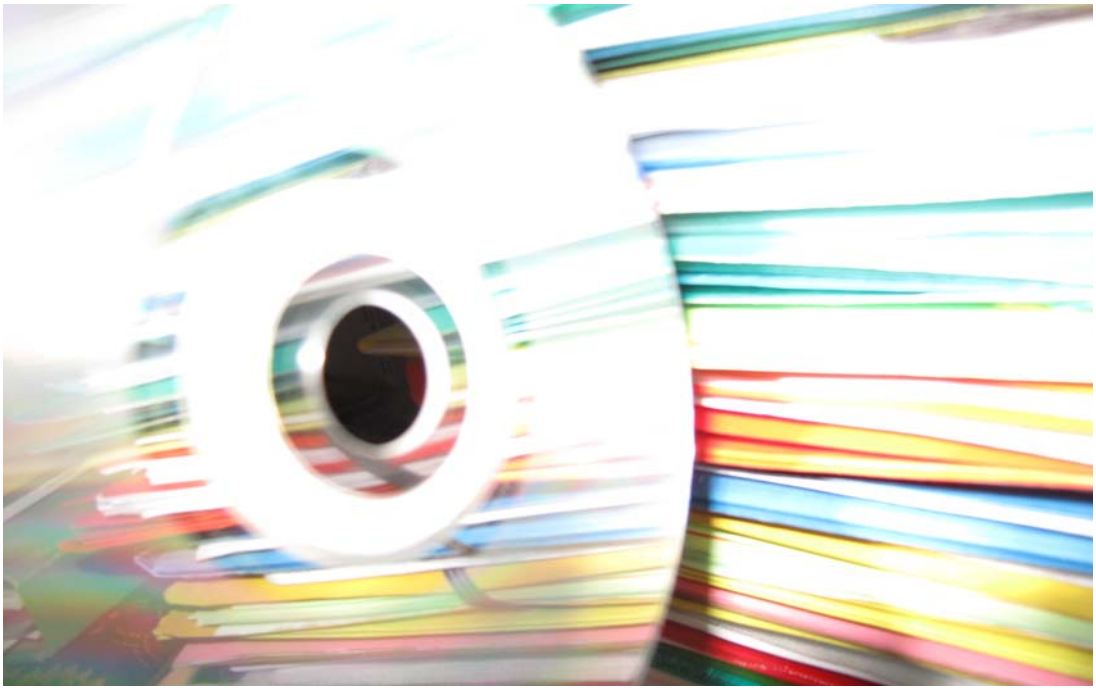
Forum des Compétences



# *VERS UNE POLITIQUE*

# *D'ARCHIVAGE ÉLECTRONIQUE*

# *DES DOCUMENTS*

# *VERS UNE POLITIQUE*

# *D'ARCHIVAGE ÉLECTRONIQUE*

# *DES DOCUMENTS*

***Le Forum des Compétences*** est un espace accélérateur d'échanges, de mise en commun et de transfert de compétences. Chacun bénéficie ainsi d'une optimisation dans l'exercice de sa fonction.

C'est pourquoi, des Entreprises travaillant dans le même secteur d'activité, la banque, acceptent de se retrouver afin d'élaborer, ensemble, les principes efficaces et communs à suivre pour atteindre l'objectif fixé par le régulateur et la hiérarchie.

Chacun restant concurrent et libre dans ses choix. Chaque année, des livrables sont édités. Résultat des différents groupes de travail, ils permettent de connaître les bonnes pratiques de travail afin de réaliser au mieux son activité. A chacun de les adapter à son environnement professionnel.

***Le Forum des Compétences*** a souhaité élaborer un guide relatif à l'archivage électronique, pour contribuer à la réflexion des Entreprises et les aider à bâtir une politique d'archivage électronique. Le Forum a confié à un groupe de travail le soin de proposer des éléments de réponse. Le groupe a réuni des praticiens de l'archivage, de la sécurité de l'information, de la conformité, et des juristes, issus de différents établissements financiers.

Le présent Guide ***« Vers une politique d'archivage électronique des documents »*** a pour ambition de soulever l'essentiel des questions à traiter pour bâtir une politique d'archivage électronique. Ce Guide est conçu pour apporter, nous l'espérons, un éclairage et des outils aux professionnels qui participent, dans leur Entreprise, à la construction ou à la gouvernance de l'archivage électronique. Les solutions restent à trouver dans chaque établissement, en fonction de ses valeurs, de ses activités et de son organisation.

# *Remerciements.*

Le ***Forum des Compétences*** remercie les représentants des Établissements Membres qui, au sein d'un groupe de travail*, ont conduit la réflexion et la rédaction de cet ouvrage :

***VERS UNE POLITIQUE***

***D'ARCHIVAGE ÉLECTRONIQUE***

***DES DOCUMENTS***

***** Voir annexe V

# Sommaire. . .

# *Introduction . . .*

L'usage des documents électroniques dans les Entreprises, et notamment les banques, est en forte expansion. Sites Web, messageries, contrats électroniques, outils collaboratifs ou coffre-fort numériques, les modes électroniques d'échange sont entrés dans les pratiques commerciales, même si le support papier reste présent pour certaines transactions.

