



## L'ARCHIVAGE LEGAL

CE QU'IL FAUT METTRE EN ŒUVRE



# Introduction

Depuis 1994, la société SYSTEMIC apporte aux utilisateurs son savoir-faire dans le domaine du stockage, de la sauvegarde et de la sécurité des données.

Dans cette continuité et dès 2004, elle a décidé d'apporter son expertise dans le domaine de l'archivage numérique légal en publiant le premier Guide Blanc : 'L'Archivage légal - Ce qu'il faut savoir...'.

En 2006, pour aider les entreprises à déterminer les critères de fiabilité que doit respecter un système d'archivage, SYSTEMIC publie le Guide Rouge : 'L'Archivage légal - Ce qu'il faut faire...'.

En 2007, face au succès de ces 2 ouvrages et aux interrogations concrètes des responsables d'entreprises, SYSTEMIC poursuit ses recommandations en proposant ce nouveau guide bleu 'L'archivage légal, ce qu'il faut mettre en œuvre ...'.

Ce document de référence s'appuie sur des expertises reconnues (Cabinet Vaughan Avocat – Experts SYSTEMIC), et propose une démarche pragmatique pour déterminer les caractéristiques fonctionnelles structurantes d'un système d'archivage légal.

Nous vous en souhaitons une bonne lecture et vous rappelons que nos experts restent à votre disposition pour tout complément d'information...



# La Société SYSTEMIC

Créée en 1994, SYSTEMIC accompagne les grandes entreprises pour l'étude, la préconisation, la mise en œuvre et le suivi de leur infrastructure de stockage, sauvegarde et archivage.

Ancien Directeur des Systèmes d'Information, Hubert Taïeb, fondateur de SYSTEMIC, continue à mettre en exergue ce qu'il avait compris très tôt :

**L'importance cruciale de la maîtrise des données dans l'exploitation optimale du patrimoine informationnel.**

Dans cet esprit, SYSTEMIC s'est appuyé sur un constructeur solide et s'est engagé avec EMC, leader des infrastructures de l'information.

Aujourd'hui, fort de ce partenariat, SYSTEMIC est devenu le premier intégrateur EMC en France et a atteint un niveau de certification des plus élevés.

En complément, SYSTEMIC a su s'entourer des experts les plus reconnus, capables d'apporter des solutions pour tous les besoins et dans tous les secteurs d'activité. Editeurs, constructeurs et sociétés de conseil savent que SYSTEMIC est l'interlocuteur de référence pour la réussite de leurs projets.

## Une offre commerciale unique

Une démarche technique reconnue avec une offre commerciale unique : **La gestion des ressources à la demande...**



Pour répondre aux besoins croissants de capacité et à un niveau de disponibilité optimum, la société SYSTEMIC propose de livrer et installer à discrétion des capacités additionnelles dans tous les équipements proposés.

L'utilisateur peut alors les consommer en fonction de ses besoins en réglant trimestriellement. Cette offre de **gestion des ressources à la demande** intègre les baisses de coût éventuelles et les niveaux de service souhaité...

### **Une organisation orientée service et qualité**

Avec une culture du service inégalée sur le marché, SYSTEMIC tisse depuis plus de 10 ans des liens étroits avec ses clients. L'exigence du service bien rendu est devenue un élément culturel solidement imprégné dans l'organisation. Cette qualité garantit aux clients de SYSTEMIC une sécurité et un soutien technologiques de tous les instants.

Anticiper, s'engager, élaborer des solutions innovantes ou au contraire choisir des mécanismes éprouvés : ces enjeux demandent de l'expérience et de l'imagination.

SYSTEMIC impose à ses équipes d'aller plus loin que la technologie, de s'appropriier la problématique client et d'en faire un défi quotidien personnel. Ainsi l'objectif n'est pas simplement d'intégrer la technologie la plus puissante, mais de veiller à l'intelligence et à la performance de cette technologie dans l'organisation.

**SYSTEMIC, IL Y A TOUJOURS  
UNE SOLUTION ...**



# L'ARCHIVAGE LEGAL

## → CE QU'IL FAUT METTRE EN OEUVRE

De nombreux responsables sont confrontés aux difficultés de mise en œuvre d'un système d'archivage numérique « légal » au sein de leur entreprise.

