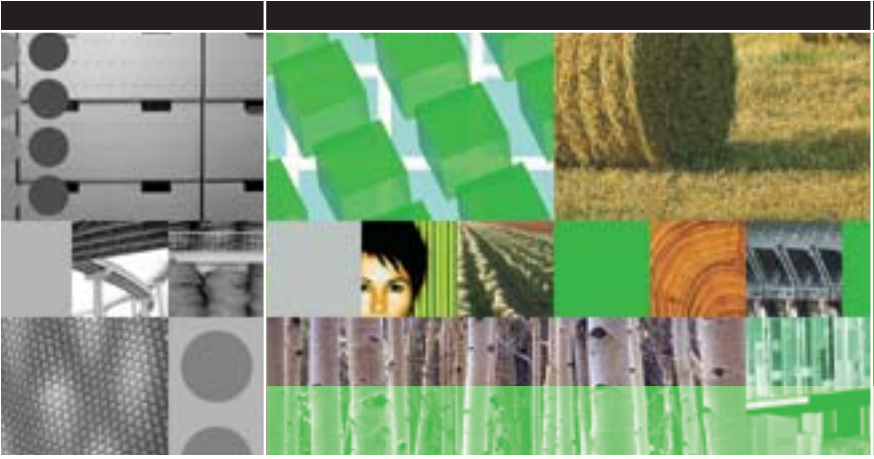
IBM Information Management software

Le courrier électronique et l'archivage légal

ASPECTS TECHNICO-JURIDIQUES

IBM Content Management



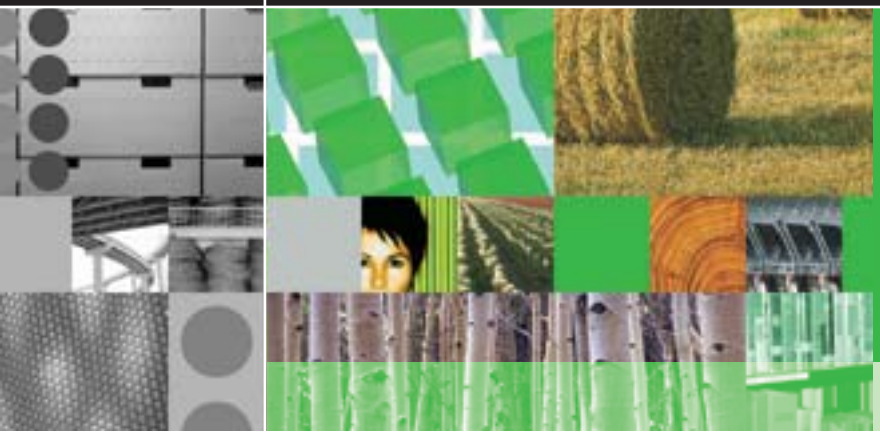
Ce document vise à sensibiliser et à accompagner les décideurs, sans qu'ils soient nécessairement des juristes. L'approche sera technico-juridique et principalement orientée vers les PME. Il sera d'abord traité de l'archivage des messages électroniques, dans le respect de la loi et des règlements. Ce cadre sera étendu à l'archivage des informations jointes sous forme électronique, en soulignant la jurisprudence et les conséquences judiciaires, au regard de la preuve. Le but est de montrer la nécessité de disposer d'une stratégie adaptée à l'entreprise, en prévision d'un système d'archivage organisé et pérenne, valorisant le système d'information et conciliant les besoins de l'entreprise, des utilisateurs et des informaticiens, et servant de fondement à une politique d'archivage légal. Il répond aux questions soulevées sur la légalité des documents numériques, leur conservation et la détermination d'un système d'archivage électronique automatique répondant aux attentes, à court comme à long terme, dans le cadre d'un projet d'entreprise.

Daniel GUINIER
Docteur ès Sciences
Consultant senior certifié CISSP, ISSMP, ISSAP en sécurité des SI
Expert Judiciaire près la Cour d'Appel de Colmar

CE : guinier@acm.org

TABLE DES MATIERES

03



04

PREAMBULE

Des chiffres convergents empruntés à diverses études confirment la croissance en taille des boîtes à lettres de la messagerie électronique des entreprises et les conséquences en termes de coûts de stockage et de difficultés de gestion des volumes qui en résultent. Ils soulignent notamment que :

- jusqu'à 70% des informations utiles[1] se trouveraient dans la messagerie électronique *(source : Enterprise Storage Group)*
- chaque utilisateur traite environ 10 MB de données par jour en 2004, pour atteindre 15,8 MB en 2008 *(source : Radicati Group, Inc)*
- entre 2001 et 2005, le nombre de messages électroniques envoyés a triplé *(source : Horison Information Strategies),*

Les chiffres soulignent aussi qu'une majorité de **temps est consacré à la recherche d'informations** plus qu'à leur exploitation, ceci pour une faible part du chiffre d'affaires, et que **l'archivage manuel reste plus coûteux que sous une forme automatique**[2]. Il y aurait également lieu de **considérer l'archivage de la messagerie électronique** en s'attachant au contexte informationnel et global de l'entreprise, d'autant que **la majorité des ordres, commandes et transactions sont maintenant acceptés par courrier électronique**[3].

Pour prendre la mesure du phénomène, et ses répercussions en termes de stockage, il suffit de considérer une entreprise de 500 utilisateurs : Il en résulte un volume de 5 GB par jour, soit 25 GB par semaine, 100 GB par mois, 1 TB par an, etc., en croissance de facto, et dont il faut considérer les obligations de rétention à long terme.

LE COURRIER ELECTRONIQUE ASPECTS JURIDIQUES

Définition légale

La définition du procédé technique relatif au courrier électronique, ou e-mail, est donnée par la loi LCEN pour la confiance dans l'économie numérique[4] : "*On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère*".

Elle inclut **les messages et les pièces jointes** et ne modifie en rien **le régime juridique de la correspondance privée qui s'applique maintenant au courrier électronique**[5]. Cependant, en cas de contestation, **la qualification du caractère privé** revient à l'autorité juridictionnelle compétente.

[1] Le terme "critique" utilisé dans l'étude paraissant exagéré ou inapproprié pour des données qui relèvent d'opérations courantes, a été substitué par celui de "nécessaire".

[2] 40 à 70% du temps serait lié à la gestion de documents *(source : Forrester Research),* ou encore 50% à la recherche de documents et 5 à 15% à la lecture des informations *(source : Pricewaterhouse Coopers),* pour 5 à 10% du CA *(source : Dataquest).* En outre, l'archivage manuel d'une facture coûte 1,80 € contre 1 € avec un processus automatisé, selon l'Observatoire IBM.

[3] 79% des organismes acceptent la confirmation des ordres par courrier électronique *(source : Osterman Research Inc).*

[4] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), Art. 1 IV, dernier alinéa. La définition est conforme à celle de la télécommunication vu l'Art. 32 du Code des Postes et des Télécommunications.

[5] Comme l'a confirmé le Conseil constitutionnel, dans sa décision n° 2004-496 DC du 10 juin 2004.

Régime juridique du courrier électronique

Les salariés utilisent Internet de manière courante pour trouver des informations ou pour **communiquer avec les membres de l'entreprise, les clients et fournisseurs.** Cet usage est également constaté à des fins non professionnelles : *consultations de sites de loisirs, envoi de messages à titre privé, etc.* Bien qu'**aucune disposition du Code du travail ne leur donne ce droit,** le recours à des fins privées à l'Internet et à la messagerie électronique professionnelle est **un usage généralement admis** pour peu que ce soit **dans des proportions raisonnables** et de façon loyale et respectable, **pour ne pas nuire à l'efficacité du travail et ne pas porter de préjudice à l'entreprise.** L'entreprise peut donc légitimement fixer des règles[6] et mettre en œuvre des contrôles, dans le respect des dispositions légales[7] et la jurisprudence.

Conformément à sa définition par la loi LCEN et à la décision du Conseil constitutionnel, vus précédemment, **le courrier électronique est protégé par le secret des correspondances**[8].

Cas des messages réputés personnels

L'ordonnance de référé rendue par le TGI de Paris le 27 janvier 2003 consacre ce respect du secret relatif aux messages électroniques et le droit des internautes à l'anonymisation[9]. Elle illustre bien la problématique liée aux données à caractère personnel, en distinguant le secret des correspondances et le droit à l'anonymat. La décision est conforme aux Arts. 5, 6 et 15 de la Directive européenne du 12 juillet 2002 concernant le traitement des données et la protection de la vie privée dans le secteur des télécommunications qui s'appliquent notamment **aux serveurs de messagerie électronique**. En outre, l'Art. 5 prévoit que les Etats membres "*interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter,* ***de stocker les communications et les données relatives afférentes,*** *ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés*". Plusieurs décisions, essentiellement en matière d'échange de messages électroniques depuis des postes de travail, ont confirmé que **le courrier électronique bénéficiait du secret des correspondances**[10]. En revanche, **le contrôle de contenus présumés professionnels** des messages, mais aussi des dossiers et des fichiers, **n'est pas attentatoire à ce droit**[11].

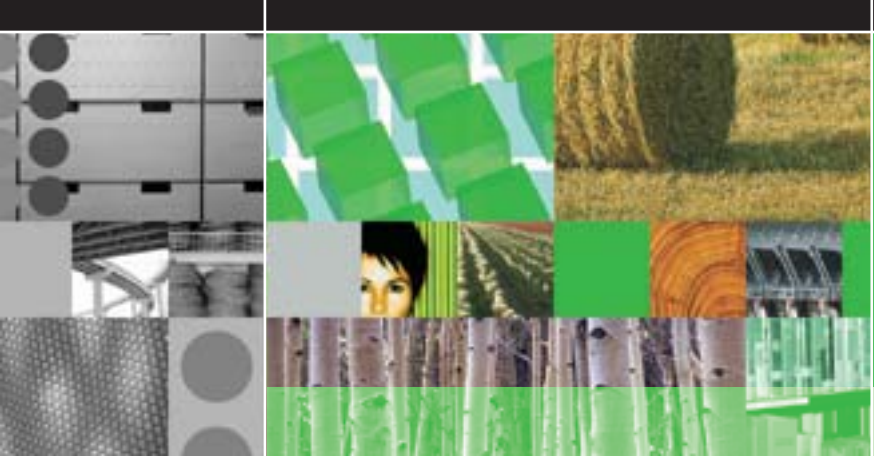
Dès lors, **les contenus et leur gestion sont concernés et le principe général à adopter serait l'effacement sans exception du contenu des messages échangés à titre privé.** Cependant, il ne faut pas en déduire que le droit à l'anonymat ou tout autre s'opposerait à la recherche de la preuve en rappelant aussi qu'en matière pénale, le juge

[6] Dans son rapport du 6 février 2002, la CNIL proposait aux entreprises la rédaction de chartes prévoyant les modalités d'utilisation de l'informatique et tout particulièrement de la messagerie : règles d'utilisation des TIC, information des salariés sur la mise en place moyens de surveillance, risques liés à cette utilisation et notamment au regard de comportements ou de pratiques illicites par ce biais pouvant engager la responsabilité civile ou pénale de l'utilisateur ou/et de l'entreprise.

[7] Etant acquis que le salarié a droit au respect de sa vie privée, y compris sur son lieu de travail, au vu de l'Art. 9 du Code civil et de l'Art. 8 de la Convention européenne des droits de l'homme.

[8] En matière de télécommunications, c'est l'Art. 1er de la loi n° 91-646 du 10 juillet 1991, relative au secret des correspondances émises par la voie des télécommunications, qui constitue la base juridique du droit positif français ; sa violation relevant des Arts. 226-15 et 432-9 du Code pénal.

[9] Désirant intenter une action contre l'auteur de messages diffamatoires, la victime réclamait la communication de l'identité de l'utilisateur de l'adresse mail et la conservation des messages envoyés à partir de celle-ci. Le juge des référés a soutenu l'opposition de Lycos du fait que : "*les courriers électroniques sont des correspondances privées bénéficiant du secret*". Le contraire aurait caractérisé une violation de l'Art. 226-15 du Code Pénal qui punit : "*l'interception, le détournement, l'utilisation ou la divulgation de correspondances émises*", conformément à l'Art. 3 de la Convention sur la cybercriminalité du Conseil de l'Europe. Plusieurs décisions, en matière d'échange de messages électroniques depuis des postes de travail, ont depuis confirmé que le courrier électronique bénéficiait du secret des correspondances.



peut ordonner l'interception[12] et la communication de l'ensemble des messages émis et reçus ou encore stockés. Dans un arrêt récent concernant les fichiers et non les correspondances, la Cour de cassation énonce les règles à respecter[13] : ***"sauf risque ou événement particulier***[14], ***l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur*** *de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé".* En précisant : *"les fichiers identifiés par le salarié comme étant personnels",* la Cour de cassation restreint **la qualification "*personnel*" à un acte volontaire de l'utilisateur.**

Avec la messagerie Outlook, le dossier principal qui contient les courriers électroniques est nommé automatiquement "*Dossiers personnels*" et selon la documentation, "*personnel*" fait référence à des fichiers non situés sur un serveur. **"*Personnel*" revêt ici un sens différent par rapport au droit** et, conformément à la jurisprudence actuelle, ne devrait pas être présumé "personnel".