Les pratiques numériques sont en constant développement et forment un secteur dynamique de l'économie mondiale, ainsi que l'énonce le Plan de développement de l'économie numérique[1]. Pour contribuer à accroître et diversifier les usages et les services numériques, pour développer le commerce électronique et investir dans l'économie numérique en toute sécurité, les Entreprises doivent s'assurer que les documents et traces de transactions sont conservés dans des conditions de fiabilité et de durabilité.
L'archivage électronique des documents représente l'une des problématiques majeures de l'économie numérique, problématique présente dès la conception des systèmes, à la différence de l'archivage des documents papier, qui intervenait en fin de cycle.

La question de la conservation sécurisée des documents, nativement électroniques ou numérisés, est devenue majeure aujourd'hui. L'archivage électronique concerne les spécialistes de l'archivage, de l'informatique et de l'organisation, mais également tous les métiers de l'Entreprise. Les problématiques sont d'ordre financier, commercial, de gestion du risque, notamment juridique, de conformité et d'environnement. Les choix sont structurants pour l'Entreprise.
L'archivage sécurisé est ainsi l'un des maillons de la continuité d'activité. Sa politique contribue à la maîtrise et la protection de l'information stratégique de l'Entreprise et s'inscrit ainsi dans une approche d'intelligence économique[2]: protection de l'information, mais aussi partage et meilleure circulation de l'information utile. Les problématiques que soulève l'organisation de l'archivage électronique sont liées aux priorités de l'Entreprise en matière de définition des besoins informationnels, de sécurisation du patrimoine informationnel et de maîtrise de l'accès à l'information.

Dans cet environnement, le ***Forum des Compétences*** a souhaité élaborer un guide relatif à l'archivage électronique, pour contribuer à la réflexion des Entreprises et les aider à bâtir une politique d'archivage électronique. Le Forum a confié à un groupe de travail le soin de proposer des éléments de réponse. Ce groupe a réuni des praticiens de l'archivage, de la sécurité de l'information, de la conformité et des juristes, issus de différents établissements bancaires.

La méthode de travail retenue a consisté tout d'abord à explorer l'environnement législatif et réglementaire de l'archivage, tant traditionnel que numérique. Le groupe de travail s'est également intéressé à l'évolution technologique qui permet la conservation sécurisée des documents électroniques dans le temps et aux questions pragmatiques posées par la conservation des documents et de leurs traces.
Les observations menées dans les établissements bancaires ont démontré que les impératifs juridiques sont similaires à ceux d'Entreprises de nombreux secteurs. Les banques sont soumises en outre, du fait de leur activité, à des exigences réglementaires qui créent, directement ou indirectement, des obligations spécifiques en matière d'archivage. Ce document, dans un souci de clarté pour le lecteur, quel que soit son secteur d'activité, traite des exigences réglementaires bancaires isolément.

Le présent Guide ***« Vers une politique d'archivage électronique des documents»*** traite différentes questions. La première est « Pourquoi archiver ? ». En d'autres termes, quels sont, outre les raisons opérationnelles, les impératifs légaux et réglementaires de conservation des documents à titre probatoire ? Cette partie intègre notamment les évolutions apportées par la réforme de la durée de prescription.

Le Guide s'intéresse ensuite à l'interrogation « Comment archiver ? », c'est-à-dire à la valeur ajoutée de l'archivage électronique, à ses éléments constitutifs, à sa localisation et à l'opportunité d'externaliser cette fonction.

1 Plan de développement de l'économie numérique, octobre 2008, www.francenumerique2012.fr

2 Consulter le guide « Intelligence Economique en milieu bancaire. Protection de l'information non structurée » édité par le Forum des Compétences, à paraître

La troisième partie traite des « procédures d'accès aux documents archivés ». Quels sont les acteurs, internes à l'Entreprise, qui accèdent aux documents archivés et dans quelles conditions ? Quels sont aussi les acteurs « externes » qui peuvent consulter les informations, notamment dans le cadre de procédures administratives et judiciaires ? Le Guide s'attache à détailler les différents droits de chacune des autorités administratives ou judiciaires, et aux limitations d'accès prévues par le droit. Outre les procédures strictement françaises, le document pose la problématique des actions étrangères (e-discovery et disclosure) visant à prendre connaissance de certains documents archivés.

Enfin, le cas pratique de l'archivage de la messagerie électronique traite des enjeux et des précautions d'utilisation. L'augmentation de la volumétrie des messages à archiver met en lumière les questions présentes dans tout système d'archivage électronique.

Le présent Guide ***« Vers une politique d'archivage électronique des documents»*** a pour ambition de soulever l'essentiel des questions à traiter pour bâtir une politique d'archivage électronique. Ce Guide est conçu pour apporter, nous l'espérons, un éclairage et des outils aux professionnels qui participent, dans leur Entreprise, à la construction ou à la gouvernance de l'archivage électronique. Les solutions restent à trouver dans chaque Entreprise, en fonction de ses valeurs, de ses activités et de son organisation.

# 1. Première partie : Pourquoi archiver ?. . .

## 1.1 CONTEXTE LÉGAL ET RÉGLEMENTAIRE

### 1.1.1 LES ENJEUX JURIDIQUES DE LA CONSERVATION

#### 1.1.1.1. Finalités de la conservation

Les documents doivent être conservés à diverses fins en raison de leur contenu (suivant que l'on soit en présence d'une facture, d'une pièce comptable, d'un contrat, d'un bulletin de paye, etc.). De plus, un même document peut se voir appliquer plusieurs règles différentes de conservation qui se cumulent, une « facture » étant ainsi également considérée comme une « pièce comptable »[3].