L'archivage légal revêt une double signification :

- La première correspond à la notion **d'obligation d'archivage** : quels sont les documents que l'entreprise **doit** archiver du fait d'une obligation légale ou réglementaire ?
- La seconde correspond à la notion de **valeur juridique des informations archivées** : quelles sont les modalités à respecter pour que les informations conservées dans un système d'archivage numérique aient une valeur probante ?

Le cadre juridique et réglementaire est posé, mais il est complexe à déchiffrer : comment respecter le droit de la preuve, la législation sur les données personnelles, les multiples réglementations spécifiques ?

Ce guide propose une démarche pragmatique pour déterminer les caractéristiques fonctionnelles structurantes d'un système d'archivage « légal ».



## ➤ **La première étape consiste à classifier l'information selon sa nature**

Toute entreprise conserve les informations qui sous-tendent son activité, d'une façon plus ou moins structurée et organisée.

La liste ci-dessous mentionne les catégories les plus courantes des informations conservées :

- Facture
- Information de nature financière
- Donnée comptable
- Contrats et commandes entre professionnels
- Contrats et commandes professionnels/particuliers
- Donnée client (fichier client, ou données personnelles détenues par les établissements financiers, les assurances, les établissements hospitaliers)
- Fiches de paie
- Contrats de travail
- Selon le secteur d'activité : résultats de recherche, cahiers de laboratoire, résultats d'essais, plans, schémas, etc.

Il est indispensable d'établir une typologie de ces informations, car des règles juridiques différentes vont s'appliquer **en fonction de la nature de l'information considérée.**



## Le cycle de vie existant de chaque type d'information devra être identifié

L'archivage légal implique l'analyse du cycle de vie de l'information au sens du « *record management* » anglo saxon : création, modification(s), transaction, conservation, destruction.

Cette analyse prendra en compte l'ensemble des supports (papier, électronique) et des modalités de production (bases de données, outils bureautiques, messages électroniques, etc.). Elle déterminera l'état dans lequel l'information devra être archivée : depuis sa création, et dans ses versions successives lorsqu'elle a un statut définitif.

Au plan juridique, la nature du support initial de création de l'information a une grande importance, car plusieurs situations peuvent se présenter :

- Original papier, mais dématérialisation du processus de consultation et archivage numérique avec conservation de l'original papier
- *Id*, avec destruction de l'original papier
- Document numérique natif (E-mail, document comptable, résultats de recherche, spécifications techniques, plans, etc.)

Si les originaux papiers sont conservés, en cas de conflit, seul le document original papier fera foi. Dès lors, les éléments relatifs à la valeur probatoire des éléments électroniques archivés ne seront pas prépondérants dans le choix de l'architecture d'archivage.



Si l'original papier est détruit, il faudra prendre garde de ne pas priver le document numérique résultant de toute valeur probatoire en sécurisant le process de numérisation.

*S'agissant par exemple d'un courrier électronique, celui-ci est un document numérique natif. Une impression papier d'un courrier électronique n'est pas un « original » papier, car rien ne prouve l'identité de l'émetteur ni l'intégrité ou l'authenticité du contenu imprimé.*

## **Le cas particulier de la messagerie**

En France, il n'y a pas eu pour l'instant, comme aux Etats Unis, de condamnations spectaculaires du fait de l'incapacité de certaines entreprises à produire des courriers électroniques dans le cadre d'enquêtes menées par des autorités de contrôle.

Pour les entreprises françaises, les seules obligations légales ayant un rapport avec l'archivage de messagerie sont issues de:

- **La loi de sécurité financière (LSF)**, qui concerne les SA faisant appel public à l'épargne.

*La LSF impose la mise en place de procédures de « contrôle interne » pour garantir la transparence et la fiabilité des résultats financiers dans un but de protection des actionnaires. Le contrôle interne implique la mise en œuvre de moyens d'archivage et de recherche de l'information pertinents.*



- **Le règlement CRBF 97-02** modifié, qui concerne les Etablissements bancaires.  
*Ce règlement est spécifique au contrôle interne des établissements financiers. Il implique également la mise en œuvre de moyens d'archivage et de recherche de l'information pertinents.*
- **Sarbanes Oxley**, pour les sociétés françaises cotées sur les marchés boursiers américains ou filiales de sociétés cotées sur ce marché.  
*La législation américaine impose expressément l'archivage de la messagerie électronique.*

**Mais ça n'est pas une raison pour les autres pour ne rien faire !**

*Les archives E-mail sont la mémoire de l'entreprise, et elles sont le support naturel d'une grande partie de son patrimoine informationnel.*

Il s'en déduit une nécessité **POUR TOUTES LES ENTREPRISES** d'organiser l'archivage de leur messagerie électronique :

- 1) de façon structurée (savoir retrouver une information à partir de divers critères)
- 2) de façon à ce que les informations archivées aient une « valeur légale »

L'E-mail et les pièces attachées se présentent sous forme native comme une donnée électronique.