Cas des données présumées professionnelles

Au vu de la jurisprudence, les correspondances : *dossiers, fichiers, ou tous écrits,* à caractère personnel ne peuvent faire l'objet d'une surveillance ou d'une saisie sans contrôle préalable, judiciaire ou émanant des représentants du personnel. Cependant, **le caractère personnel ne peut être présumé** et l'apposition d'une mention "personnel" reste déterminante. **C'est la qualification formelle de "personnel" de l'information qui paraît être le critère à retenir** pour considérer s'il y a atteinte ou non à la vie privée. Sans cela, **les informations reçues sur le lieu de travail sont présumées comme relevant du domaine professionnel.**

Le juste équilibre entre l'exercice du pouvoir de direction et le respect de la vie privée n'est pas évident. La difficulté réside dans la matérialisation de la frontière entre ce qui relève de la vie privée et de la vie professionnelle. Si le pouvoir de contrôle de l'entreprise sur le lieu de travail s'accorde avec la nécessité de direction[15], ce pouvoir unilatéral n'est pas sans limite. Il est soumis au droit du respect à l'intimité de la vie privée qui continue d'exister au sein de l'entreprise[16], lequel est différencié du droit au secret des correspondances. **Il reste soumis au respect des principes de proportionnalité, de transparence, de bonne foi et de respect du contradictoire,** et s'arrête si le domaine "personnel" est expressément identifié.

[10] En particulier l'Arrêt de la Cour Cassation, Ch. Soc., du 2 octobre 2001, D.2001, p. 3148, dit : "*Arrêt Nikon*", disant que "*le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur*".

[11] Arrêt de la Cour d'Appel de Bordeaux, Ch. Soc., du 10 juin 2002

[12] Au vu des Arts. 100 à 100-7 du Code de Procédure Pénale.

[13] Arrêt de la Cour de cassation, Ch. Soc., du 17 mai 2005. En l'occurrence, après la découverte de photos érotiques dans le tiroir du bureau d'un salarié, il avait été procédé à une recherche sur le disque dur de l'ordinateur de ce dernier, ce qui avait permis de trouver des dossiers étrangers à ses fonctions figurant dans un répertoire intitulé "perso".

[14] Le principe de proportionnalité tel posé par l'Art. L. 120-2 du Code du travail impose aussi que les faits présentent un degré de gravité suffisant pour que l'employeur soit autorisé à outrepasser le principe du contradictoire.

[15] Au sens de l'Art. 1384 al. 5 du Code Civil et de l'Art. 121-2 du Code Pénal.

[16] L'employeur est tenu au respect de la vie privée de ses salariés, en vertu de l'Art. 9 du Code civil et de l'Art. 8 de la Convention européenne des droits de l'homme, et l'Art. L 120-2 du Code du travail interdit : "*d'apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*".

07

Cas de suspicion légitime et tendance des obligations

Il reste délicat voire impossible de contrôler un contenu indiqué comme "personnel" lorsque des indices laissent penser que des informations professionnelles sont présentées comme personnelles, notamment pour leur **détournement,** ou en cas d'**utilisation abusive** des moyens de l'entreprise ou du temps de travail, à des fins personnelles. **Dans un tel cas de suspicion légitime, l'entreprise peut effectuer un contrôle, sous réserve de respecter les principes précédents.** La collecte loyale des preuves selon ces principes est une **mesure de sécurité juridique,** tant pour l'entreprise que pour le salarié. Il est cependant prudent que ce contrôle soit effectué en présence de l'intéressé, avec information des représentants du personnel[17]. Il peut être utile de déposer une requête[18] visant à établir la preuve d'un comportement fautif, en autorisant un huissier compétent à instrumenter une copie à l'identique des informations présentes sur le serveur et du disque dur du poste de travail incriminé, en les plaçant sous scellés pour expertise, avec l'aide d'un expert nommé. La saisine de l'autorité judiciaire compétente s'impose de fait si les agissements sont pénalement répréhensibles.

La jurisprudence, stricte en matière de contrôle de l'usage des technologies de l'information et de la communication (TIC) **place les employeurs dans une situation délicate.** En outre, ils viennent d'être qualifiés de fournisseur d'accès par la Cour d'appel de Paris, ce qui a pour conséquence, **l'obligation de conserver et détenir les données de connexion** permettant d'identifier toute personne ayant contribué à la création d'un contenu illicite, alors que le contrôle de salariés peu respectueux est encore compliqué à mettre en œuvre. Ceci impose visiblement une stratégie pour la sensibilisation et la formation des personnels pour le respect de la politique de sécurité interne et des règles en vigueur pour la messagerie et l'archivage.

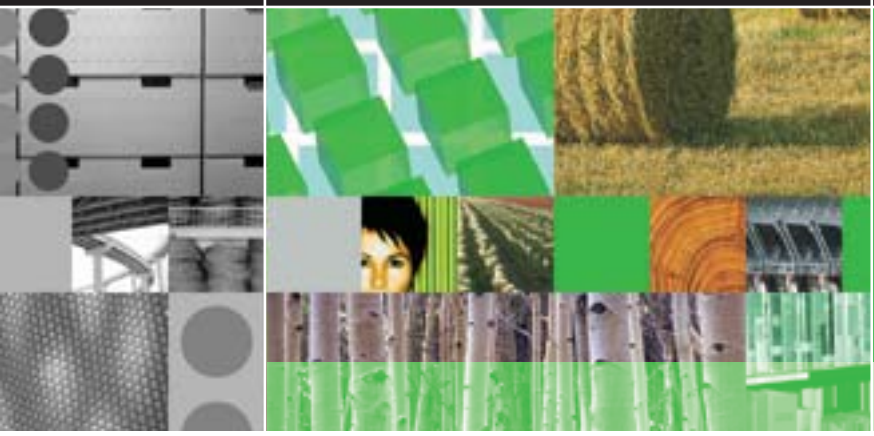
Confirmant la tendance à l'obligation de loyauté des utilisateurs, un arrêt de la Cour d'appel de Besançon du 9 septembre 2003, a précisé qu'un salarié ne saurait utiliser un ordinateur professionnel à des fins personnelles, sans que cette possibilité lui ait pour cela été notifiée. De plus, un arrêt de la Cour de cassation, Ch. Crim., du 19 mai 2004 avait condamné un salarié qui gérait un site pornographique via la connexion de l'entreprise et ceci, pendant ses heures de travail, en retenant ici la qualification d'abus de confiance.

EN RÉSUMÉ

La messagerie électronique inclut les messages et les documents joints. Son régime juridique relève en grande partie de la protection du secret des correspondances en distinguant le cas des messages réputés personnels de celui des données présumées professionnelles. La jurisprudence fondée sur la loyauté et la sécurité juridique place les employeurs en situation délicate en imposant le respect de principes stricts et la suprématie du domaine "personnel".

[17] Voir les arrêts de circonstances opposées de la Cour d'appel de Besançon, du 21 septembre 2004, jugeant légitime le processus de collecte des moyens de preuve, et de la Cour d'appel de Paris, du 5 janvier 2005, jugeant irrecevable le fait copier l'intégralité du disque dur de l'ordinateur du salarié licencié au motif apparent de sécurité informatique.

[18] Fondée sur l'Art. 145 du Nouveau Code de procédure civile, aux fins d'obtenir une ordonnance du tribunal.



08

L'ARCHIVAGE ELECTRONIQUE ASPECTS JURIDIQUES

Définition légale

La définition légale est donnée par la loi 79-18 du 3 mars 1979 sur les archives et l'Art. L211-1 du Code du patrimoine : "*Les archives sont l'ensemble des documents,* ***quels 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 leur activité.* ***La conservation de ces documents est organisée*** *dans l'intérêt public tant pour les* ***besoins de la gestion*** *et de* ***la justification des droits*** *des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche*".

L'énoncé fait apparaître la **reconnaissance de l'archivage électronique de documents provenant de tout support :** *papier, électronique, etc.,* **et introduit sa force probante,** au vu de sa destination pour la justification de droits. Il introduit les contraintes de pérennité des informations et de leur restitution à l'identique ; ce qui implique la **fiabilité** et la **sécurité** du dispositif. Il s'agit pour cela de disposer de composants et de services pour réaliser un archivage conforme à l'état de l'art et dans des conditions légales et économiques acceptables[19].

Régime juridique de l'archivage électronique

Des **contraintes sont imposées** par les dispositions du Code du patrimoine[20] concernant les archives et l'organisation de la conservation des documents. Elles **distinguent les archives publiques et privées, sans que le régime applicable à la conservation ne soit pas précisé** en ce qui concerne ces dernières, et donc les entreprises. Elles seront alors trouvées d'une part, dans le Code civil, le Code de commerce, le Code du travail, le Livre des procédures fiscales[21], et d'autre part, en rapport avec d'autres éléments, au regard du droit d'auteur[22] et de la propriété intellectuelle[23]. D'autres enfin relèvent de la réglementation, comme les déclarations à la CNIL, ou du secteur ou des activités, ou pour assurer **la traçabilité relative à la chaîne du risque.**

Enjeux au vu de loi de sécurité financière

Des enjeux relatifs à l'archivage électronique naissent aussi de la loi de sécurité financière (LSF) n° 2003-706 du 1er août 2003, *suite à la loi américaine Sarbanes Oxley (SOX) de juillet 2002.* Il est dorénavant fait **obligation aux dirigeants de mettre en place un système de contrôle interne** dans l'entreprise. Bien que le contrôle interne n'ait pas de définition juridique, il s'agit d'un dispositif visant à fournir une assurance raisonnable du respect des obligations légales à appliquer, la fiabilité des informations, et l'efficience de la conduite des opérations. **L'Ordre des Experts**

[19] La norme ISO 15489 le définit comme "*un système d'information qui intègre les documents, les organise, les gère et les rend accessibles à terme*", et la norme française Afnor NF Z42-013, de façon voisine comme "*l'ensemble des actions, des outils et des méthodes mises en œuvre pour conserver, à moyen ou long terme, des informations dans le but de les exploiter*".

[20] La codification remplace les dispositions définies par la loi n° 79-18 et sa modification par la loi n° 2000-321, en particulier au vu de la loi n° 2004-801 du 7 août 2004 et des données à détruire à l'expiration d'une durée prévue.

[21] Code civil : Arts. 2262 et 2277 ; Code de commerce : Arts. L110-1 et -4, L123-21, L123-22 et L235-9, Code du travail : Arts. L143-14, L231-9, L424-5, R620-3 et L620-3, Livre des procédures fiscales : Arts. L102 B, L169 et L176.

[22] En particulier, loi n° 85-660 du 3 juillet 1985, relative aux droits d'auteurs de logiciels, loi n° 92-597 du 1er juillet 1992, relative au Code de la propriété intellectuelle, et loi n° 94-361 du 10 Mai 1994 relative à l'environnement, aux critères d'originalité, à la création des logiciels dans l'entreprise.

[23] Le droit d'auteurs vise à protéger une œuvre pour une durée de 70 ans après le décès de l'auteur ou du dernier auteur pour une œuvre de collaboration, et 70 ans après sa publication pour une œuvre collective, et le brevet d'inventeur, le contrôle par le détenteur pour une durée de 20 ans à compter de la date de dépôt.

Comptables français le définit comme l'ensemble des politiques et procédures[24] mises en œuvre en vue d'assurer, dans la mesure du possible, la gestion rigoureuse et efficace de ses activités ; ce qui n'est pas limité exclusivement aux informations comptables et financières.