La durée de conservation de ces documents qu'il convient d'observer varie de même, en fonction de chacune des finalités considérées. Ainsi :

- L'exigence de conservation peut être imposée par un texte légal ou réglementaire (à titre d'exemple, l'article L.123-22 alinéa 2 du Code de commerce énonce que « *Les documents comptables et les pièces justificatives sont conservés pendant dix ans. (...)* »). Rentrent donc dans cette catégorie les hypothèses où la réglementation impose la conservation de documents particuliers (fiscaux, etc.) à des fins de contrôle par les autorités de régulation (respect des règles fiscales, respect des règles prudentielles, contrôles opérés sur la connaissance du client par les Entreprises de crédit, etc.) ;

- Mais le document pourra également faire office de preuve dans le cadre d'une action en justice (ex. nécessité de production d'un contrat à l'occasion d'un litige devant un tribunal) si celle-ci n'est pas prescrite. La durée de conservation à observer dépendra alors du délai de prescription extinctive, c'est-à-dire du délai à l'expiration duquel une action n'est plus possible ou un droit ne peut plus être exercé ;

- Enfin, le document pourra être conservé en raison de règles spécifiques à l'Entreprise, que ces règles soient le résultat des exigences des organes de contrôle interne de l'Entreprise ou que cette conservation soit nécessaire à des fins purement opérationnelles (hypothèse de suivi de la relation clientèle, de plan de continuation d'activité. Les règles applicables sont alors déterminées au sein de chaque Entreprise et ne sont pas opposables aux tiers.

#### 1.1.1.2. Principaux délais légaux de conservation et de prescription

Une étude attentive des textes applicables montre qu'il existe nombre d'obligations de conservation des documents dans le droit français, et notamment le Code de commerce, le Livre des Procédures Fiscales, le Code monétaire et financier ou encore dans certaines législations spécifiques.

Les principaux délais légaux de conservation et de prescription déduits des règles légales sont les suivants :

- conservation des documents comptables et des pièces justificatives en matière commerciale : dix ans (art. L.123-22 du Code de commerce précité) ;

- conservation en matière fiscale : six ans (art. L.102B et L.169 du Livre des procédures fiscales) ;

*3* Voir à ce sujet les développements au paragraphe 1.1.2.4.

- prescription extinctive en matière civile : en principe cinq ans pour les actions personnelles ou mobilières avec un point de départ « glissant » commençant à courir « *à compter du jour où le titulaire du droit a connu ou aurait dû connaître les faits lui permettant de l'exercer*» (art. 2224 du Code civil), mais sauf exception, un délai butoir de vingt ans a toutefois été fixé *« à compter du jour de la naissance du droit »* (art.2232 du Code civil)[4];
- prescription extinctive applicable aux obligations nées à l'occasion de leur commerce entre commerçants ou entre commerçants et non commerçants : cinq ans (art. L.110-4 du Code de commerce) ;
- délai général de la prescription extinctive pour les actions engagées par les professionnels vis-à-vis des consommateurs : deux ans (art. L.137-2 du Code la consommation ; auparavant seul un délai de forclusion était appliqué aux litiges nés d'un contrat de crédit à la consommation).

#### 1.1.1.3. Limitation des durées de conservation

A côté de ces obligations de conservation et donc d'archivage des documents, l'Entreprise doit également faire face en parallèle à des obligations de ne pas conserver les données qu'elle détient (et contenant des données personnelles) pendant une durée supérieure à ce que la législation en matière de protection des données personnelles pourrait prévoir, et donc de prévoir leur destruction au-delà de ces délais (cf. paragraphe 1.1.4).

Les Entreprises doivent donc mettre ces deux types de règles en cohérence et les prendre en compte lors de la mise en place de solutions d'archivage.

### 1.1.2. LES NOTIONS FONDAMENTALES CONCERNANT LES ÉLÉMENTS DE PREUVE À CONSERVER

#### 1.1.2.1 Preuve des actes et des faits juridiques

Les documents qui doivent être conservés notamment en application des textes ci-dessus peuvent revêtir des valeurs juridiques différentes, suivant la façon dont ils sont formalisés (document signé ou non) en réponse à des exigences textuelles et suivant le type de preuve qu'ils permettent d'apporter.

En matière juridique, la justification des droits allégués est fondamentale et l'on considère suivant l'adage « *Idem est non esse et non probari* » que « *il revient au même de n'avoir point de droit ou d'en avoir un et de ne pas pouvoir en établir l'existence* ». Il est donc essentiel que la partie qui se prévaut d'un droit ou de l'application d'une règle de droit par exemple, démontre l'existence des éléments qui sous-tendent sa prétention (selon l'article 1315 du Code civil).

Ce principe est usuellement désigné par l'expression de charge de la preuve ou « fardeau de la preuve » : à défaut de démontrer l'existence de ces éléments, la partie supportant la charge de la preuve risque de perdre son procès.

A contrario, si elle réussit à démontrer cette existence, la charge de la preuve est transmise à la partie opposée.

Ainsi, au fur et à mesure des preuves apportées par l'une ou l'autre partie en fonction de leurs allégations réciproques, la charge de la preuve pèse alternativement sur chacune d'entre elle au

4 Les délais de prescription indiqués intègrent la loi du 17 juin 2008 « portant réforme de la prescription en matière civile » (Loi n° 2008-5 61 du 17 juin 2008, JO du 18 juin).

cours du procès. Au final, « *l'incertitude ou le doute sont retenus au détriment de celui qui en à la charge* ».