**Le cycle de vie d'un E-mail est souvent un cheminement tortueux** : par le jeu des transferts, des « *reply to all* », le mail est répliqué dans plusieurs répertoires, tel quel ou dans le corps d'autres messages, et il peut rentrer et sortir de l'entreprise plusieurs fois.

La première décision à prendre consistera à organiser le **tri préalable des E-mails qui seront archivés** (certains systèmes sont conçus pour éviter les archivages multiples de messages identiques).

### **Premier écueil : la nature par définition «personnelle» de l'E-mail**

L'utilisation de la messagerie électronique à des fins personnelles est une tolérance accordée dans beaucoup d'entreprises, qui génère des problèmes importants liés à l'impossibilité pour l'entreprise de prendre connaissance des messages personnels, considérés comme une « correspondance privée ».

Il en découle que les messages personnels ne devraient pas, en théorie, être stockés par l'entreprise (ou du moins sous un régime très spécifique).

Il faut donc trouver un moyen de séparer les E-mail privés des E-mail professionnels, qui seuls rentreront dans le système d'archivage à long terme de l'entreprise.

- Suggestion pour trier les E-mails sortants : demander aux salariés, par l'intermédiaire de la « charte informatique » de qualifier eux même la nature de l'information en apposant la mention « PRV » sur leurs E-mails personnels.



*Tout ce qui n'est pas expressément marqué comme «personnel» sera réputé être de nature professionnelle.*

- Limite : malgré cette précaution, les E-mail archivés peuvent contenir des données personnelles : soit parce que ce sont des E-mail personnels « entrants » non marqués, soit parce qu'ils contiennent des données personnelles sur les clients et les partenaires de l'entreprise.
- Recommandation : déclarer à la CNIL le traitement d'archivage de la messagerie, et se conformer à la délibération CNIL n°2005-213 du 11 octobre 2005 relative aux modalités d'archivage électronique dans le secteur privé.

## **Second écueil : les E-mail professionnels véhiculent des informations de nature très différentes**

Information financière ou comptable, échanges commerciaux, échanges techniques en rapport avec du savoir faire confidentiel, gestion de projets, etc.

Des règles différentes (durée, modalités de conservation) s'appliquent selon que l'information correspondante tombe sous le coup d'une réglementation spécifique, ou qu'elle est conservée à des fins uniquement probatoires.

On choisira entre deux options, selon le métier et la taille de l'entreprise :



- Pas de pré-classification : l'information est disponible par critère chronologique et systématiquement détruite après une certaine durée [*entreprises moyennes*]
- Pré-classification par type : information financière / technique / commerciale / projet, etc.[*Nécessite un travail important de préparation de l'information et une éducation des utilisateurs de la messagerie*]
- **La seconde étape consiste à identifier les règles juridiques qui régissent l'information à archiver**
  1. Si l'information est un « fait juridique » (des données de connexion par exemple) : *la preuve est libre.*
  2. Si l'information est un « acte juridique » qu'il faut conserver à des fins probatoires : *la valeur probatoire de l'écrit numérique répond à des exigences légales définies dans le Code Civil.*
  3. Si une réglementation spécifique s'applique à l'information considérée (SOX, LSF, CNIL, CFCI, instruction fiscale ...) : *il faut identifier les contraintes en résultant.*

En pratique, on pourra retenir la règle de prudence suivante :

- **Toutes les informations doivent être archivées de façon à en assurer la valeur probatoire** (catégorie 2), ce qui représente un socle minimum d'exigences fonctionnelles qui est défini ci-après.



- **Si une réglementation spécifique s'applique** : il faut identifier les contraintes qui ne sont pas satisfaites par le socle minimum précité.