La loi française apparaît moins précise que la loi américaine. Elle ne définit ni les procédures de contrôle interne, auxquelles elle fait référence, ni les moyens permettant d'assurer ce même contrôle. Elle dispose que les dirigeants doivent rendre compte des **procédures de contrôle interne** mises en place au sein de l'entreprise en assurant la meilleure transparence possible[25]. **La loi américaine** s'applique à toute société qui émet des titres enregistrés auprès de la SEC ou placés sur le marché public américain. Elle concerne aussi les quelques entreprises françaises qui entrent dans ce cadre. Elle prévoie des dispositions pour l'obligation des dirigeants d'évaluer la **qualité du contrôle interne** afin de permettre la présentation d'une situation financière fidèle et également les fraudes susceptibles d'avoir été réalisées. En outre, **elle impose la mise en place d'un système d'archivage susceptible de fournir rapidement des informations sur l'historique financier.**

Il est clair que **les systèmes d'informations participent au contrôle interne,** dès lors que la grande majorité des transactions de l'entreprise sont enregistrées sous une forme électronique. **L'obligation d'archivage des données relève ici de la mise en œuvre des procédures de contrôle interne** en disposant de moyens adéquats, pour retrouver rapidement les informations comptables, financières, et de gestion, communiquées aux organes sociaux, et ensuite en contrôler la pertinence et le reflet de la sincérité par rapport à l'activité et la situation de l'entreprise. De plus, la loi américaine impose de façon formelle **la conservation de la messagerie électronique.**

Aussi, en **vue d'appréhender correctement l'archivage,** il paraît nécessaire de **prévoir :**

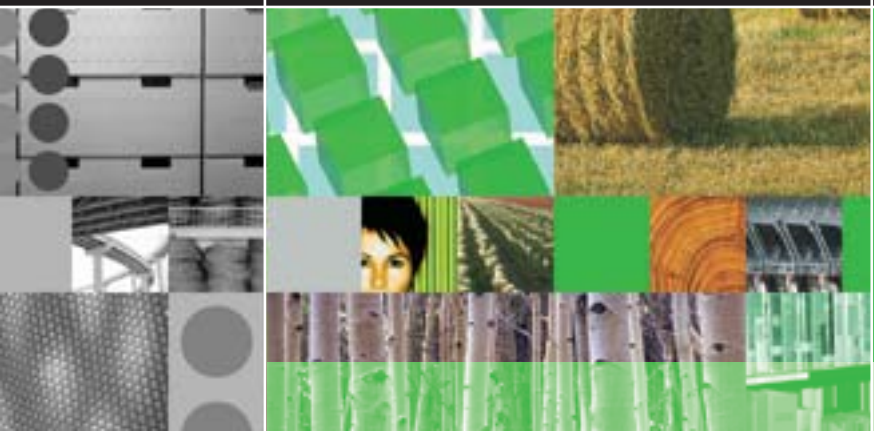
- **les obligations usuelles et celles relatives au contrôle interne,**
- **les relations entre les directions** impliquées,

Les directions générale, financière, juridique, de l'audit, et celle des systèmes d'information, seront appelées à se rapprocher pour travailler ensemble. Il est utile de rappeler que **la direction générale demeure responsable du respect des obligations légales,** tandis que l'archivage est à considérer ici comme un **outil de la lutte contre la fraude.**

Règlements attachés aux établissements financiers

Le Code monétaire et financier prévoit notamment que la Banque de France (Art. L 141-4 –I), veille au bon fonctionnement et à la sécurité des systèmes de paiement. Elle est habilitée au sens de l'Art. L 144-1 à se faire communiquer par **les établissements de crédit et financiers** tous **documents et renseignements** qui lui sont nécessaires pour exercer les missions qui lui ont imparties par la loi.

Le règlement du Comité de la réglementation bancaire et financière **CRBF n° 97-02** du 21 février 1997, relatif au contrôle interne des établissements de crédit[26], fixe des règles de conservation des données qui imposent aux entreprises des contraintes nouvelles en termes d'archivage de données, de conservation de la documentation, des applications, à l'Art.14. En outre, l'Arrêté du 31 mars 2005 portant sur **sa modification** intègre aussi des exigences en vue de la **continuité des activités** dans les **conditions applicables en matière d'externalisation,** ce qui traite du plan de continuité (PCA) ou de reprise (PRA) d'activité, selon le cas.



10

Le règlement général relatif aux **conseillers en investissements financiers** (CIF) prévoit dans son Art. 335-8, que le CIF doit disposer de moyens techniques et de procédures adaptés à l'exercice de son activité, et aux termes de la consultation du 3 juin 2004, il lui est fait **obligation de disposer en permanence** de moyens techniques suffisants et notamment d'un **outil d'archivage sécurisé.**

EN RÉSUMÉ

L'archivage électronique concerne l'organisation et les règles de sélection et de conservation, en particulier liées à la messagerie, essentiellement pour les besoins de gestion des documents et de la justification des droits. Sa force probante, implique de disposer de composants et de services pour réaliser un archivage conforme à l'état de l'art, et dans des conditions légales et économiques acceptables. De nouveaux enjeux sont liés à l'obligation de mise en place d'un système de contrôle interne. Ils imposent la mise en place d'un système d'archivage adéquat, avec prise en compte de la messagerie et de la nécessité de rapprocher les directions pour un tel projet. D'autres sont attachés au respect des règlements particuliers aux secteurs bancaire et financiers.

[24] Visant le respect de politiques de gestion, l'exactitude et l'exhaustivité des enregistrements comptables, et la fourniture en temps voulu d'informations fiables.
[25] Dans le rapport annuel présenté aux actionnaires lors de l'assemblée amenée à statuer sur les comptes de l'exercice.
[26] Traitant du contrôle des procédures et des opérations internes, du contrôle de conformité, du système de surveillance des risques, et des conditions en matière d'externalisation.

LA PREUVE ELECTRONIQUE ET SON APPRECIATION

Enjeux et fondements de la preuve

L'archivage électronique est une préoccupation majeure des entreprises et de l'Etat. Les besoins ne sont pas toujours bien définis et le traitement reste délicat, compte tenu des enjeux, des volumes variés et croissants générés et des aspects légaux relatifs au secteur et aux activités, avec notamment un délai de conservation à plus ou moins long terme. **Il devient encore plus sensible s'il s'adresse au courrier électronique,** lequel peut être professionnel, mais aussi personnel. La confiance dans les procédures et leur mise en œuvre par **un dispositif automatique est un facteur clé.** Les principaux enjeux sont de trois types :

- **Les enjeux juridiques** se situent au niveau des **responsabilités,** en fonction des différents services et fonctionnalités envisagés, et de celui des obligations au vu de la **réglementation** et de **la preuve,**
- **Les enjeux organisationnels** se situent au niveau de **la politique** pour la prise en charge de l'archivage par l'entreprise ou de s'en remettre à un tiers,
- **Les enjeux techniques** se situent au niveau de la **capacité** à offrir ces services en fonction de l'architecture et des technologies utilisées, de leur niveau de maturité et de leur mise en œuvre, **dans le respect de l'état de l'art au vu des normes.**

L'ensemble renvoie à **la question de la force probante** qui doit être pérenne, au travers de la fiabilité et de la sécurité, et de façon récurrente, à la conservation de la preuve elle-même. En outre, la loi française sur la Sécurité Financière[27] dispose que la direction générale doit rendre compte des procédures de contrôle interne en place au sein de

l'entreprise, mais ne définit ni les procédures auxquelles elle fait référence, ni les moyens permettant d'assurer ce contrôle[28]. L**a principale difficulté est d'assurer en toutes circonstances** le stockage et la restitution des documents électroniques ayant une valeur légale, sur une période différentiée à plus ou moins long terme **malgré l'obsolescence technologique.**

La valeur légale des documents électroniques est consacrée par la loi n° 2000-230 du 13 mars 2000[29]. Outre la définition précise des **notions de preuve et de signature,** les dispositions de la loi reconnaissent **la même force probante à l'écrit sur support électronique que celui sur support papier**[30]. Cette valeur est à apprécier sous les angles de la qualité du document original ou de sa copie, des **modalités de conservation et du système probatoire dans lequel elle s'inscrit**[31]. En particulier, **les factures** peuvent être transmises par voie électronique[32], et archivées sous cette forme, dès lors que l'authenticité de l'origine et l'intégrité du contenu sont garantis. Il en découle qu'ainsi, **elles tiennent lieu d'original**[33]. Des besoins en archivage organisé naissent donc de cette loi, pour la conservation à des fins probatoires.

Systèmes probatoires

La notion de preuve et sa validité sont intimement liées au système probatoire auxquelles elles se réfèrent. **En matière civile**[34], **la preuve est limitée** et **caractérisée par une hiérarchie** où l'acte authentique occupe le rang de preuve le plus élevé[35]. Elle repose sur une présomption de probabilité relative. Il est à rappeler qu'**en droit du travail,** "*si un doute subsiste, il profite au salarié*"[36], en matière de licenciement ou de sanction disciplinaire. **En matière pénale, la preuve** est **libre de tout moyen** et **caractérisée par l'absence de hiérarchie** de preuves. Dans tous les cas, elle repose sur l'intime conviction du juge, au bénéfice du doute. Enfin, **la forme électronique ne constitue pas un obstacle** aux moyens de la preuve qui est soumise à contradiction. Il y a cependant lieu de disposer d'une **copie réputée fidèle et durable**[37] par rapport à l'original indépendamment de la forme : *électronique ou papier.*

[27] Loi française de sécurité financière n° 2003-706 du 1er août 2003.

[28] Contrairement à la loi américaine avec le "*Sarbanes Oxley Act 2002*" (SOX), qui s'applique aux sociétés qui émettent des titres placés sur le marché américain, où il est prévu l'obligation d'évaluer la qualité du contrôle interne et notamment la mise en place d'un système d'archivage des données financières et comptables, ce qui est assurément l'un des moyens attendus pour produire des justificatifs rapidement et en toutes circonstances. De surcroît, la règle 17a-4 de la commission SEC (Securities Exchange Commission) oblige les institutions financières américaine à archiver les documents électroniques, y compris les messages électroniques, au moins six ans. Enfin, le standard US DoD 5015-2-STD, considère que les messages électroniques sont à traiter comme tout autre document enregistré.

[29] Cette évolution s'est traduite par la refonte des Arts. 1316 et suivants du Code civil. Des précisions ont été apportées par le décret n° 2001-272 du 30 mars 2001 et par l'arrêté du 26 juillet 2004.

[30] Art. 1316-3 du Code civil.

[31] C'est pourquoi, au sens juridique, la qualification de valeur légale d'un document reste préférable à celle d'archivage légal, plus générale et couramment utilisée.

[32] L'extension à la facturation électronique relève de loi de finances rectificative n° 2002-1576 du 30 décembre 2002 et des décrets d'application n° 2003-632 du 7 juillet 2003 et 2003-659 du 18 juillet 2003.

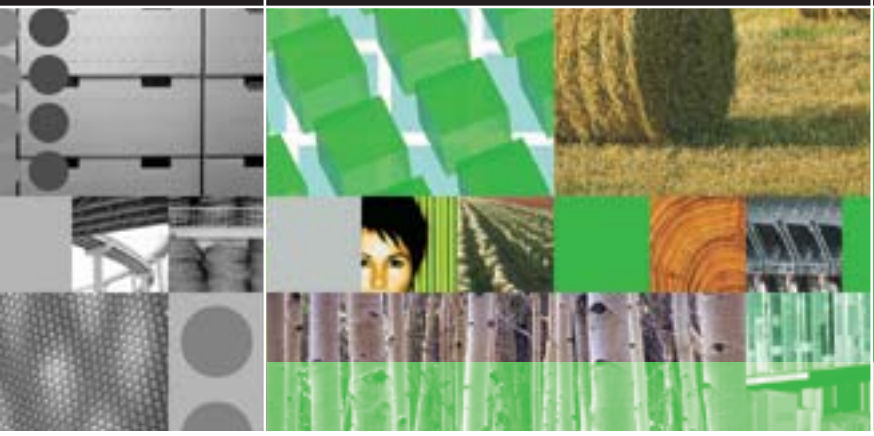
[33] En application de l'Art. 25 de la loi n° 2000-230 du 13 mars 2000 et de l'Art. 286 du Code général des impôts.

[34] Au titre du droit civil, les règles de preuve peuvent être aménagées conventionnellement. En droit commercial la preuve est libre mais n'exclut pas une hiérarchie des preuves, comme en droit civil, pour les transactions inférieures à 762 ?. En droit administratif, elle est libre et sans hiérarchie, et le juge a un rôle actif dans la recherche de la preuve.

[35] Ainsi, un acte authentique établi dans la régularité ne pourrait être combattu par un acte sous seing privé.

[36] Art. L 122-14-3 du Code du travail.

[37] Une reproduction indélébile de l'original qui entraîne une modification irréversible du support est réputée durable. Ceci justifie l'archivage électronique sur des supports non réinscriptibles de documents issus d'originaux transformés par des procédés de numérisation.