Par ailleurs, la preuve qui est apportée par une partie peut toujours être discutée ou remise en cause par la partie adverse ou par le juge, dans les cas où il peut se saisir d'office de certaines questions.

Si ce qui est avancé par une partie n'est pas discuté par l'autre, alors le juge ne pourra que relever la reconnaissance des faits allégués par la partie à qui on les oppose (sachant que le silence opposé à l'affirmation d'un fait ne vaut pas à lui seul reconnaissance de ce fait).

Dans l'hypothèse où la réalité d'un fait, du contenu ou de l'existence d'un acte est discutée, c'est un tiers aux parties (le juge) qu'il faudra convaincre de la pertinence de ses arguments, afin que celui-ci puisse qualifier juridiquement la situation dans un premier temps et appliquer ce que les textes prévoient dans de tels cas dans un second temps.

Le droit opère classiquement une différence fondamentale entre la preuve des événements qu'il s'agit d'apporter. Ainsi :

- La preuve d'un fait juridique peut être apportée par tous moyens. C'est un fait quelconque qui s'est produit et dont les conséquences juridiques n'ont pas été envisagées dès l'origine (accident de travail, connexion à un site Internet, envoi d'une information). Ainsi, on peut prouver par tous moyens imaginables la réalité d'un accident, d'une chute, etc. qui s'est produite sans avoir à prévoir de formalité particulière (pas de présence de notaires, de document écrit telle qu'une attestation obligatoire, etc.) car on ne pouvait logiquement prévoir dans quel cadre ce fait, anodin ou inattendu, pourrait avoir des conséquences juridiques.

- Par contre, s'il s'agit d'établir l'existence d'un acte juridique – contrat entre deux parties ou engagement pris unilatéralement par une partie – il faudra apporter la preuve de manifestations de la volonté ayant pour objet et pour effet de produire une conséquence juridique. Compte tenu de l'importance de ces actes pour chacune des parties et surtout de leur prévisibilité de leur existence et de leurs conséquences (ex : contrat de prêt, etc.), le droit va alors exiger le respect de certaines formalités. Chaque partie devra donc par exemple et en principe se pré constituer une preuve de l'engagement pris.

Cette dichotomie va donc entraîner des conséquences importantes quant aux modalités et aux exigences d'archivage.

Enfin, certains actes juridiques prévoient des engagements si importants aux yeux du législateur comparativement aux intérêts de certaines parties qu'il convient de protéger (consommateur, auteur) que celui-ci a prévu des règles spécifiques. Ainsi, la tenue d'un écrit n'est plus seulement nécessaire en termes de preuve, mais est surtout obligatoire à la validité même de l'engagement (sans cette forme, le contrat est nul et non avenu). Nous verrons les conséquences en termes d'archivage de ces actes particuliers plus avant dans ce Guide.

#### 1.1.2.2 Les règles de preuve spécifiques selon les domaines du droit

Les règles applicables en matière de droit de la preuve sont différentes suivant la branche du droit applicable.

En droit commercial, dans les relations entre « commerçants » au sens juridique du terme (ce qui inclut la très grande majorité des Entreprises), la preuve est dite « libre » en vertu de l'article L.110-3 du Code de commerce : tous les modes de preuve sont donc acceptables par le juge y compris pour la preuve des actes juridiques. Reste que c'est à lui qu'il appartiendra de trancher en cas de litige quant à l'évaluation de leur force probante réciproque.

En droit pénal également, la preuve est libre, quel que soit l'acte ou le fait juridique à démontrer.

De plus, sauf exception, la preuve est libre en droit administratif et sa force probante dépend de l'intime conviction du juge.

Les principes sont différents en droit civil.

#### 1.1.2.3 Les principes en droit civil

En droit civil, le système de preuve est prévu et encadré par la loi et seuls certains modes de preuve sont acceptés pour les actes juridiques.

### Exigence de preuve par écrit

La preuve par écrit, c'est-à-dire par document signé, est exigée pour tout acte juridique supérieur à 1 500 EUR. (depuis le 1er janvier 2005 ; auparavant 800 EUR.) en vertu de l'article 1341 du Code civil et de son décret d'application du 15 juillet 1980, plusieurs fois modifié.

En outre, il n'est en principe pas possible de recourir à la preuve par témoins « contre et outre » un écrit qui constate un contrat.

### Exceptions à l'obligation de produire un écrit

Il faut considérer comme une exception à l'obligation de fournir un écrit, la possibilité qu'il n'y ait pas d'original écrit en dessous du seuil fixé (de 1 500 EUR). En dessous de ce seuil, la preuve est libre et peut donc être apportée par tout moyen.

Par ailleurs, comme nous l'avons indiqué, les actes de commerce peuvent se prouver par tous moyens (art. L.110-3 du Code de commerce).

A l'inverse, les règles du droit civil s'appliquent entre deux particuliers.

Enfin, quant à l'application entre un particulier consommateur et un commerçant (telle qu'une société), la situation se complique quelque peu : le commerçant est tenu par les règles du droit civil, posant comme principe la primauté du document signé. A l'opposé, le particulier se voit appliquer, quant à lui, les règles plus favorables du droit commercial et peut donc apporter la preuve des engagements conclus avec le commerçant par tout moyen.