Ces contraintes supplémentaires peuvent être liées :

- à la nécessité légale de signer électroniquement les documents,
- à des exigences particulières en terme de traçabilité, de support physique, de durée et de modalités de conservation, etc. [cf. pour les entreprises soumises à SOX les contraintes précises relatives à l'archivage posées par la « *Rule 17-CFR 17a* »],
- au fait que l'information comprend des données personnelles : obligations spécifiques de confidentialité et sécurité définies par la loi « Informatique et Libertés ».

La nature des contraintes n'est pas la même selon la réglementation concernée : certaines réglementations ne renseignent que sur la durée de conservation, d'autres (notamment les textes fiscaux) sont très précis sur les modalités techniques à mettre en œuvre.

En face de chacune des contraintes, il faut évaluer le risque afférent à une non conformité : amende, redressement fiscal, risque d'image, etc.



## La durée d'archivage

La durée d'archivage est celle définie par la loi (si elle existe) augmentée de la durée de prescription. Selon la nature de l'information considérée, cette durée variera de quelques années à une durée illimitée.

Pour ne parler que des documents commerciaux couramment utilisés par l'entreprise, les durées de conservation et de prescription sont malheureusement très disparates, et il faudrait en théorie procéder à une analyse document par document.

Pour les relations entre commerçants, la durée de prescription est de dix ans.

Pour les pièces comptables, la durée de conservation imposée par l'administration fiscale est de six ans, mais le délai de prescription prévu par le Code de Commerce est de dix ans.

Pour les actions en paiement de créance, la durée de prescription est de cinq ans.

**On peut en déduire que pour couvrir la majorité des documents archivés, le système d'archivage numérique de l'entreprise doit prévoir *a minima* une durée de conservation de dix ans.**



➤ **La troisième étape consiste à élaborer les spécifications fonctionnelles du système d'archivage à partir des informations collectées lors des étapes précédentes**

1. Un premier ensemble de spécifications, qui constitue le **socle de base**, correspond aux exigences fondamentales que doit respecter le dispositif de gestion de l'information numérique afin d'avoir une valeur « légale » [c'est à dire une valeur probatoire].
2. Un second ensemble de spécifications découle des contraintes spécifiques à l'information considérée, s'il en existe.
3. La durée d'archivage aura quant à elle un impact sur le format d'archivage et l'architecture du système en terme d'évolutivité, de capacité à effectuer des migrations et de réversibilité.



## La définition du SOCLE DE BASE

L'information archivée doit avoir une valeur probante. Il est inutile de mettre en place de coûteuses structures d'archivage si l'entreprise ne peut pas démontrer, en cas de conflit sur la teneur de l'information archivée, que celle-ci est juridiquement recevable.

Depuis la fin des années 1990, l'**écrit numérique** a acquis une reconnaissance légale dans les pays industrialisés.

En France, aux termes de l'article 1316 du Code civil : « *La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission* »

L'écrit numérique est donc fondamentalement différent de l'écrit papier en ce que l'information est dissociée du support. Ce qui importe est que l'information reste intelligible dans le temps.

Encore faut-il que cet écrit numérique ait une valeur probante, car « *qui n'a pas de preuve n'a pas de droit* ». Si dans un litige les pièces importantes sont non datées, sans aucune garantie d'intégrité et perdues au milieu de téra octets de données stockées, l'entreprise sera en très mauvaise position pour défendre ses droits.

De nombreux textes régissent maintenant l'écrit numérique en France :



- ✓ Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- ✓ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
- ✓ Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.

Ils ont tous été transposés dans le Code Civil.

L'article 1316-1 du Code Civil définit les conditions à remplir pour qu'un écrit numérique ait une valeur probante : *« 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 en garantir l'intégrité ».*

L'écrit numérique a une valeur probatoire si l'entreprise peut démontrer que son système d'archivage assure les fonctionnalités du SOCLE DE BASE :

- Capacité à identifier l'**origine** de l'information
- Garantie de l'**intégrité** de l'information **depuis sa création et pendant tout au long de son cycle de vie**, c'est à dire : sa lisibilité, la stabilité de son contenu informationnel, la traçabilité des opérations effectuées sur le document [définition de l'intégrité donnée par le Forum des Droits sur l'Internet].



## La signature électronique

L'article 1316-4 Code Civil définit la notion de signature électronique comme: « *l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* ».