En matière civile, la notion de "*risque ou événement particulier*", qui permettrait à l'entreprise d'examiner et copier un domaine attribué à un employé, doit être interprétée de manière restrictive et limitée à des cas exceptionnels ou de force majeure. En outre, hors de sa présence, les termes "*dûment appelé*" imposent que le salarié soit personnellement informé et donne son accord, pour ne pas violer le principe du contradictoire et ainsi, **éviter l'insécurité juridique**[38]. En revanche, **en matière pénale, "*aucune disposition légale ne permettait au juge répressif d'écarter les moyens de preuve produits*** *par les parties aux seuls motifs qu'ils avaient été obtenus de façon illicite ou déloyale.* ***Il lui appartient seulement d'en apprécier la valeur probante***"[39].

Lors d'un contentieux opposant un employeur et un salarié, les juges, conscients des possibilités de mystification et de truquage et de la fugacité des données électroniques, examineront l'ensemble des preuves, indépendamment des termes de la charte ou du règlement interne. Il y a donc lieu à être **prudent en matière de collecte de preuve électronique,** qui doit être fidèle, fiable et inaltérable, pour ne pas être rejetée. Il ne doit pas non plus exister de doute quant à l'**imputabilité** des faits à la personne ou à l'identité de l'expéditeur de messages incriminés.

Critères et limites associés à la preuve

D'une façon générale, **la preuve est indissociable de l'archivage** et répond à des critères d'origine et de fidélité concernant l'acquisition des documents selon l'ensemble des procédés qui sont utilisés tant **pour la réalisation que pour la transmission et la conservation intègre des messages et des fichiers.** Ceci traite de l'intégrité du contenu et des données afférentes, de la durabilité de la conservation et de l'accessibilité par un format et un dispositif adéquats, soutenus par une bonne organisation et des procédures opérationnelles, de contrôle et d'audit qui sont appliquées.

Au vu de l'Art. 1316 du Code civil[40], la preuve couvre désormais les écrits sous format électronique, sous réserve que puisse être dûment

[38] Etendant à l'informatique un arrêt du 11 décembre 2001, la Cour de cassation, dans son arrêt du 17 mai 2005 pose le principe que la nature personnelle d'un fichier ne suffit pas à le soustraire au contrôle de l'employeur ; reconnaissant ainsi à ce dernier le droit d'accéder aux fichiers personnels d'un salarié enregistrés sur son poste de travail, en précisant les conditions étroites restrictives :
"*... sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé...*", pour ne pas entrer en violation avec les Arts. 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du Code Civil, 9 du nouveau Code de Procédure civile et L.120-2 du Code du travail.

[39] En vertu de l'Art. 427 du Code de Procédure Pénale. Par exemple : Suite à la preuve rapportée par l'examen du contenu du disque dur de son poste de travail, le Directeur de cabinet du Conseil général de la Sar¬the a été condamné pour enregistrement et recel d'images à caractère pédo-pornographique, par le Tribunal correctionnel du Mans.

[40] L'Art. 1316 du Code Civil énonce que : "*La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous les autres signes dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*", l'Art. 1316-1 précise que : "*L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à garantir l'intégrité*". L'Art. 1316-4 du Code civil poursuit : "*La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat*". Avant même l'adoption de textes lui reconnaissant sa valeur juridique, un arrêt du 20 octobre 2000 de la Cour d'Appel de Besançon, montre que juge apprécie librement cette fiabilité.

[41] Le décret n° 2001-272 du 30 mars 2001 précise les exigences d'un procédé de signature électronique pour qu'il soit considéré comme fiable. Dans les faits, la signature sécurisée reposera sur l'utilisation d'un certificat électronique pour en permettre la vérification, en plus du dispositif sécurisé pour sa création. C'est le Décret n° 2002-535 du 18 avril 2002 qui fixe les conditions d'évaluation et de certification de la sécu¬rité offerte. Enfin, c'est l'Arrêté du 26 juillet 2004 qui donne les modalités de la reconnaissance de la qualification des prestataires de services de certification électronique et de l'accréditation des organismes qui procèdent à leur évaluation.

[42] Voir Art. 1 du Décret n° 2001-272 du 30 mars 2001.

[43] L'existence légale des conventions de preuve, sans toutefois en fixer les conditions de validité relève de la loi n° 2000-230 du 13 mars 2000 et de l'Art. 1316-2 du Code civil.

identifié l'émetteur et que l'établissement et la conservation soient dans des conditions de nature à garantir l'intégrité. Dans ces conditions, **la valeur probante** de la forme électronique **est subordonnée à l'archivage et aux critères de la fiabilité.** Celle-ci sera présumée, jusqu'à preuve contraire, **lorsque la signature électronique** est créée[41], l'**identité** du signataire assurée et l'**intégrité** de l'acte garantie, dans des conditions fixées par la loi.

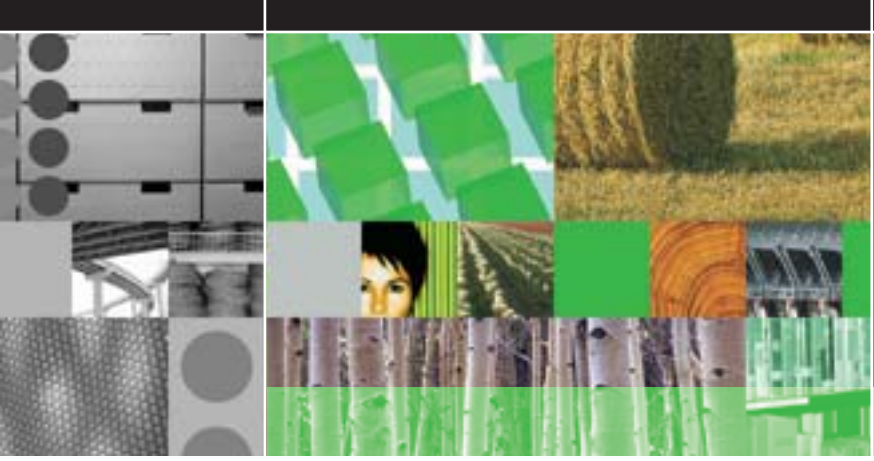
Cependant, si la Loi du 13 mars 2000 a posé le principe d'indépendance entre l'écrit et son support, un document numérique reste lié à son environnement : *matériel, logiciel, système d'exploitation, système de fichiers, format, etc.* Aussi, **la pérennité des signatures électroniques sécurisées**[42] reste un point délicat, à cause du **délai entre la création de la signature et sa vérification** potentielle, **des années après,** alors qu'une migration incontrôlée risquerait d'affecter la visibilité du document, le processus de vérification de la signature ou la disponibilité du certificat, notamment dans la cas du recours à un tiers de confiance. En tout cas, il doit être possible de prouver qu'un contenu est ce qu'il est censé être et qu'il a bien été créé, approuvé ou transmis par la ou les personnes prétendues, de surcroît au moment indiqué ; **ce qui implique aussi l'horodatage.**

Conventions de preuves

En l'absence ou en complément de dispositions légales expressément applicables à l'archivage électronique et au de la faiblesse de la jurisprudence sur l'applicabilité du régime juridique des copies à l'archivage électronique, il est à la fois possible et prudent de **recourir à des mécanismes contractuels de conventions de preuve**[43]. Il s'agit d'un contrat ayant une existence légale et conclu entre deux parties dont l'objet est de définir les **modes de preuve admissibles** en renvoyant à des textes législatifs et normatifs, **la charge de la preuve et les modalités de règlement des conflits de preuve,** peur peu que le contrat respecte la loi et les règlements applicables et ne porte atteinte ni aux règles d'ordre public, ni aux dispositions légales et réglementaires sur les clauses abusives. La finalité est d'apporter des garanties et précisions sur la force probante des documents découlant du système d'archivage électronique. Dans ces conditions les juges d'un libre et meilleur pouvoir d'appréciation. De telles conventions seront **particulièrement utiles** en cas d'externalisation ou de recours à des tiers de confiance, et pour les relations avec des **entreprises et filiales étrangères.**

Cas de copies d'originaux

Lors de l'archivage électronique des originaux sur support papier ou sur microformes, il faut s'interroger sur le document électronique qui en résulte, en particulier s'il peut être **considéré comme la copie électronique du document original et admis comme preuve** sous réserve du respect de certaines conditions. Sans précisions sur les modalités, il est possible de se reporter aux dispositions du Code civil qui définissent les **caractéristiques que doivent présenter les copies pour être admises à la place des originaux.** L'Art. 1334 du Code civil prévoit notamment qu'une copie peut être présentée à la place d'un original notamment en cas de perte du titre par la suite d'un cas fortuit ou d'une force majeure (Art. 1348 al. 1) ou lorsque l'original n'a pas été conservé et que la partie présente une copie qui en est la reproduction non seulement fidèle mais aussi durable (Art. 1348 al. 2), alors que ces dispositions étaient déjà invoquées pour reconnaître la force probante de photocopies. Toutefois, elles sont soumises aux mêmes caractéristiques de fiabilité et de durabilité déjà évoquées et **les débats sur la fidélité** précisent que la copie doit porter en elle les traces de toute



modification ou altération intervenue et les garanties d'intégrité du contenu. Enfin, en raison des difficultés qui existent pour rapporter la preuve du caractère fidèle et durable, **une expertise judiciaire est souvent ordonnée.**

Cas des marchés publics

Depuis le 1er janvier 2005, **les collectivités territoriales doivent être en mesure d'accepter les réponses à appels d'offre publics transmises par voie électronique**[44]. Ainsi, le règlement et la lettre de consultation, le cahier des charges, et les documents et autres renseigne¬ments peuvent être mis à disposition par voie électronique, selon les termes du Décret n° 2002-692 du 30 avril 2002[45]. Réciproquement, les candidatures et les offres peuvent être communiquées à la personne publique par voie électronique par les soumissionnaires. Par ailleurs, l'authentification de la signature du candidat fait référence aux exigences des Arts. 1316 à 1316-4 du Code civil. Ainsi, la si¬gnature électronique établie dans les conditions spécifiées par le dispositif réglementaire[46] permet de donner à un écrit électronique la même force probante que sur un support papier. De même, **des enchères électroniques peuvent être organisées** pour l'achat de fournitures courantes selon les termes du Décret n° 2001-846 du 18 septembre 2001[47].

L'archivage et les aspects sécurité sont tout particulièrement importants dans ces procédures, pour éviter toute présentation ou modification frauduleuse ou contestation intempestive ou injustifiée, ou remise en cause l'anonymat ou des responsabilités.

Cas des formalités et actes authentiques électroniques

L'ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines **formalités contractuelles par voie électronique**[48] modifie les Arts. 1369 et 1325 du Code civil. Elle complète le dispositif législatif pour la **reconnaissance juridique des actes et des contrats électroniques, transmis par courrier électronique,** et notamment le recours à l'envoi d'une **lettre recommandée électronique** acheminée par un tiers par ce mode de transmission. En particulier, l'Art. 1369-9 prévoit que **la remise d'un écrit sous forme électronique est effective lorsque le destinataire en a accusé réception,** après avoir pu en prendre connaissance. En outre, les conditions de validité d'un contrat conclu à titre professionnel sous forme électronique se réfèrent aux Arts. 1369-4 et 1369-6 du Code civil, suite à la loi LCEN et à l'ordonnance citée, et s'appliquent notamment aux prestations de biens et de services, et tout particulièrement aux logiciels et informations fournis à titre onéreux ou gratuit, avec la nécessité de marquer le consentement au moyen d'un "*double clic*".

[44] Au vu du dispositif réglementaire et notamment du 3° de l'Art. 56 du Nouveau Code des marchés publics qui consacre à son tour la valeur juridique des procédures de passation des marchés dématérialisées.
[45] Pris en application des I° et 2° du même Art. 56 du Code des marchés publics.
[46] Les conditions sont liées à l'authentification du signataire et à l'intégrité des documents pour présumer de la fiabilité du dispositif de signature qui implique la mise en œuvre de moyens techniques et organisationnels pour répondre à ces conditions.
[47] Pris en application du 3° de l'Art. 56 du Code des marchés publics.
[48] Faisant suite à la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000, notamment l'Art. 9, et à la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), elle-même modifiée par la loi n° 2004-669 du 9 juillet 2004, en particulier l'Art. 26 et l'Art. 25-I qui complète l'Art. 1108 du Code civil, qui permet de conserver l'écrit sous forme électronique, dans les conditions introduite par la loi du 13 mars 2000 en termes d'identification de la personne dont émane et de conservation dans les conditions qui en garantissent l'intégrité, lorsqu'il est exigé pour la validité d'un acte juridique.