Si le principe du droit civil est celui de la primauté de l'écrit signé au-delà de 1 500 EUR, il est également assorti d'exceptions. Ainsi :

- A défaut d'écrit, il est possible selon l'article 1347 du Code civil de produire un commencement de preuve par écrit (document non signé tel qu'un courriel, une publicité, etc.) complété par un autre mode de preuve extérieur à l'acte tel qu'un témoignage, un autre commencement de preuve par écrit ou encore une présomption. L'ensemble est alors recevable à l'égal du document écrit et c'est donc au juge qu'il reviendra de peser la force probante des preuves contraires apportées devant lui.
- En cas d'impossibilité matérielle (perte de l'acte par suite d'un cas fortuit) ou morale (liens familiaux ou d'affection) de se procurer une preuve littérale, ou en cas de perte du titre par suite d'un cas fortuit ou d'une force majeure (art. 1348 al. 1er du Code civil).
- A défaut de conservation de l'original par une partie ou le dépositaire, il est possible de produire une copie fidèle et durable pour prouver un acte (art. 1348 al. 2 du Code civil).

Ainsi, l'exigence d'un écrit n'impose pas nécessairement la production d'un original (cf. infra).

Précisons toutefois que certaines législations particulières, notamment le droit de la consommation, imposent de disposer d'un écrit dans certains cas particuliers (garanties, etc.).

les développements précédents ne s'appliquent pas à ces situations, même si le montant du contrat est inférieur à 1 500 EUR (cf. paragraphe 1.2.1.).

Des règles particulières régissent également les contrats conclus par voie électronique en raison de leur nature dématérialisée (cf. paragraphe 1.3.).

### Exceptions à l'obligation de produire un original : les copies

Une dérogation notable est prévue par les textes, lorsqu'une partie ou le dépositaire n'a pas conservé le document original et présente une copie qui en est la « *reproduction non seulement fidèle mais aussi durable* ». Le terme « durable » est défini comme étant « *toute reproduction indélébile de l'original qui entraîne une modification irréversible du support* » (art. 1348 al. 2 du Code civil).

Ce qui est visé par ce texte n'est pas l'hypothèse où la non conservation du titre original vient d'une impossibilité matérielle ou morale de se procurer une preuve littérale ou encore la perte du titre par cas fortuit ou de force majeure. **Il s'agit bien de la volonté d'une partie ou du dépositaire de ne pas conserver le titre original mais seulement une copie qui, sous certaines conditions de fidélité et de durabilité, aura une valeur probante équivalente à celle d'un écrit traditionnel.**

Notons que ces règles concernent les écrits nécessaires à titre de preuve ou de validité. Elles ne devraient donc pas trouver à s'appliquer pour la preuve de faits juridiques : preuve de l'envoi d'une lettre, d'une notification ou d'une information.

La réalité d'un fait juridique se prouvant par tous moyens, aucune forme particulière ne devrait être requise, notamment pour la copie électronique issue d'un document papier.

Or une décision récente de la Cour de cassation du 4 décembre 2008, à laquelle celle-ci de surcroît a voulu donner toute la publicité possible, semble remettre en cause ce schéma. Ainsi, en cassant l'arrêt d'appel qui avait reconnu que la preuve de l'envoi de la lettre d'information pouvait être faite par tous moyens et qui n'avait pas exigé de démonstration particulière sur le contenu allégué de la copie électronique, la Cour de cassation semble en définitive imposer une forme particulière (copie dont il convient de démontrer la fiabilité et la durabilité) aux copies électroniques, y compris lorsque la preuve ne concerne que des faits juridiques. Si l'on ne peut que s'étonner de la rigueur de la démonstration juridique, il faut bien en tirer les conséquences et, à défaut d'évolution prochaine contraire, considérer que la notion même de copie électronique suppose un formalisme particulier, quelle que soit la nature juridique de l'original.

➔ *Se reporter à l'annexe II – Tableau sur le régime de la preuve en droit français*

### Application pratique : la preuve par copie

Depuis la mise en place de l'Échange Image Chèque (EIC) en juin 2002 visant à dématérialiser le dernier moyen de paiement qui ne l'était pas en France, les banques ne conservent plus que des images numériques des chèques. Ainsi, l'EIC compense de façon électronique les chèques sur le Système Interbancaire de Télé-compensation (SIT). Il remplace les 108 chambres de compensation et les Centres Régionaux d'Échanges d'Images Chèques (CREIC) répartis dans toute la France.

Il arrive qu'à défaut de pouvoir présenter l'original, une partie produise en justice une copie de l'original, notamment par photocopies ou télécopies (cf. en annexe II – la jurisprudence en matière de preuve par copies). Il a été jugé que des photocopies et télécopies étaient des **copies fidèles et durables** (au sens de l'article 1348 alinéa 2 du Code civil) et pouvaient dès lors constituer la preuve de l'existence d'un contrat ; mais leur admission en tant que preuve ressort de l'appréciation souveraine des juges du fond ce qui fait peser un aléa certain dans la présentation d'une photocopie ou une télécopie en lieu et place d'un original. La décision précitée de la Cour de cassation du 4 décembre 2008 en est un parfait exemple.

C'est pourquoi dans le cadre d'une politique d'Entreprise, les copies d'originaux avec destruction des originaux peuvent être envisagées mais à condition d'avoir la certitude de fiabilité sur le long terme des procédés utilisés pour la copie des documents.