Au regard des textes européens et français, la signature électronique résulte de l'utilisation d'outils et de services délivrés par des «Prestataires de services de certification électronique» qui exploitent une technologie cryptographique à clé publique (PKI) :

- Les « outils de création de signature » comportent une clé privée, strictement personnelle au signataire.
- Le « certificat de signature électronique » comprend la clé publique associée à la clé privée. Il permet de vérifier l'authenticité du message signé.

La signature électronique remplit de façon parfaite les deux fonctions du socle de base, car le document est crypté [donc son intégrité peut être vérifiée], avec un identifiant qui est propre au signataire.

De plus, un écrit numérique signé électroniquement peut être maintenant utilisé là où, autrefois, un écrit papier était requis à titre de validité. [*articles 1108-1 et 1108-2 du Code Civil*].

**Dans certains cas, l'écrit numérique doit être signé électroniquement par obligation légale :**

- **Les factures numérisées [hors EDI] ;**
- **Les marchés publics dématérialisés ;**
- **Les actes authentiques dématérialisés ;**



- Tous les actes pour lesquels un écrit est requis à peine de validité (crédits à la consommation, assurances, contrats de travail...).

*Dans tous les autres cas, l'utilisation de la signature électronique n'est pas obligatoire, mais elle sert à renforcer la valeur probatoire de l'écrit numérique* : si le document est signé électroniquement au moyen d'un « procédé fiable d'identification garantissant son lien avec l'acte auquel [la signature] s'attache », les fonctions du « socle de base » sont *de facto* assurées.

## **Quid d'une identification par *username* / *password* ?**

Le fait de s'identifier par un système de « *username/password* » est souvent considéré comme une garantie suffisante sur l'identité de l'émetteur d'un document.

Il s'agit effectivement d'une présomption de cette identité. Mais il ne faut pas oublier que si l'émetteur présumé du document en question nie en être à l'origine, les tribunaux accueilleront volontiers cet argument si l'entreprise ne dispose pas d'arguments sérieux pour démontrer que le système de « *username / password* » était très sécurisé.

Il est en tout état de cause recommandé, au sein de l'entreprise, de mentionner dans la charte informatique que toute transaction ou tout document initialisés avec les *username / password* d'une personne lui seront imputables. Cette précaution évite la dissémination inconsidérée de leurs identifiants personnels par les utilisateurs sur système d'information.



## L'évaluation du facteur risque dans le choix de recourir ou non à la signature électronique

Dans l'état actuel du droit, la solution idéale pour un archivage légal consisterait à archiver des « originaux numériques », c'est à dire des documents qui ont été signés électroniquement par leur émetteur.

La pratique est toute autre, et il faut se résoudre à admettre que dans le monde numérique, on devra souvent se contenter de documents qui sont l'équivalent de « copies » dans le monde papier.

*En effet, l'usage de la signature électronique est encore loin d'être banalisé, pour un certain nombre de raisons :*

- *Elle est coûteuse.*
- *Elle est difficile à mettre en place depuis la création du document dans de nombreux cas.*
- *Les modalités d'archivage d'un document signé électroniquement sont techniquement très contraignantes sur le long terme, puisque il faut garder l'ensemble de l'environnement afférent (applications, certificats, listes de révocation). Il en résulte un risque d'obsolescence, ajouté au risque de falsification des clés cryptographiques, qui oblige à « resigner » de façon régulière les documents archivés.*

Il faut donc au cas par cas s'interroger sur le risque lié à l'incapacité de démontrer la valeur probante de l'information considérée.



*Par exemple :*

- *Si les archives d'un projet reposent en majorité sur des courriers électroniques non signés, l'entreprise sera incapable de prouver l'authenticité d'un courrier « important » qu'elle verse au débat si le prestataire en conteste le contenu.*
- *En cas de manque de valeur probante de ses archives R&D et de ses cahiers de recherche, l'entreprise sera incapable de faire valoir ses droits face à un contrefacteur.*
- *En cas de manque de valeur probante du plafond d'un contrat d'assurance conclu à distance avec un consommateur, un établissement financier risque de devoir indemniser à hauteur d'un montant beaucoup plus élevé que prévu.*

Ce qui importe, même si l'information n'est pas « signée électroniquement » (au travers de l'utilisation de certificats de signature délivrés par des PSCE), est que le système d'archivage mis en place respecte les fonctionnalités du socle de base.