Aux termes de l'Art. 1317 du Code civil, **l'acte authentique** est celui qui a été reçu par des officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises. Il peut être dressé **sur support électronique s'il est établi et conservé** dans des conditions fixées par décret en Conseil d'Etat. Un décret fixant les conditions générales applicables aux actes électroniques, complété par des décrets particuliers, étaient attendus depuis 2003. Ce sont en fait deux décrets sectoriels consécutifs, l'un concernant les huissiers de justice et l'autre, les notaires qui ont été publiés au JO du 11 août 2005 en vue de la réalisation d'actes authentiques.

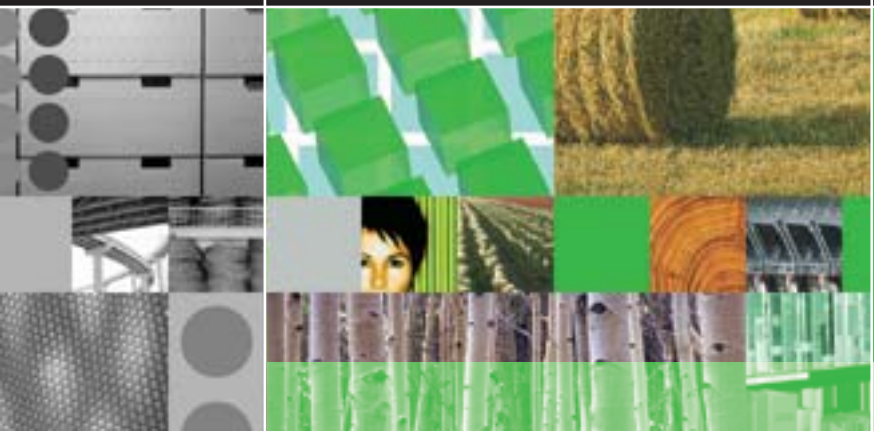
Le décret n° 2005-972 du 10 août 2005[49], **relatif aux actes des huissiers de justice,** prévoit dans son Art. 29 que : "*l'acte établi sur support électronique doit être* ***conservé dans des conditions de nature à en préserver l'intégrité et la lisibilité***", et aussi que "*celui qui délivre une expédition sur support électronique y mentionne la date et y appose* ***sa signature électronique sécurisée***". Le second décret n° 2005-973 du 10 août 2005, **relatif aux actes des notaires,** prévoit notamment les exigences des actes établis sur support électronique[50] (Ch. III). L'Art. 17 indique que : "*l'acte doit être signé par le notaire au moyen d'un procédé de* ***signature électronique sécurisée***", et que : "*pour leur signature,* ***les parties et les témoins*** *doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de* ***l'image de leur signature manuscrite***".

Ces décrets répondent aux questions sur la formalisation d'un acte électronique authentique et sur la lisibilité externe de la signature. En outre, les systèmes informatiques utilisés devront être agréés par les instances nationales concernées et être interopérables. **Il reste à prendre en compte l'ensemble du cycle de vie des actes :** établissement, utilisation, *-dont la mise en circulation, la mise à jour, les émargements-*, **et particulièrement l'archivage, pour la conservation** à plus ou moins long terme.

Traitement de l'obsolescence technologique

Avec le nombre, la volumétrie et les flux d'informations, **la variété des ressources numériques et l'obsolescence technologique** qui les affecte introduisent une grande complexité de gestion. Cette obsolescence est différente selon qu'il s'agisse du support, du matériel ou du logiciel nécessaire à son traitement, ou encore du contenu lui-même, en fonction du délai de rétention attendu pour la conservation pour une éventuelle présentation. Il est notamment observé que les standards de copie sur différents supports : *bandes, disques, etc.*, ont parfois un **cycle de vie plus court que ce délai** et que les versions des logiciels ne sont directement compatibles qu'avec la version utilisée lors de la création du document d'origine ou celle juste après. Ceci nécessite une veille constante en prévision de maintenir ou d'émuler successivement divers environnements ou encore d'effectuer une migration partielle ou totale des contenus à préserver.

[49] Modifiant le décret n° 56-222 du 29 février 1956, pris en application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice.
[50] Modifiant le décret n° 71-941 du 26 novembre 1971, et possibilité prévue dans la loi n° 2000-230 du 13 mars 2000.
[51] Conformément aux exigences du décret n° 2001-272 du 30 mars 2001, en application de l'Art. 1316-4 du Code civil.
[52] Selon la norme sécuritaire ISO 15489.
[53] Pour Open Archive Information System, spécifié dans la norme ISO 14721:2003. Le modèle OAIS ainsi décrit peut être applicable toute archive et précisément pour les organisations qui ont des responsabilités d'archivage à long terme. Il est également possible d'utiliser des structures XML pour encapsuler les métadonnées de préservation dans les objets lors de leur soumission à l'archivage.



Le défi est de pouvoir gérer efficacement les informations, depuis l'acquisition jusqu'à l'utilisation sur une période plus ou moins longue, en prenant en compte cette obsolescence technologique au vu du contenu. **La préservation invite à archiver un ensemble d'informations sous forme de "*métadonnées*"**[52] qui sont définies comme : "*des données* ***décrivant le contexte, le contenu et la structure des documents ainsi que leur gestion dans le temps***". Celles-ci sont descriptives, pour l'identification, administratives, pour la gestion d'une ressource, ou structurelles, pour lier les composants d'une ressource. **Le modèle d'information de référence est l'OAIS**[53]. Il fournit un cadre pour la création des **métadonnées de préservation**. L'information contenue et ces dernières, complémentaires à la pérennisation, seront **essentielles pour la préservation à long terme**.

EN RÉSUMÉ

Les enjeux se situent au niveau de la capacité à offrir des services d'archivage électronique légal fiable. Les fondements relèvent de la loi reconnaissant la même force probante à l'écrit sur support électronique que celui reconnus au support papier, mais aussi de modalités de conservation et du système probatoire. En complément des dispositions légales expressément applicables à l'archivage il est prudent de recourir à des mécanismes contractuels de conventions de preuve. Il y a lieu de considérer le cas des copies d'originaux et des actes authentiques électroniques et les critères qui relèvent de l'intégrité du contenu et des données afférentes, de la durabilité et de l'accessibilité et du traitement de l'obsolescence technologique par le recours à des normes qui figurent l'état de l'art, en s'appuyant en particulier sur un modèle de référence.

PRINCIPE DE PRECAUTION

Fondements historiques

Autrefois, l'homme se contentait de calmer son angoisse par des offrandes et des prières aux divinités. Après qu'une distance décisive avait été prise dès 1637 par Descartes, avec son "*Discours de la méthode*" qui constituait un ensemble de processus de découverte, du simple au compliqué, fondé sur une logique déductive, **la responsabilité de l'homme** intervient en 1756 avec Rousseau et sa méthode hypothético-déductive. **L'approche analytique** jetait désormais **les bases du *"lien de causalité"* sur lequel repose notre droit.** L'affirmation : "*ne recevoir jamais aucune chose pour vraie qui ne soit connue évidemment pour telle*" ne saurait être définitive, au risque de restreindre l'évidence aux connaissances du moment et de se soustraire au **principe de précaution**[54].

Fondements juridiques

Le principe de précaution naît de la Loi n° 95-101 du 2 février 1995 relative à l'environnement, ainsi énoncée : "L'absence de certitudes, compte tenu des connaissances scientifiques et techniques du moment, ne doit pas retarder l'adoption de mesures effectives et proportionnées...". En droit communautaire, il relève notamment de l'Art. 130 du Traité sur l'Union Européenne de 1993 qui cherche à équilibrer les communautés d'intérêts ; l'Art. 95, Par. 3, précisant à son tour que : "les mesures prises à cet effet doivent être basées sur une évaluation des risques tenant compte de tous les facteurs de risque pertinents, ainsi que les aspects technologiques, des meilleures preuves scientifiques disponibles...".

[54] Guinier D. (2001) : Justifications du principe de précaution Application aux antennes radio-téléphoniques. *Expertises des systèmes d'information*, n° 250, pp. 263-267.

Transposition à l'archivage

Les projets d'archivage s'imposent du fait d'obligations, avec comme motivation première la conservation des preuves alors que la sécurité juridique est en cause du fait que les établissements, publics ou privés, ne maîtrisent pas totalement le cadre juridique et manquent d'indications et de retours d'expériences. De plus, la neutralité technologique accordée par le droit peut entraîner des ambiguïtés et des implémentations hasardeuses qui peuvent constituer autant de sources de conflits. **La transposition des fondements du principe de précaution est donc attendue du fait de telles incertitudes** juridiques, avec les modalités d'application, mais aussi techniques.

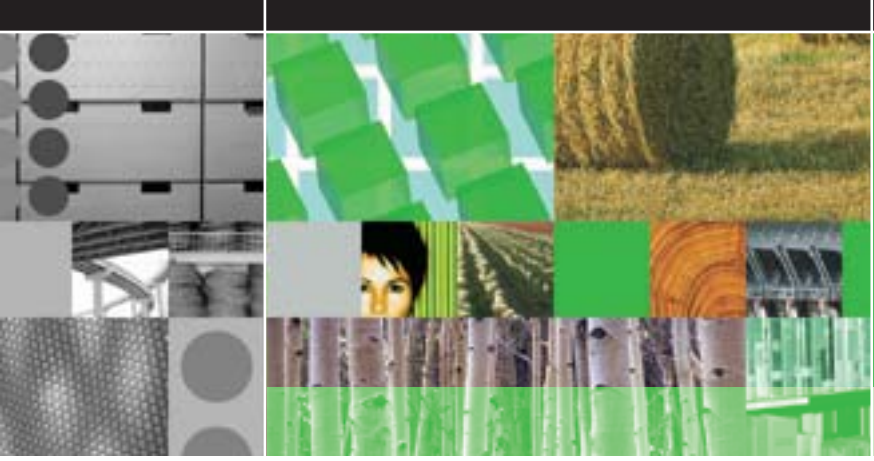
L'application du principe de précaution concerne notamment l'**évaluation globale des risques** dans leur dynamique[55]. Il s'agit d'en réduire les effets par un **dispositif robuste,** à court comme à long terme, **en conscience de la portée des décisions prises** et non prises, et conformément à la **destination de l'archivage et de sa valeur probante**. Ceci permettrait de maintenir un niveau acceptable, en anticipant à plus long terme, avec une éventuelle prise en charge des risques résiduels par l'assurance, dans un souci de juste équilibrage pour les parties concernées.

Illustration du fait de migrations inéluctables

Si le dépositaire ou une des parties ne dispose pas de l'original du document, une copie, dont la **reproduction est fidèle et durable**, présente la **même force probante** que l'original[56]. Il reste néanmoins **au juge d'apprécier et de retenir le caractère "*fidèle et durable*"**. En conséquence, il appartient d'**évaluer le risque avant de procéder à l'effacement d'originaux** ou à la destruction d'objets liés à leur conservation ou à leur restitution, en fonction des réglementations particulières. **L'application du principe de précaution** nécessite aussi d'établir une procédure de conversion de l'écrit papier en électronique, ou de migration selon le cas, **conforme à l'état de l'art**, et à **mettre en place des conventions** aménageant le régime de preuve en fonction de l'objectif recherché et de la territorialité des parties. Une illustration est donnée au travers d'un exemple lié à un contrat et aux diverses migrations attendues.

L'Art. 1369-1 du Code civil, créé par l'Art. 25 de la LCEN, prévoit l'obligation pour le vendeur, de mentionner dans ses conditions générales de vente : "*En cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre et les conditions d'accès au contrat archivé*". **L'archivage est imposé**[57] **avec l'obligation à la charge du professionnel de conserver tout contrat conclu par voie électronique** d'un montant de plus de 120 **?** pendant une durée de dix ans à compter de sa conclusion ou de son exécution, avec garantie l'accès à ce document pour le contractant à sa demande et à tout moment. Relativement à la commercialisation à distance de produits financiers auprès des consommateurs, il est prévu[58] que : "*le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition et auquel il a accès en temps utile et avant tout engagement, les conditions contractuelles...*". **Cette obligation implique :**

- la **conservation des conditions contractuelles et des informations indiquées** à l'Art. L. 121-20-10 du Code de la Consommation,
- de **disposer d'un support de stockage durable** pour ces informations et le courrier électronique : *CD, DVD, disque, etc.*
- de **conserver les informations relatives au certificat électronique** et autres utiles pour faire la preuve en justice de cette certification.