➔ *Se reporter à l'annexe III, panorama de la jurisprudence relative à la preuve par copie.*

**Convention sur la preuve**

La convention sur la preuve est un contrat ou un ensemble de clauses insérées dans un contrat plus global conclu entre deux parties. Elle a pour objet de définir les modes de preuve admissibles entre les parties, la charge de la preuve et les modalités de règlement des conflits de preuve. Ce type de stipulations peut également prévoir les dispositions applicables entre les parties en matière d'archivage (durée et/ou modalités).

La validité de ces conventions avait été reconnue en jurisprudence dès 1989 ; elle a implicitement été consacrée par la loi en 2000, à l'article 1316-2 du Code civil[5].

Les parties vont donc prévoir, dans le contrat, les règles selon lesquelles la preuve littérale pourra être apportée. Ainsi, elles pourront admettre que le fait d'utiliser un système d'archivage électronique n'altère pas a priori la force probante des documents. A titre d'exemple, c'est le système mis en place pour les enregistrements informatiques qui constate les opérations réalisées par cartes bancaires.

Les conventions sur la preuve ne peuvent déroger ni aux règles d'ordre public, ni à la réglementation sur les clauses abusives, ni interdire à une partie d'apporter une preuve contraire. En cas de contestation, la validité de la convention et la force probante des éléments de preuve produits seront soumises à l'appréciation du juge.

Nous invitons le lecteur intéressé par toutes ces questions à consulter également les recommandations du Forum des Droits sur l'Internet sur la conservation électronique des documents du 1er décembre 2005[6].

#### 1.1.2.4 Quelques illustrations pratiques de l'évolution des contraintes juridiques de l'archivage

L'objectif de ce document n'est pas de recenser de manière exhaustive l'ensemble des documents dont la législation, française et le cas échéant internationale, impose la conservation.

Une étude exhaustive sur les délais de conservation des archives en matière bancaire, a été faite par le CFONB (brochure « La banque et les durées de conservation d'archives » parue en 1993, mise à jour en octobre 2005 et faisant l'objet d'une actualisation).

5 « À défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable ».

6 Disponibles sur http://www.foruminternet.org/specialistes/concertation/recommandations/recommandation-du-forum-des-droits-sur-l-internet-la-conservation-electronique-des-documents.html

Notre propos ici se concentrera sur quelques exemples concrets d'obligations juridiques de conservation de documents afin que lecteur puisse, au sein de l'Entreprise dans laquelle il appartient se poser les bonnes questions lors de la mise en place d'une politique d'archivage.

**Documents comptables**

Le Code de commerce édicte un certain nombre d'obligations en matière de conservation des documents comptables.

Rappelons que les opérations de banque étant de nature commerciale (à moins qu'elles ne soient réalisées sans intention spéculative), ces obligations s'appliquent aux banques en sus des obligations spécifiques propres à la réglementation bancaire.

Ainsi, l'article L.123-22 du Code de commerce énonce que les documents comptables et les pièces justificatives doivent être spécifiquement conservés, et ce pendant dix ans.

A cette obligation générale, le Code de commerce ajoute quelques précisions sur la forme que peut ou doit prendre cette conservation, comme par exemple pour certains documents particuliers (livre journal, grand livre et livre d'inventaire) ou encore pour les comptes annuels.

Tout commerçant se doit ainsi de tenir un livre-journal, un grand livre et un livre d'inventaire (art. R.123-173 du Code de commerce).

Il est précisé par ailleurs que ces documents peuvent être conservés sous forme électronique, étant donc entendu que la loi n'impose pas une telle conservation sous forme électronique, elle ne fait que la rendre possible. Pour autant, lorsque cette faculté est choisie par l'établissement, les textes prévoient un formalisme particulier : ces documents conservés sous forme électronique doivent être identifiés, numérotés et datés dès leur établissement par des moyens offrant toute garantie en matière de preuve (art. R. 123-173 du Code de commerce).

Autre obligation, cette fois-ci concernant les comptes annuels : les mouvements affectant le patrimoine de l'entreprise doivent être enregistrés en comptabilité et de manière chronologique (art. L.123-12 du Code de commerce).

L'entreprise doit notamment établir des comptes annuels à la clôture de son exercice au vu des enregistrements comptables et de l'inventaire. Ces comptes annuels comprennent le bilan, le compte de résultat et une annexe (art. L.123-12 du Code de commerce).

**Factures**

Tout achat de produits ou toute prestation de service pour une activité professionnelle doivent faire l'objet d'une facturation (art. L.441-3 du Code de commerce).

La facture est donc un document qui atteste de l'achat ou de la vente de biens ou services. Sa conservation diffère selon que l'on se place d'un point de vue comptable, fiscal ou commercial.

La facture, en tant que pièce comptable, doit être conservée, comme vu précédemment sur tout support, (y compris électronique), dix ans à compter de la clôture de l'exercice comptable, en vertu de l'article L.123-22 du Code de commerce.

La facture, en tant que pièce justificative de TVA, doit être conservée quant à elle six ans à partir de la date à laquelle le document a été établi ou à partir de la date de la dernière opération mentionnée (art. L.102 B al. 1 et L.169 al. 1er du Livre des procédures fiscales LPF).

Enfin, en tant que preuve d'une obligation née à l'occasion de rapports commerciaux, la facture doit être conservée dix ans après la clôture du compte (art. L.110-4 du Code de commerce).

Par ailleurs, le volume de papier très important généré par ces obligations de conservation a amené à une réflexion, notamment au niveau européen, sur le sujet de la dématérialisation de ce type de document, et donc à la création de « factures électroniques ».