Ces fonctionnalités (identification de l'origine, intégrité et traçabilité) peuvent en effet être assurées par un ensemble de moyens techniques et de processus adéquats, que l'entreprise devra prendre soin de documenter dans sa politique d'archivage.



## Une solution intermédiaire intéressante

Même si l'on a surmonté l'obstacle des modalités de distribution de la signature électronique, reste à résoudre celui de la complexité technique de l'archivage des documents signés électroniquement sur une longue durée.

Cet obstacle peut être contourné : il suffit de procéder à la vérification de signature, d'une façon fiable et incontestable (par exemple au travers de l'intermédiation d'un tiers ou de systèmes certifiés) *avant* de rentrer l'information dans le système d'archivage.

Cette solution représente un bon compromis, car elle présente les garanties liées à l'utilisation de la signature électronique tout en permettant de mettre en place un système d'archivage performant sur le long terme.

## Impact de la durée d'archivage sur le choix du format d'archivage et sur la capacité de migration de la technologie choisie

La durée prévisible d'archivage permet d'associer une pondération adéquate à la capacité de la technologie choisie à supporter les migrations et la réversibilité du support d'information.

Quant au choix du format logique, les formats fermés propriétaires sont à proscrire pour la conservation des informations à long terme. Un format texte en standard ouvert ou un format image sera à privilégier.



➤ **La quatrième étape consiste à élaborer les choix structurants pour la mise en œuvre du système d'archivage**

A l'issue de la démarche qui vient d'être décrite :

- Nous connaissons les contraintes juridiques en terme d'obligations spécifiques de conservation.
- Nous connaissons les contraintes juridiques en terme de valeur probatoire de l'information archivée (ce qui, selon l'importance de l'information, dictera un choix plus ou moins sécurisé avec recours ou non à la signature électronique).
- Nous avons évalué les risques liés à une non conformité aux contraintes réglementaires et/ou à l'incapacité de démontrer la valeur probatoire de l'information stockée.

Nous pouvons faire un certain nombre de choix structurants :

- Les critères de sélection des informations à archiver.
- Le choix d'utiliser ou non la signature électronique pour créer et/ou archiver les documents.
- Le format d'archivage de l'information
- Les modalités de détermination de l'émetteur/propriétaire de l'information.
- Les règles de sécurité et les droits d'accès.
- Les modalités de garantie de d'intégrité et de pérennité (migrations, réversibilité).
- Les procédures de destruction.



Et :

- Le choix des infrastructures techniques matériel/logiciel qui garantissent les caractéristiques fondamentales du SOCLE DE BASE : identification de l'origine, intégrité, traçabilité.

Le choix de l'architecture définitive du système d'archivage et des outils matériel/logiciel résultera d'un compromis entre le coût et le niveau de sécurité recherché.

A l'heure actuelle, plusieurs constructeurs proposent des solutions à base de technologies disque dur qui permettent de conserver l'information de façon fiable, intègre et pérenne.

Pour autant, la construction du système d'archivage ne se résume pas au choix de la technologie. Le système d'archivage, vu dans sa globalité, devra intégrer tous les autres éléments qui ont été présentés ici : les critères de classification et d'accès à l'information, la durée de vie de l'information, la capacité à migrer les données pour prévenir le risque d'obsolescence, la garantie de lisibilité de l'information au cours du temps. Selon le niveau de sécurité recherché, le système sera plus ou moins redondé.

La datation de l'information, même si elle n'est pas abordée de façon explicite dans les textes juridiques, est bien entendu aussi un élément intrinsèque essentiel de l'information. Selon le niveau de sécurité souhaité, la date sera intégrée à l'information archivée par des moyens internes à l'entreprise, ou en utilisant des jetons d'horodatage distribués par des tiers spécialisés, ou ajoutée par l'équipement de stockage.



## **Il n'y a pas de solution d'architecture unique**

Le choix de la PME ne sera pas le même que celui d'un grand groupe, et surtout, c'est la nature de l'information à archiver qui déterminera le rapport « qualité/prix » de la solution retenue.