La durée de conservation par le serveur d'archives étant longue, le prestataire devra **prévoir des opérations de migration techniques pour assurer la pérennité et la lisibilité** des documents et autres données archivées, conformément aux possibilités offertes[59]. Ces migrations pourront s'effectuer :

- **en conservant intégralement le format du document,** en préservant la chaîne binaire, *en cas de basculement vers un autre environnement technique*,
- **en transformant le format du document tout en gardant le contenu**, *en cas d'obsolescence technologique ou par sûreté de fonctionnement,*

alors que **le nouveau support peut avoir des caractéristiques identiques ou différentes**, selon le cas. Il faut observer que **les migrations sont inéluctables à plus ou moins long terme**.
L'archivage relève alors du risque juridique lié à la qualité d'original d'écrits ayant subi des transformations, lesquelles sont cependant indispensables pour pallier les difficultés d'évolution et de durée.

La problématique à prendre en compte concerne la préservation d'intégrité de l'information utile, le transfert de la qualité "d'original" à la copie après migration, la destruction éventuelle du document d'origine, et les signatures électroniques et les certificats, et plus généralement les données de preuve associées, alors qu'il appartient au juge d'apprécier et de retenir le caractère "*fidèle et durable*" de la copie et de la préservation de l'intégrité de l'information du document.

Les décrets n° 2005-972 et 2006-973 du 10 août 2005 portant sur les actes authentiques établis sous forme électronique, par les huissiers de justice et les notaires, y répondent en partie, mais l'extension de leurs effets à des écrits sous seing privés n'est pas généralisable à ce jour.

EN RÉSUMÉ

En application du principe de précaution, il est suggéré de recourir à l'évaluation du risque qui conjugue la possibilité de réalisation d'un évènement redouté et la gravité au vu des conséquences en cas d'occurrence de celui-ci. Il s'agira de prendre des mesures proportionnées pour le limiter et mettre en place des conventions pour l'aménagement du régime de la preuve, dans l'intérêt des parties et, si nécessaire, contracter une assurance du risque résiduel. Il conviendra aussi de s'appuyer sur un référentiel normatif qui représente l'état de l'art du domaine, pour éventuellement s'en prévaloir en justice, au vu de la jurisprudence et lors de l'expertise qui pourrait être demandée au motif de la complexité, et notamment en l'absence d'original et du fait de migrations inéluctables.

[55] Guinier (1994) : Oriented-scenario dynamics in information systems safety, Introduction to propagation paths, channels of risk and "*revulsion momentum*", ACM SIGSAC REVIEW, Vol.12, n° 3, pp. 6-11.
[56] Cour de Cassation, 3ème Ch. Civile, du 4 février 1976 et en vertu de l'Art. 1348 al. 2 du Code civil.
[57] Par l'Art. 34-2 du Code de la consommation, complété par le Décret n° 2005-137 du 16 février 2005 pris pour l'application de l'Art. L. 134-2 du Code de la consommation.
[58] Par l'Art. L. 121-20-11 au Code de la consommation, créé par l'ordonnance n° 2005-648 du 6 juin 2005.

NORMES RELATIVES A L'ARCHIVAGE

Il faut déjà distinguer **les normes de droit** des standards de fait[60]. Les normes de droit sont celles avalisées par un organisme de normalisation : *ISO, ANSI, AFNOR, etc.,* suite à un développement sur une longue période et approbation par tous les membres du comité du domaine d'application, lesquels sont généralement des professionnels su secteur : concepteurs de technologie *et experts en spécifications.* **Celles relatives à l'archivage électronique sont essentielles.** Elles constituent un **référentiel couvrant un ensemble d'exigences complémentaires** pour l'archivage légal. Elles ont cependant une **portée limitée car elles n'ont pas force de loi.**

La norme ISO internationale 15489

La norme ISO 15489 relève des politiques et procédures de gestion documentaire de façon à garantir que tous les documents enregistrés dans un système de **conservation** bénéficient d'une attention appropriée. Elle vise la **gestion des documents et preuves électroniques** sous "Records management"[61]. Le rapport technique[62] qui l'accompagne traite des questions de gouvernance, de stratégie d'implantation, du contrôle, etc. Ainsi :

- **l'archivage est considéré comme un processus de gestion,** et les documents considérés dans leur **dimension de preuve,**
- les principes et procédures rendent compte de l'**environnement réglementaire** et des **conventions du domaine d'activité** de l'organisme.

Elle précise qu'un système d'archivage fiable doit intégrer automatiquement **toutes les archives relevant du champ d'activité de l'organisme,** et en outre, que le document doit contenir les **métadonnées nécessaires pour documenter une action.**

La norme ISO internationale 14721

La norme ISO 14721 représente l'état de l'art en matière de **métadonnées de préservation.** Il constitue un guide qui définit des responsabilités et spécifie le **modèle de référence OAIS pour un système d'archivage ouvert.** Celui-ci comporte un **ensemble de fonctions en vue de la préservation du contenu** à court comme à long terme, concernant le stockage, la gestion, l'accès et la distribution, etc., et de **la migration** sous de nouvelles formes et sur de nouveaux supports. Il décrit aussi les **échanges entres archives et les interfaces.**

La norme internationale ISO 15408

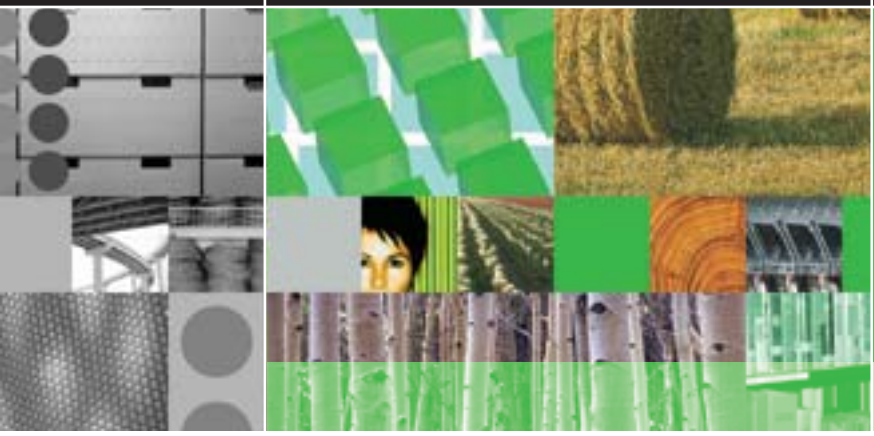
La norme ISO 15408 constitue un guide structuré qui repose sur un **catalogue formel de critères de fonctionnalités et d'assurance de la sécurité** d'un système d'information et sur un profil de protection rationnel et argumenté. Il permet d'estimer le **niveau de confiance que l'on peut avoir** dans tout ou partie d'un système d'archivage concernant les différents composants et acteurs, **tout au long de son cycle de vie** et en rapport aux données archivées. Sa finalité est liée à l'évaluation et à la certification d'un tel système[64].

[61] La norme indique "Records Management" (RM). "Records" pouvant être traduit par "enregistrement", selon la norme ISO 9000, mais apparaissant ici dans un sens de "Gestion des Documents et Preuves électroniques".

[62] 5 sections examinent : les politiques et les responsabilités, la stratégie de conception et d'implantation, les procédés et les contrôles, la surveillance et l'audit au vu de vérifications de conformité, de démonstration de la valeur probante des documents conservés et d'amélioration de performance organisationnelle, et enfin les besoins en formation.

[63] Pour Open Archival Information System.

[64] Il faudrait aussi citer la norme ISO 17799 qui constitue un code de bonnes pratiques pour la sécurité de l'information.



La norme française NF Z 42-013

La norme française NF Z 42-013 comporte un ensemble de spécifications pour l'enregistrement, le stockage et la restitution de documents électroniques, afin d'assurer la **conservation** et l'**intégrité** de ceux-ci. Elle s'applique exclusivement aux équipements et supports **non réinscriptibles assurant un stockage permanent** des documents électroniques[65]. Elle vise donc essentiellement les systèmes de gestion électronique de documents (GED), plutôt que l'archivage légal, et ne prend pas en compte l'obligation d'effacement des données personnelles en fin de durée, de façon sélective.

Autres normes et standards de fait

En dehors de ces normes essentielles, il y a lieu de noter l'existence d'autres normes et standards connexes[66], notamment pour les supports et les formats d'archivage. Ils sont à considérer, même s'i pour certains ils relèvent de points qui s'écartent du sujet traité. De plus, le suivi de l'ensemble de ces normes s'impose, compte tenu de leur évolution et des délais de conservation.

EN RÉSUMÉ

Les normes internationales : *ISO 15489, ISO 14721, ISO 15408,* et française : *NF Z 42-013,* sont essentielles. Elles couvrent un ensemble d'exigences utiles pour l'archivage électronique légal. Elles ont cependant une portée limitée réservée à l'état de l'art, mais n'ont pas force de loi.

DEMARCHE POUR LA DETERMINATION DE LA SOLUTION ET RECOMMANDATIONS

Une démarche méthodique et pratique s'impose sur une base rationnelle qui prend en compte le contexte environnemental et interne, mais aussi la stratégie de l'entreprise. Elle requiert une étape de sensibilisation avant le démarrage, et se déroulera par phase d'activité validée par l'équipe de projet et la direction. La dernière phase **traduit le besoin de suivi et assure la pérennité de la solution.** Le tableau suivant présente **les tâches essentielles en fonction des activités** de chaque phase.

[65] En particulier aux disques optiques WORM *(Write Once Read Many)*.

[66] Du ressort plus général de la qualité, du stockage, de la gestion électronique des documents *(GED)*, et de la gestion électronique des contenus *(GEC ou ECM, pour Enterprise Content Management)*. En voici une liste non exhaustive :
Norme ISO 8879, concernant les systèmes bureautiques, le langage normalisé de balisage généralisé,
Norme ISO 9001, concernant le système de management de la qualité,
Norme ISO 9660, concernant la structure relative au support CD-ROM pour les échanges d'information,
Norme ISO 12083, concernant la préparation et le balisage de manuscrits électroniques,
Norme ISO 12652, concernant la préparation de documents existants pour les systèmes de capture d'image,
Norme ISO 13346, concernant le format de gestion des volumes et des fichiers sur support amovibles : CD, DVD, etc.
Norme ISO 15445, concernant les langages de description et le traitement de documents,
Norme ISO 15801, concernant le stockage et les recommandations pour les informations de valeur et leur fiabi¬lité,
Norme ISO 16111, concernant les conditions environnementales de préservation des collections numériques,
Norme ISO 17799, concernant les bonnes pratiques pour la sécurité de l'information,
Norme ISO 18492, concernant la conservation à long terme de documents électroniques,
Norme ISO 19005-1, concernant l'utilisation du format PDF pour l'archivage (PDF/A-1),
Norme ISO 23950, concernant la recherche d'information, en particulier, la définition du service de l'application et spécification du protocole – avec norme ANSI/NISO Z39.50,
Norme NF Z 43-400, concernant la micrographie informatique en noir et blanc. Le procédé implique l'irréversibilité de l'enregistrement et la qualité résultante des microformes : *conservation, fiabilité, non-obsolescence*, etc. La norme s'applique aux données scripturales ou graphiques en 2D, établies, transformées ou reçues sous forme électronique ; elle a été homologuée le 20 août 2005.

