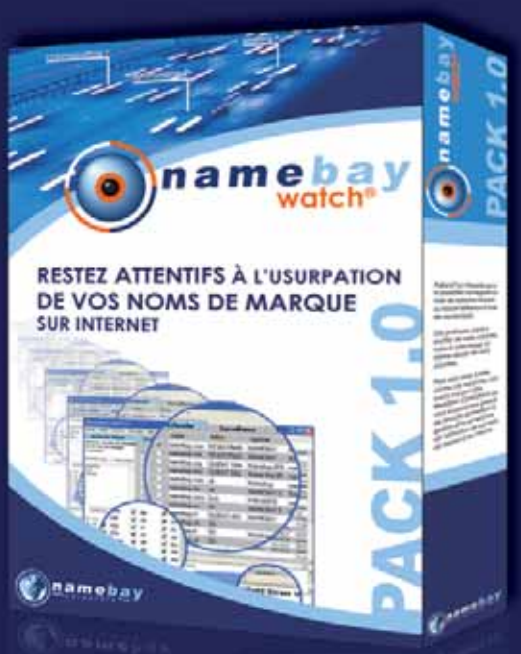
spamming ?

namebay corporate®

votre bureau d'enregistrement de noms de domaine
spécialisé dans la protection de vos noms de marque

services d'assistance personnalisés

dans le réglement des litiges
sur les noms de domaine



solution puissante et performante

de lutte contre les nuisances
sur internet

(surveillance de marques,
gestion des noms de domaine, ...)

CONTACTEZ-NOUS

NAMEBAY - Service Corporate - 27 Bd des Moulins MC98000 MONACO
email : commercial@namebaycorp.com - http://www.namebaycorp.com

LE CFM AU SERVICE DES ENTREPRISES

UN ANCRAGE HISTORIQUE

Créé en 1922, le CFM Monaco est l'établissement de référence à Monaco avec plus de 400 collaborateurs et huit implantations sur tout le territoire de la Principauté.

Son appartenance au groupe CREDIT AGRICOLE, sa position dominante et son ancrage historique lui confèrent un rôle majeur dans la vie économique de la Principauté : soutien du tissu industriel et des projets d'infrastructures.

Au-delà de sa proximité auprès des résidents monégasques, le CFM Monaco entretient un dispositif international, au service d'une clientèle non-résidente, personnes physiques ou entreprises.

LE SERVICE AUX ENTREPRISES

La Direction des Entreprises, offre aux entreprises, son concours en matière de crédits d'exploitation, de financements d'activité d'import-export, de traitement des transactions de règlements avec l'étranger ou encore d'opérations documentaires.

L'offre s'étend également à la gestion des excédents de trésorerie destinée notamment aux Institutionnels de la Place, ou encore à la réalisation d'opérations de couverture sur le change et les taux.

Le CFM Monaco offre à sa clientèle d'entreprises et de professionnels une solution standard, automatisée, sécurisée et compatible avec les principaux progiciels de trésorerie disponibles sur le marché, pour traiter par télétransmission les opérations bancaires et les flux financiers courants.

Les opérations bancaires sont traitées automatiquement sans rupture de charge et transmises à distance. Cette procédure limite les incidences des problèmes d'acheminement par voie postale et se fait en toute sécurité. Après contrôle et validation, les opérations sont traitées dans les circuits et les systèmes d'échange de la Place : SIT,CRI, SWIFT, à moindre coût et dans les meilleurs délais.

Le fichier des relevés de comptes peut être directement exploité par un ordinateur équipé d'un logiciel de gestion de trésorerie.

L'ensemble de ces services est traité intégralement sur Monaco par les équipes du CFM Monaco.

E-PRIVATE.MC, LA SOLUTION INTERNET BANQUE PRIVEE DU CFM MONACO

e-Private.mc est un outil multilingue accessible partout dans le monde pour la consultation en ligne des comptes ; Il offre un reporting détaillé sur tous les portefeuilles et les opérations effectuées ainsi que la possibilité d'effectuer des virements internes et interbancaires en temps réel.

e-Private.mc est également équipé d'un système de messagerie pour permettre des échanges confidentiels entre nos clients et nos conseillers, avec le même degré de sécurité que pour la consultation des comptes. Cette sécurité s'appuie sur un triple niveau d'authentification forte : utilisation d'un nom d'utilisateur, d'un mot de passe et d'une carte à code SecurID®.

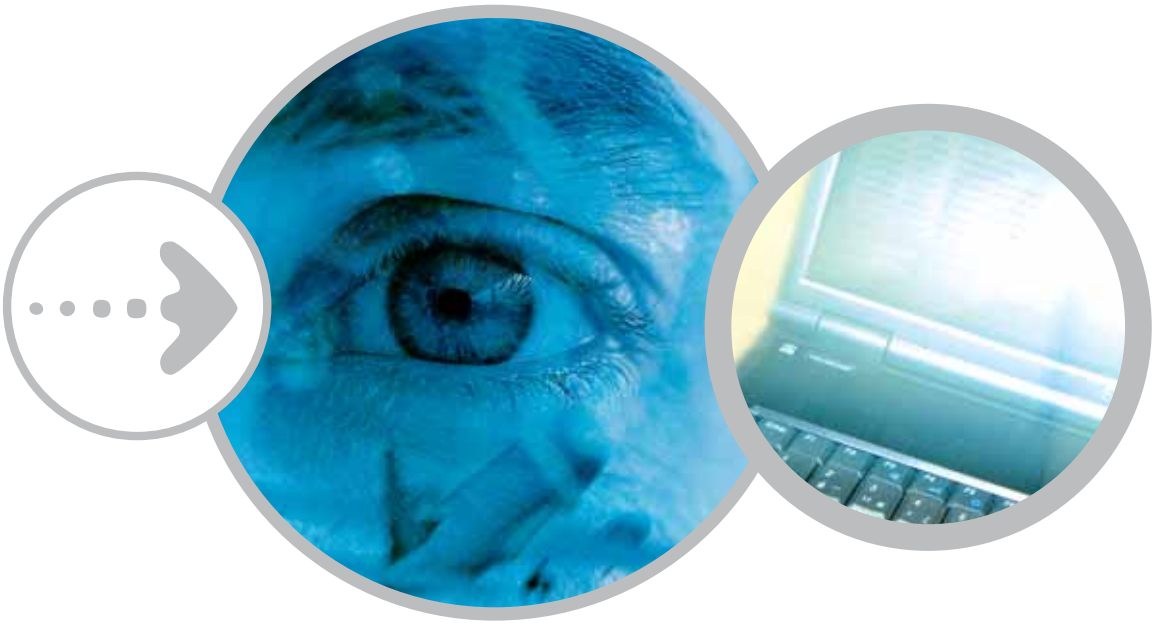
CFM
MONACO

TEKWORLD
GROUPE MICROTEK

> Managers Worldwide Mobile Access (IPass, WeRoam)

> **E-vision** : Entreprise WLAN, VPN Security Solutions & WIFI solutions, IP plateform “VOIP”

> **Activ Portal** : Net Platform allowing CRM, Portal, Workflow, Reporting, Billing, Customized Applications



Ou contactez-nous :
TEKWORLD
2, boulevard Rainier III
MC 98000 Monaco
Tél. +377 93 10 42 82
Fax +377 93 10 42 83
e-mail : info@tekworld.mc

TEKWORLD
GROUPE Microtek