**Cas particulier de la facture électronique**

Ainsi, s'agissant de la facture électronique, la loi du 29 décembre 1990 permet notamment la télétransmission des factures via un système d'Échanges de Données Informatisées, également appelé « EDI ». Plus récemment, la Directive du 20 décembre 2001 modifiée le 28 novembre 2006 et transposée par la Loi de finances rectificative en date du 30 décembre 2006 a rendu possible la transmission de facture par voie électronique et plus précisément l'envoi de « *factures transmises par voie électronique et sécurisée au moyen d'une signature électronique* » en remplacement de factures papier.

Les obligations relatives à la conservation de telles factures sécurisées au moyen d'une signature électronique sont contenues à l'article L.102 B du Livre des procédures fiscales (LPF) et précisées dans le décret d'application n° 2003-659 du 18 juillet 2003 et surtout dans la circulaire de la Direction Générale des Impôts (DGI) n° 136 du 7 août 2003.

L'article L.102 B énonce ainsi que la conservation des factures électroniques doit être réalisée sur des supports informatiques, et pendant une durée de six années « *à compter de la date de la dernière opération mentionnée sur les livres ou registres ou de la date à laquelle les documents ou pièces ont été établis* ».

Question formalisme, ce même article indique que les factures électroniques doivent être émises et transmises par voie électronique dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique (le procédé à utiliser étant décrit dans le décret d'application susmentionné).

Enfin, à l'instar de ce que l'on vient de voir concernant la facture, la durée de conservation des factures électroniques est différente selon que l'on se place d'un point de vue fiscal (six ans après l'échéance de l'année civile) ou comptable (dix ans). Il est précisé que les modalités de conservation de la facture sécurisée au moyen d'une signature électronique sont strictes au regard du plan fiscal, donc pendant les six premières années, alors qu'elles peuvent être atténuées (notion de copie papier acceptable par exemple) pendant les quatre années restantes.

Par ailleurs, certaines obligations de conservation des documents obéissent à des règles plus spécifiques selon l'activité de la société.

Ainsi en va-t-il des Entreprises de crédit soumises à la réglementation bancaire telle que le Code monétaire et financier ou le Règlement Général de l'AMF, mais également potentiellement à des règles plus spécifiques (marché Euronext, par exemple).

**Exemples tirés de la réglementation bancaire**

S'agissant de la réglementation bancaire, l'essentiel des obligations de conservation des documents se trouve dans le Code monétaire et financier et dans le Règlement Général de l'AMF.

Comme évoqué supra, le CFONB a mené une étude de fond sur l'archivage des documents dans le domaine bancaire. Sont évoqués notamment les archives spécifiquement relatives à

l'activité bancaire – à titre d'exemple les documents liés aux comptes, les cautionnements, les ordres de Bourse – ainsi que les archives relatives à l'établissement bancaire.

Sans que cette liste puisse être considérée comme exhaustive, doivent aussi être conservés :

- tous les documents préparatoires à l'élaboration des publications diffusées sous la responsabilité d'un service d'analyse financière ou d'une agence de notation, pendant un délai de trois ans (art. L.544-3 du Code monétaire et financier) ;

- les enregistrements mentionnés aux articles L.533-8 et au 5 de l'article L.533-10 du Code monétaire et financier et ce pendant au moins cinq ans, soit les documents suivants (art. 13-49 du Règlement Général de l'AMF) :
- les informations pertinentes relatives à toutes les transactions sur instruments financiers conclues ;
- tout service qu'ils fournissent et de toute transaction qu'ils effectuent, permettant à l'Autorité des Marchés Financiers de contrôler le respect des obligations du prestataire de services d'investissement et, en particulier, de toutes ses obligations à l'égard des clients, notamment des clients potentiels ;
- l'historique des mouvements sur instruments financiers (art. 322-25) du Règlement Général de l'AMF) ;
- l'historique des comptes d'instruments financiers ouverts en toutes classes du plan comptable (art. 322-25 du Règlement Général de l'AMF).

La Commission Bancaire, de son côté, détermine la liste, le modèle et les délais de transmission des documents et informations qui doivent lui être remis. Elle peut demander aux personnes soumises à son contrôle tous renseignements, documents, quel qu'en soit le support, et en obtenir la copie, ainsi que tous éclaircissements ou justifications nécessaires à l'exercice de sa mission. Elle peut également demander la communication des rapports des commissaires aux comptes et, d'une manière générale, de tous documents comptables dont elle peut, en tant que de besoin, demander la certification ainsi que tous renseignements et informations utiles (art. L.613-8 Code monétaire et financier).

**Exemple particulier : La plate forme boursière NYSE-Euronext**

Il existe également des réglementations particulières applicables à certaines activités.

A titre d'exemple, les Entreprises exerçant une activité sur la plate forme boursière NYSE-Euronext sont soumises à la réglementation de cette dernière. En ce qui concerne les échanges sur les Marchés de Titres d'Euronext, doivent ainsi être conservés les enregistrements des conversations téléphoniques pendant une période d'au moins six mois (règles de marché d'Euronext, 8303 livre 1er).