Activités et tâches essentielles

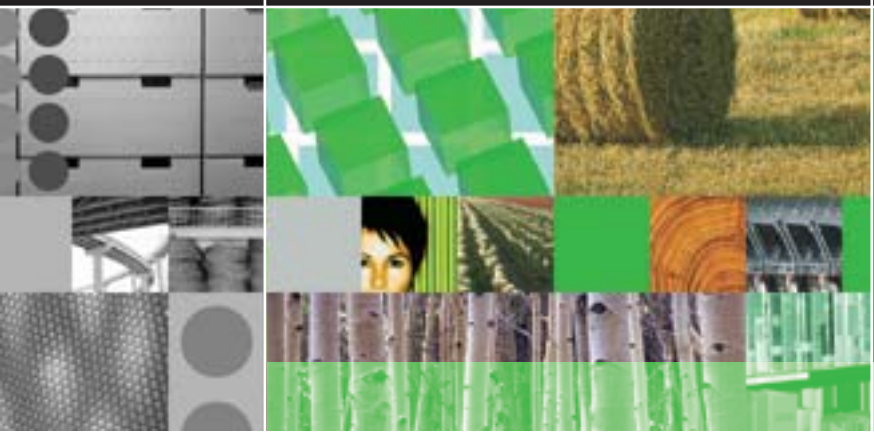
Les activités et tâches essentielles sont les suivantes par phase, après celle d'initiation du projet :

PHASE	ACTIVITÉS	TÂCHES ESSENTIELLES
	Initiation	• *Séminaire de sensibilisation* • *Démarrage du projet : périmètre, équipe, jalons, communication, etc.*
Phase 1	Analyse de l'existant	• Etablissement du référentiel de l'entreprise : *obligations, normes, contraintes, etc.* • Etude des enjeux et de l'impact au vu de la messagerie et de l'archivage • Typologie, classification, flux et volumétrie des messages et données relatives • Audit et diagnostic de la messagerie et de son archivage actuels
Phase 2	Expression des besoins	• Politique : *archivage de la messagerie et sécurité,* et règles qui en découlent • Sélection des éléments normatifs et des métadonnées • Détermination des besoins techniques et organisationnels • Réalisation d'un modèle répondant aux besoins
Phase 3	Choix rationnel	• Rédaction d'un cahier des charges résultant des phases précédentes • Recherche et sélection d'une solution technique automatique pérenne • Bilan des offres sur la base de critères objectifs préalablement pondérés • Présentation et validation du choix
Phase 4	Mise en exploitation	• Intégration de la solution technique au système d'information • Procédures et mesures à mettre en œuvre : *normales et d'exception* • Organisation interne, rôles et responsabilités, formation et documentation • Tests et exploitation après qualification du système
Phase 5	Suivi et maintenance	• Dispositions de veille, de contrôle et d'audit • Dispositions de qualification : *correction, modification, mise à jour, etc.* • Dispositions de migration : *obsolescence, événement, saut technologique, etc.* • Dispositions d'élimination : *fin du délai de conservation, événement, etc.*

Points clés de la réussite

La démarche doit s'inscrire dans le cadre d'un véritable projet d'entreprise avec une **approche pluridisciplinaire** pour traiter des différents aspects. En complément, **dix recommandations** paraissent essentielles :

1 **Une politique de gestion de la messagerie et de son archivage doit être définie** par la direction de l'entreprise, laquelle en assume la responsabilité suprême
2 **Les enregistrements contenant des données à caractère personnel** relèvent de la responsabilité de la direction et du correspondant "informatique et libertés"[69].
3 **La politique suit les objectifs découlant des obligations** légales et réglementaires et de la gouvernance de l'entreprise, avant les impératifs informatiques ou autres
4 **La politique s'appuie** sur une infrastructure informatique en réseau conforme et efficace et sur solution technique prenant en charge la messagerie et son archivage de façon automatique et transparente pour les utilisateurs
5 **Les décisions de conservation ou de suppression** doivent être prises au niveau de la politique, selon les règles centralisées qui en découlent, et non laissées aux utilisateurs, sauf pour les messages réputés personnels
6 **Les règles prennent en compte** les messages émis et reçus, internes et externes, et ceux réputés personnels, les pièces attachées et les données à caractère personnel
7 **Les enregistrements à caractère personnel** seront supprimés au terme de la période de conservation prévue au titre de la déclaration à la CNIL[70].
8 **Les utilisateurs auront une connaissance de ces règles,** formalisée après formation
9 **L'application des règles** sera auditée et les résultats rapportés à la direction et, le cas échéant, aux organismes externes, selon la réglementation et le cas.
10 **Des corrections** seront éventuellement apportées et suivies pour la conformité, avec les actions qui s'imposent aux écarts et aux évolutions technologiques et réglementaires.



22

Il reste aussi à insister sur la nécessité de distinguer et de poursuivre les sauvegardes journalières, hebdomadaires, mensuelles et annuelles, qui ont d'autres vocations que les archives légales ou de conservation. En effet, les sauvegardes s'attachent à l'ensemble du système d'information, et sont dites "de production", en cas d'incident opérationnel et "de recours", en cas de sinistre.

En cas d'externalisation, le dispositif contractuel devrait prévoir des clauses spécifiques visant à limiter la propagation des effets de l'interruption du service. Ceci apparaît comme un **moyen de prévention** apte à distinguer les obligations et les responsabilités de chacun, en temps normal, mais aussi en cas de dysfonctionnement et de sinistre, en plus des **moyens de protection** : plan de reprise d'activité (PRA), plan de sauvegarde, etc., dans le respect des normes et règlements.

Recommandations de la CNIL en la matière

Face à la rémanence de la mémoire électronique, le droit à l'oubli est en mesure de garantir que les données collectées sur les personnes ne seront pas conservées pour des **durées qui pourraient apparaître comme manifestement excessives,** au vu des enjeux de la protection de la vie privée et de ses enjeux. Pour ce motif, la délibération n° 2005-213 du 11 octobre 2005[71] de la CNIL a adopté une **recommandation sur les modalités d'archivage électronique de données à caractère personnel, dans le secteur privé,** après avoir précisé avant cela, dans sa délibération n° 88-052 du 10 mai 1988[72] les modalités relatives à l'archivage public, pour les administrations et organismes du **secteur public**. Ainsi, **les archives courantes et intermédiaires** doivent répondre à des **durées de conservation spécifiques, proportionnées à la finalité poursuivie, qui doivent être précisées** dans le cadre des dossiers de formalités de déclarations préalables adressés à la CNIL. Il est indiqué au responsable des traitements :

- d'établir des **procédures aptes à gérer des durées de conservation distinctes selon les catégories de données** et, le cas échéant, de **permettre toute purge ou destruction sélective** de données,
- de mettre en œuvre les **mesures techniques et organisationnelles** pour assurer un **niveau de sécurité approprié** au regard des risques présentés par le traitement et de la nature des données à protéger.

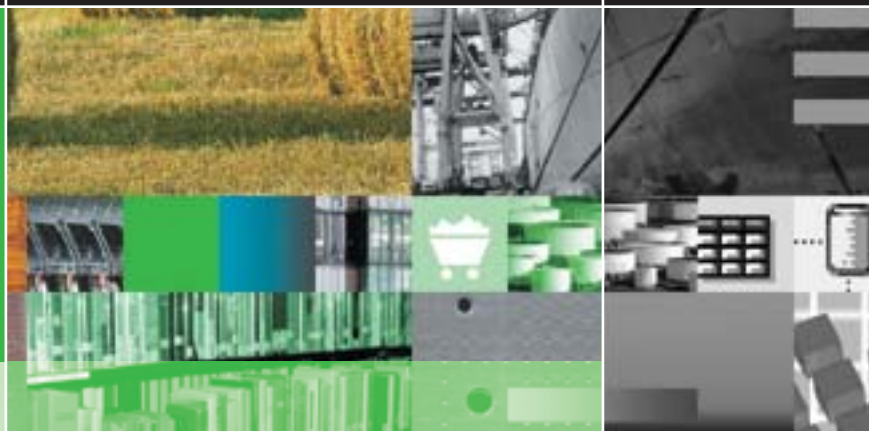
[70] La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit notamment la désignation d'un correspondant informatique et libertés, laquelle doit être notifiée à la CNIL et portée à la connaissance des instances du personnel. Dans un tel cas *"les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux Arts. 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé"*. Le correspondant est *"une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la CNIL des difficultés qu'il rencontre dans l'exercice de ses missions"*.

[71] Vu la loi n° 78-17 du 6 janvier 1978, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

[72] Au vu de la compatibilité entre la loi n° 78-17 du 6 janvier 1978 et la loi n° 79-18 du 3 janvier 1979 sur les archives.

[73] Au sens de l'Art. 8 de la loi *"Informatique et Libertés"* modifiée, qui énumère la liste des données dont la collecte et le traitement sont en principe interdits. Par dérogation, certains traitements sont possibles dans la mesure où la finalité du traitement l'exige et moyennant le strict respect de certaines conditions qui sont spécifiées.

[74] Au-delà de 50 personnes en charge de la mise en oeuvre ou ayant directement accès aux traitements pour lesquels le responsable entend désigner un CDP, seul peut être désigné un correspondant exclusivement attaché au service de la personne, de l'autorité publique ou de l'organisme, ou appartenant au service, qui met en œuvre ces traitements, ce qui exclut un CDP externe.



Il est rappelé les sanctions encourues au vu du Code pénal en cas de non-respect. Il est aussi indiqué que **de telles garanties sont aussi à respecter en cas de sous-traitance.** Choisie pour apporter des garanties suffisantes, cette dernière fera l'objet d'un acte ayant une valeur juridique qui *"lie le sous-traitant au responsable de traitement et prévoit notamment que le* ***sous-traitant n'agit que sur la seule instruction du responsable de traitement*** *et que* ***les obligations en matière de sécurité*** *incombent également à celui-ci".*

Outre les mesures de sécurité recommandées, l'accès aux **archives intermédiaires,** *-attachées à des durées de conservation fixées par les règles de prescription-,* devra être limité, et il sera procédé au moins à l'isolement des données archivées par la gestion des droits d'accès et des habilitations. Les **archives définitives,** *-ne devant faire l'objet de destruction par définition-*, devront être conservées sur un support indépendant, non accessible par les systèmes de production et n'autorisant qu'un accès distinct, ponctuel et motivé auprès d'un service habilité à la consultation. **Pour les données sensibles**[73], **il est recommandé le recours à l'anonymisation.** D'une façon plus générale, la CNIL recommande, dans le cadre de procédures formalisées, **la définition de règles d'archivage répondant à ses préconisations** et qu'une information puisse être fournie sur ces règles, en cas de demande exprimée de leur part, aux personnes faisant l'objet des traitements archivés.

Le Décret n° 2005-1309 du 20 octobre 2005 précise le **dispositif relatif au correspondant à la protection des données à caractère personnel** (CDP) : *qualifications, tâches, subordination et indépendance, etc.,* **en excluant le responsable des traitements et le représentant légal de cette fonction. Il est prévu qu'un CDP externe ne puisse être désigné** au-delà de cinquante personnes chargées ou ayant directement accès à ces traitements[74].

EN RÉSUMÉ

La démarche méthodique et pratique proposée permet de décliner les principes adoptés pour une solution d'archivage automatique répondant aux attentes. En outre, la traduction des activités sous forme de tâches, et les recommandations essentielles, devraient permettre l'assurance de suivi et de pérennité de la solution matérielle qui sera choisie. Les recommandations de la CNIL sont à examiner avec attention, y compris en cas de sous-traitance, et pour la désignation du correspondant à la protection des données à caractère personnel (CDP).

PRINCIPES D'UNE SOLUTION D'ARCHIVAGE REPONDANT AUX ATTENTES

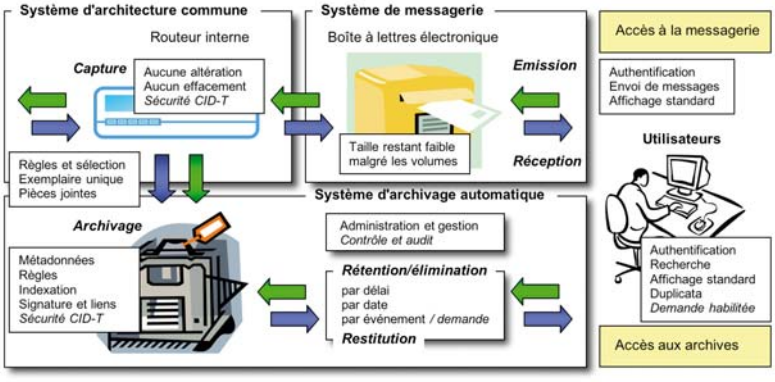
La solution pressentie permettra l'archivage automatique des messages et des documents de façon transparente pour l'utilisateur. Elle s'articulera autour de trois systèmes, deux préexistants concernant l'architecture en réseau et la messagerie, et un nouveau constituant le **système d'archivage** proprement dit. L'utilisateur ayant maintenant **accès à la messagerie et aux archives,** dans les conditions prévues et contrôlées.

La capture des messages entrants et sortants se fera au niveau du routeur et non de la boîte à lettres pour préserver d'intégrité en vue de l'archivage légal au niveau de l'architecture commune en réseau. Le système de messagerie continuera à opérer comme auparavant, en émission comme en réception, mais sans avoir à recourir à des actions arbitraires au vu de la taille des boîtes aux lettres.

La figure présente les fonctionnalités attendues au niveau des différents composants avec la sécurité

CID-T[75]. Le système d'archivage sera géré et administré, mais aussi contrôlé et audité, en référence aux obligations légales et autres traduites préalablement dans les politiques d'archivage et de sécurité interne du système d'information (PSSI). Une attention particulière sera portée à la rétention, à la restitution et à l'élimination, déclenchées par délai, par date ou par événement ou sur demande, au vu des règles et métadonnées, et du contrôle d'accès et de signature. L'archivage des messages, des documents et de leur signature de fera en un seul exemplaire, selon les règles de sélection établies.