Enfin, il faut insister sur **l'importance de l'élaboration d'une Politique d'archivage, et ce quelle que soit la taille de l'entreprise.**

La Politique d'Archivage [Voir contenu ci-après], documente la façon dont l'entreprise organise et gère l'archivage numérique de son patrimoine informationnel. En cas de conflit avec une autorité de contrôle ou avec un tiers, la Politique d'Archivage sera une pièce indispensable de la défense de l'entreprise.

© *Isabelle Renard – Février 2007*



# **LES INCONTOURNABLES DE L'ARCHIVAGE NUMERIQUE**

### **➤ La déclaration CNIL**

Tout traitement de données personnelles (l'archivage étant considéré comme un « traitement » au sens de la loi) doit être signalé à la CNIL conformément à la Loi de 1978. Certains traitements font l'objet d'une simple déclaration. D'autres, compte tenu des données traitées, sont sujets à autorisation.

Le défaut de déclaration à la CNIL est sanctionné pénalement.

Les tribunaux considèrent que le défaut de déclaration CNIL rend le traitement illégal. S'agissant des données permettant de contrôler l'activité des salariés (badgeuses, logs), une information est inopposable au salarié si son traitement n'a pas été déclaré à la CNIL.

### **➤ L'élaboration d'une charte informatique**

La charte informatique est le document qui informe les employés de l'entreprise des modalités d'utilisation du système d'information, des risques, et des préconisations qu'ils sont tenus de respecter. La charte les informe également des moyens de surveillance mis en place par l'entreprise, des informations conservées, et des limites d'utilisation de la messagerie à des fins personnelles.



La charte prévoit en particulier une procédure selon laquelle les courriers électroniques personnels ne sont pas archivés par l'entreprise (que ceux-ci soient entrants ou sortants).

La charte doit être précise : sur les modalités et les fonctionnalités de surveillance, sur la navigation internet autorisée ou non, sur le respect de la confidentialité de ses login/mots de passe, sur la participation aux *blogs*, *chat*, *forum*, et enfin sur la procédure de marquage et de classement des données personnelles.

Ne pas oublier :

- de consulter le Comité d'entreprise et les représentants du personnel ;
- de déclarer à la CNIL l'ensemble des traitements de surveillance des salariés.

Il est préférable d'intégrer la charte informatique au règlement intérieur de l'entreprise pour que celle-ci soit opposable aux salariés. Si cela n'est pas possible, il faut au moins veiller à ce que la charte soit portée à la connaissance de chaque salarié, par tous moyens adaptés au mode de fonctionnement de l'entreprise : plaquette d'information, affichage, publication de la charte sur la page d'accueil du login, et/ou encore courrier électronique avec A.R. à chaque salarié.



# LA CHARTE INFORMATIQUE

## Exemple

La présente Charte a pour objet d'encadrer l'utilisation du système d'information de la SOCIETE.

Le Système d'Information constitue une ressource vitale pour la SOCIETE, tant au regard de sa fonction de communication, que de la valeur des actifs qui y résident.

Le Système d'Information est accessible aux salariés et prestataires de la SOCIETE, ainsi qu'aux tiers via le réseau internet. La SOCIETE souhaite établir des règles claires d'utilisation de son Système d'Information :

- garantir sa sécurité et la confidentialité de ses actifs ;
- maîtriser les coûts de connexion ;
- veiller au bon fonctionnement technique du réseau ;
- encadrer la responsabilité de la SOCIETE ;
- alerter les utilisateurs du Système d'Information sur les limites d'utilisation de celui-ci.

A ces fins, l'utilisation des moyens informatiques et réseau de la SOCIETE est encadrée par les principes suivants :

*[nota : ces principes sont ensuite déclinés et explicités dans le corps du document] :*