Le statut des messages "personnels" sera établi préalablement dans la politique, afin de les archiver ou non. Les données archivées seront conservées selon les nécessités et éliminées en fin de vie. Elles pourront être consultées après restitution, conformément aux règles et contrôles formels, en toute transparence pour l'utilisateur et avec une facilité d'accès du fait de l'indexation, répondant ainsi aux contraintes et aux attentes des utilisateurs, des informaticiens et de l'entreprise.



CE QU'IL NE FAUT PAS FAIRE

Les mauvais exemples présentent les dénominateurs usuels suivants :

- la solution est qualifiée de "rapide" ou de "minimum",
- la solution ne dispose pas de moyens de contrôle sur les opérations,
- la solution ne prend pas en compte l'obsolescence technologique,
- l'archivage repose sur une organisation informelle des dossiers informatiques,
- l'archivage est soumis à l'arbitraire de l'utilisateur et non aux règles de l'entreprise,
- l'archivage n'est pas associé à l'application de règles de gestion,

Lorsque l'utilisateur décide de la conservation ou non du message ou du document, à moyen ou long terme, selon un jugement subjectif ou de sa seule volonté, ceci ne manquera pas de se traduire par des déviances, alors que de surcroît la capture qui se fait au niveau de la boîte à lettres entraîne une incertitude sur la préservation de l'intégrité des données. Dans l'ensemble, **ces caractéristiques ne garantissent pas le respect des règles** et ne répondent ni aux besoins réglementaires, ni au contexte de l'entreprise. En conséquence, **une telle solution serait hasardeuse**[76], d'une complexité croissante, peu pérenne et non conforme aux attentes, alors qu'elle est d'apparence simple au départ.

L'ARCHIVAGE ELECTRONIQUE SUR LA SELLETTE

Les systèmes de gestion de documents et le courrier électronique au cœur des jugements.

Si elles devaient être adoptées par le Congrès, deux propositions d'amendements aux règles de procédure civile **visant des éléments de preuve électronique,** feraient encourir un risque majeur aux entreprises des Etats-Unis. Pour la première fois, **les tribunaux seraient amenés à impliquer directement les systèmes d'information des entreprises au cœur des litiges.**

Les amendements proposés à la **règle 26** précisent que les avocats des parties d'un litige introduit devant la Cour fédérale **devront présenter le système de gestion de documents** de leur client préalablement aux débats, et que chaque entreprise devra **désigner un porte-parole relevant du SI.** Il est parallèlement attendu un changement de la règle 37(f), *-connue sous le nom de "Safe harbor"-*, qui stipulait que les entreprises ayant perdu des informations mais qui, par ailleurs, ont agi en toute bonne foi, ne pouvaient être sanctionnées pour cela. L'élimination de cette condition pourrait être en mesure d'engendrer un véritable *"désastre légal".*

En observant les **conséquences d'une mauvaise gestion des documents électroniques** illustrée par deux **précédents judiciaires homologues,** il est plus facile de **comprendre la portée de tels changements** aux règles 26 et 37(f), du fait générateur qu'**aucune des sociétés condamnées n'était en mesure de fournir les informations demandées** et que **des préjudices** ont été considérés comme possibles :

- *dans l'affaire Laura Zubulake / UBS Warburg,* considérant les **manquements au vu des messages** et des **sauvegardes,** cette dernière a été condamnée à verser la somme de **20 millions de dollars** à la Laura Zubulake *(South District New York),*
- *dans l'affaire Ronald Perelman / Morgan Stanley,* considérant les **manquements au vu de la messagerie,** Morgan Stanley a été condamné à verser la somme totale de **1,45 milliard de dollars** à Ronald Perelman *(West Palm Beach, Floride),*

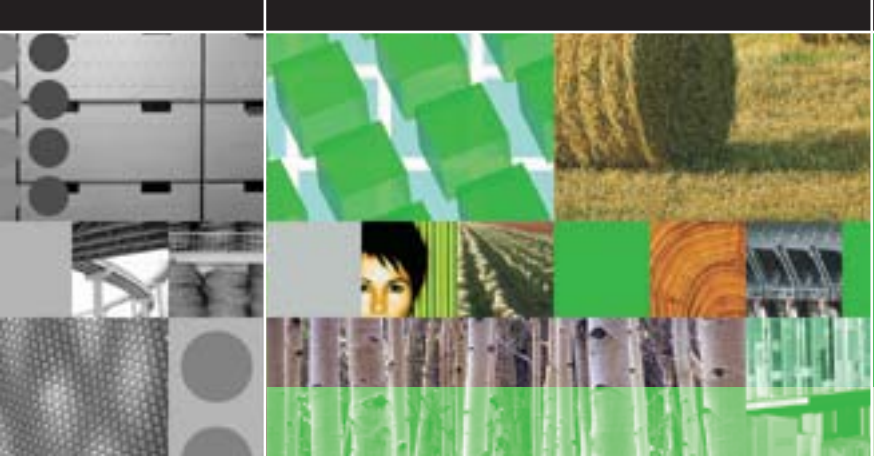
malgré les explications fournies sur les difficultés qu'il y avait à retrouver ces informations, et les efforts accomplis *a posteriori.*

Si les changements de la règle 26 et la suppression de la protection de la règle 37(f) sont adoptés par le Congrès, on peut donc s'attendre à des **conséquences gravissimes voire catastrophiques pour les entreprises qui n'auront pas pris les mesures nécessaires** fondées sur une politique définie et des plans adéquats. Ceci concerne **l'archivage,** *-de la* ***messagerie électronique*** *en particulier-,* les **sauvegardes,** la **continuité ou la reprise d'activité** et plus généralement, **la sécurité**[77].

[75] CID-T, pour Confidentialité, Intégrité, Disponibilité et impuTabilité, qui sont les propriétés essentielles de la sécurité.

[76] Rappelons que la non présentation de renseignements lors d'un contrôle fiscal, quel qu'en soit le motif : *évolution incompatible, destruction partielle du système d'information, dépassement de délais exigibles, etc.,* a pour conséquence d'entraîner une évaluation conduisant à des redressements importants ; ceci s'applique aussi aux documents sociaux.

[77] Citons la condamnation par la Commission fédérale américaine du commerce *(Federal Trade Commission (FTC))* en date du 27/01/06 de la société ChoicePoint, à une amende d'un montant total de **15 millions de dollars,** suite au "piratage" d'un serveur contenant des données personnelles de clients, et qui hébergeait des informations bancaires. Bien que d'autres sociétés ont aussi été victimes du même type d'intrusion : *Bank of America, Citigroup, Mariott, etc.,* ChoicePoint est pour l'instant la première a être condamnée **pour négligence en matière de sécurité** alors que c'est un point critique pour les consommateurs, comme l'a rappelé la commission, après avoir considéré qu'il s'agissait d'une violation du Fair Credit Reporting Act (FCRA).



CONCLUSION

Le respect des obligations pour la conservation électronique des informations est impérieux au vu des risques et des poursuites judiciaires et pour une bonne gouvernance. Il s'agit aussi de veiller au suivi de l'archivage avec des dispositions adéquates, conformément à l'état de l'art et donc aux normes en vigueur, **dans des conditions légales, réglementaires et économiques acceptables.**

Une solution d'archivage automatique et transparent répondant aux obligations légales et à la présentation des preuves s'impose. Elle s'accorde avec la gestion active et contrôlée de l'espace de stockage sur disque qui prend en compte la durée de vie du support et des données. **Il devrait en découler des bénéfices** qui concernent notamment la performance et la sécurité de la messagerie, l'accès aux messages et aux documents indexés, la conservation des seuls éléments nécessaires et suffisants. D'autres concernent la disparition des actions arbitraires.

La sensibilisation est un préalable utile aux décideurs, responsables et autres intéressés, pour **élargir le champ de vision** sur la messagerie et l'arbitrage légal. Les initiatives en cours ou à venir pourraient bénéficier d'un apport et d'une collaboration pluridisciplinaires, et ainsi constituer un **projet d'entreprise** prenant en compte divers aspects : *managériaux, juridiques, économiques, techniques et d'autres encore, en particulier d'ordre organisationnel.* Il y a tout lieu d'être attentif à l'implication des responsabilités, internes et externes, notamment en cas d'externalisation de certains services, directement ou indirectement liés à l'archivage, en prenant en compte les spécificités et règlements particuliers attachés au secteur et à l'entreprise elle-même.

Quelques références annexes

Archives de France
http://www.archivesdefrance.culture.gouv.fr/

Association des professionnels de la gestion électronique de documents
http://www.aproged.org/

Association française de normalisation
http://www.afnor.fr/

Club informatique des grandes entreprises françaises
http://www.cigref.fr/

Commission Nationale de l'Informatique et des Libertés (CNIL)
http://www.cnil.fr/

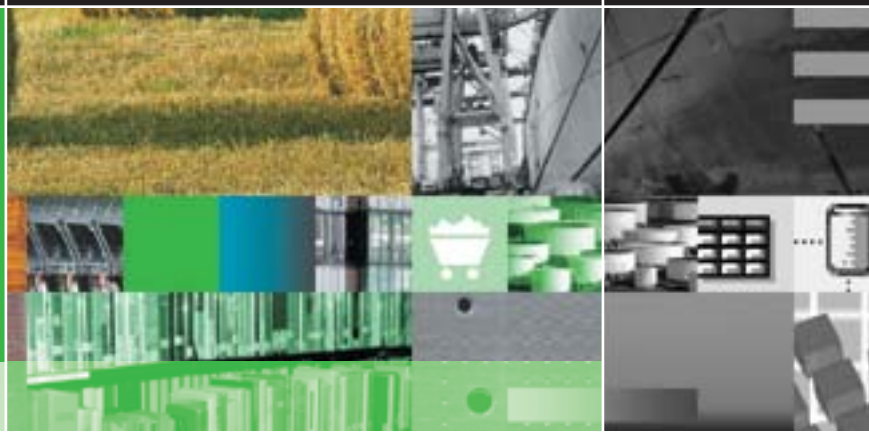
Conseil international des archives
http://www.ica.org/

Direction centrale de la sécurité des systèmes d'information (DCSSI)
http://www.ssi.gouv.fr/fr/dcssi/

Ministère de l'économie, des finances et de l'industrie
http://www.minefi.gouv.fr/

Organisation internationale de normalisation (ISO)
http://www.iso.org/iso/fr/

Poivre J. (2004) : L'archivage des documents bureautiques - Manuel pratique. La Documentation Française



Biographie

Daniel GUINIER, intervient comme conseil auprès d'établissements publics et privés de toute taille. Il est aussi expert judiciaire et expert ANVAR. Il participe à la révision des normes internationales sécuritaires et à l'évolution du droit, en particulier en matière de signature électronique et de preuve. Il est l'auteur de plus de 180 publications scientifiques et techniques, de deux livres édités par Masson et deux autres aux Editions d'Organisation en collaboration. Il participe à des conférences majeures : OAKLAND, MONTEREY, OTTAWA, ORLANDO, LONDRES, PARIS, etc. Il enseigne au niveau Master dans plusieurs universités, à Strasbourg, Compiègne, Paris XI. Après avoir été ingénieur de recherche au CNRS, et professeur au US Naval Postgraduate School, il dirige la société OSIA depuis 1990, où il poursuit des actions de veille et de R&D en méthodes et mécanismes de sécurité et d'audit en rapport avec les NTIC et les plans de reprise d'activité en cas de crise de divers secteurs.

Silicon Valley Laboratory Route 100555 Bailey AvenueSan Jose, CA 95141U.S.A.

POUR PLUS D'INFORMATIONS.
Pour en savoir plus sur l'archivage et la sécurité, rendez-vous : **ibm.com/software/fr/db2**

Compagnie IBM France
Tour Descartes - La Défense 5
2, avenue Gambetta
92066 – Paris La Défense Cedex
Tél. : 0810 011 810
ibm.com/fr

Ouvrages parus :

Auteur de :

1-Sécurité et qualité des systèmes d'information – Approche systémique (Masson)
1992 - 300 pages, préface de M.-F. de Kervénoaël, Présidente de l'IFACI

2-Catastophe et management – Plans d'urgence et continuité des SI (Masson)
1995 - 323 pages, préface de A. Marcilhacy, Ancien Président et Délégué général de l'IFACI, également ancien Directeur des systèmes de contrôle d'IBM France.

Co-auteur de :

3-Systèmes d'information - Art et pratiques – La vision globale (Pratiques et mise en œuvre, chap. 5)
2002 - 512 pages

4-Tableaux de bord pour diriger dans un contexte incertain (Mise en œuvre et sécurité, chap. 13)
2004 - 383 pages.

Coordonnées : OSIA
BP 86 - 67034 STRASBOURG
Cedex 2
Tél. 03 88 76 12 81
CE : guinier@acm.org