- 1- L'USAGE PERSONNEL DES MOYENS INFORMATIQUES ET RESEAU MIS A DISPOSITION DES UTILISATEURS PAR LA SOCIETE EST TOLERE, MAIS IL DOIT RESTER MODERE ET NE PAS AVOIR D'IMPACT SUR L'ACTIVITE PROFESSIONNELLE.
- 2- L'UTILISATEUR CONTRIBUE AU RESPECT DE LA SECURITE INFORMATIQUE AU SEIN DE LA SOCIETE. L'UTILISATEUR EST TENU RESPONSABLE DE TOUTE UTILISATION DU SYSTEME D'INFORMATION AU MOYEN DE SES IDENTIFIANTS PERSONNELS.
- 3- L'UTILISATEUR RESPECTE LA CONFIDENTIALITE DES INFORMATIONS RESIDANT SUR LE SYSTEME D'INFORMATION DE LA SOCIETE.
- 4- L'UTILISATEUR EXPLOITE UNIQUEMENT DANS LES LIMITES AUTORISEES LES ELEMENTS PROTEGES PAR UN DROIT DE PROPRIETE INTELLECTUELLE.
- 5- L'UTILISATION DE LA MESSAGERIE INTERNET DE LA SOCIETE DOIT SE FAIRE DANS UN CADRE LICITE ET CONFORME AUX CONSIGNES EDICTEES PAR LA DIRECTION INFORMATIQUE. TOUT MESSAGE QUI NE PORTE PAS LA MENTION « PERSONNEL » DANS SON OBJET SERA REPUTE PROFESSIONNEL.



- 6- LA CONSULTATION DE SITES WEB RESTE LIMITEE A CE QUI EST NECESSAIRE A L'USAGE PROFESSIONNEL CONSIDERE, ET L'ACCES A DES SITES A CARACTERE ILLICITE EST STRICTEMENT PROHIBE.
- 7- IL EST INTERDIT DE CRÉER DES SITES WEB PERSONNELS A PARTIR DU SYSTEME D'INFORMATION DE LA SOCIETE, DE PARTICIPER A DES BLOGS OU A DES FORUMS.

L'ensemble de ces prescriptions fait l'objet de différents contrôles de la part de la Direction Informatique de la SOCIETE, qui sont détaillés ci-après.



## ➤ L'élaboration d'une politique d'archivage

La politique d'archivage est le document qui décrit les objectifs attendus du système d'archivage et l'ensemble des procédures mises en œuvre pour atteindre ces objectifs et garantir la fiabilité du système.

La politique d'archivage décrit :

- les contraintes juridiques associées à chaque type d'information archivée ;
- les choix structurants qui ont été opérés [cf. étape IV ci-dessus] ;
- les moyens qui permettent d'assurer la traçabilité des opérations et l'intégrité des archives ;

La politique d'archivage est un outil précieux en cas de litige sur la validité d'une information archivée : elle démontre la sensibilité de l'entreprise à l'importance de la conservation de son patrimoine informationnel et elle guide la démarche de l'expert mandaté pour analyser les aspects techniques du litige.

Mais attention : Compte tenu de l'évolution rapide des technologies, la politique d'archivage n'a de valeur que si elle est régulièrement mise à jour, et que le système d'archivage lui-même est régulièrement audité.



## ➤ **La souscription d'une police d'assurance adaptée**

Votre police d'assurance dommage couvre-t-elle le risque de perte de vos archives numériques ? Il est probable que non.

Vous devez mettre en place une couverture qui couvre tant les dommages matériels (dégradation des supports, couverture des coûts de reconstitution), que les dommages immatériels (c'est à dire ceux qui sont la conséquence de la perte des données).

Cette couverture est bien sûr à adapter en fonction de la taille et de l'activité de l'entreprise : l'assurance doit surtout viser à couvrir la perte des données qui sont fondamentales pour l'activité de l'entreprise.



## INFORMATIONS PRATIQUES - ICONOGRAPHIE :

- **Isabelle RENARD** a une formation d'ingénieur. Avocate au Barreau de Paris, associée du cabinet VAUGHAN, elle anime un groupe à forte valeur ajoutée, *au carrefour de la technique et du droit*.
- Rédaction : **SYSTEMIC**
- EMC Corporation, le numéro 1 mondial des produits, services et solutions de stockage et de gestion d'informations
- AFNOR : <http://www.afnor.fr/>
- Norme ISO 15489 : Information et documentation "*Records Management*"
- « *Guide pour la conservation des Informations et des documents numériques* » de l'ATICA, Agence pour les Technologies de l'Information et de la Communication dans l'Administration
- « *Manuel pratique des Archives électroniques* », publié par la Direction des Archives de France

Note : Les informations fournies dans ce document sont susceptibles d'avoir été modifiées depuis son impression.





**24, rue de Caumartin, 75009 Paris**  
**Tel : 33(0)1 58 18 38 88 Fax : 33(0)1 58 18 30 57**  
**[www.systemic.fr](http://www.systemic.fr)**