**Exemple tiré du droit de la consommation**

Par ailleurs, d'autres dispositions particulières existent, telles que par exemple celles issues récemment du droit de la consommation. Ainsi, l'article L.134-2 du Code de la consommation oblige le contractant professionnel, lorsqu'un contrat a été conclu en ligne et porte sur une somme égale ou supérieure à 120 EUR (somme fixée par le décret n° 2005-137 du 16 février 2005), à conserver l'écrit électronique constatant le contrat pendant une durée de dix ans (durée fixée par le même décret) et à en garantir l'accès au cocontractant non professionnel à « *tout moment* ». Notons que, selon le Forum des Droits sur l'Internet, cette expression doit être comprise « *comme n'imposant pas une fourniture immédiate et en ligne du contrat, mais une communication de celui-ci dans un délai raisonnable* »[7].

7 Nous renvoyons le lecteur intéressé, notamment sur l'applicabilité de ce texte aux Etablissements de crédit, à la recommandation du Forum des Droits sur l'Internet « Droit de la consommation appliqué au commerce électronique », disponible ici : http://www.forumInternet.org/specialistes/concertation/recommandations/recommandation-du-forum-des-droits-sur-l-internet-droit-de-la-consommation-applique-au-commerce-electronique.html

### 1.1.3. LES SANCTIONS ET CONSÉQUENCES DE LA NON-CONSERVATION DES DOCUMENTS

Celles-ci peuvent être de plusieurs ordres :

- amendes,
- sanctions disciplinaires et/ou administratives,
- sanctions financières,
- redressement fiscal,
- perte de procès,
- préjudices d'image,
- etc.

Les tribunaux ont ainsi eu l'occasion de sanctionner à plusieurs reprises la non-conservation de documents, notamment en matière fiscale.

#### 1.1.3.1. La jurisprudence

Ainsi, une société s'est vue notifier un redressement par l'administration fiscale à hauteur de 301 087, 42 EUR pour défaut de présentation des documents comptables des années 1980 à 1984.
Or, cette Entreprise avait une société mère qui s'était engagée par contrat à conserver, pour le compte de la filiale, les documents de celle-ci, ce qu'elle n'a pas fait. En raison de cette carence, la filiale a été sanctionnée et s'est donc retournée en justice contre sa société mère.

La cour d'appel de Paris[8] a alors sanctionné la société mère qui *« s'était engagée à assurer la garde des archives de son ancienne filiale pendant les délais légaux de conservation, soit pendant le délai de dix ans prescrit par l'article L.123-22 du Code de commerce, mais également pendant tout le temps où son ancienne filiale pourrait être appelée à faire valoir ses droits ou obligations, notamment en matière fiscale et avait détruit en 1995 les archives de la filiale concernant les exercices 1980 à 1984, alors que le droit de contrôle de l'administration n'était pas prescrit ».*

La société mère n'a pas respecté ses engagements contractuels et a été condamnée à indemniser l'ancienne filiale du préjudice que cette dernière a subi, soit les 301 087, 42 EUR à titre principal.

Dans une affaire différente, la Cour de cassation[9] a jugé, quant à elle, que *« X … en tant que professionnel averti, ne pouvait légitimement ignorer les obligations de conservation des documents justificatifs prévus par les articles 290 quater II et 96 B et suivants de l'annexe III du Code général des impôts ; (...) que le caractère nécessairement approximatif de cette évaluation est imputable au moins pour partie au prévenu qui n'a pas été en mesure de représenter les documents qu'il était tenu de conserver ».* La sanction de trois mois d'emprisonnement avec sursis et de 60 000 FRF d'amende prononcée par la Cour d'appel dans cette affaire a en l'occurrence été maintenue.

Pour autant, ces obligations de conservation ne se prolongent pas au-delà des délais requis. Ainsi, la Cour de cassation[10] a affirmé dans une troisième affaire, pour décharger un établissement bancaire qui n'avait pas conservé les documents comptables au-delà de dix ans, *« qu'il résulte de l'article L.123-22 du Code de commerce que les documents comptables et pièces justificatives n'ont pas à être conservés par un commerçant au-delà d'une durée de dix ans ».*

8 Cour d'appel Paris - 21 Mars 2003 – n° JurisData : 2003-214195.

9 Cour de cassation chambre commerciale 30 mai 2001 n° de pourvoi 00-83862.

10 Cour de cassation Chambre commerciale 24 avril 2007 n° de pourvoi 05-21.477.

#### 1.1.3.2. Sanctions imposées par les régulateurs

Par ailleurs, outre les sanctions des tribunaux, les régulateurs, que ce soit l'AMF ou la Commission Bancaire peuvent émettre des sanctions contre l'Entreprise de crédit qui ne respecterait pas ses obligations réglementaires.
A titre d'exemple, nous pouvons citer deux cas, le premier à propos d'une sanction de l'AMF, le second à propos d'une sanction de la Commission Bancaire.

**Sanctions de l'AMF**

L'AMF peut prononcer des sanctions allant de l'avertissement jusqu'à l'interdiction définitive d'exercer une activité, éventuellement assorties de sanctions pécuniaires (jusqu'à 10 millions d'EUR ou au décuple du montant des profits éventuellement réalisés selon l'article L.621-15 du Code monétaire et financier).

**Sanctions de la Commission Bancaire**

La Commission Bancaire peut adresser des sanctions allant de l'avertissement jusqu'à la radiation, éventuellement assorties de sanctions pécuniaires (au plus égales au décuple du montant du capital minimum auquel est astreinte la personne morale sanctionnée), et d'une publication, à moins que cette publication ne risque de perturber gravement les marchés financiers ou de causer un préjudice disproportionné aux parties en cause (art. L.613.21 Code monétaire et financier).

### 1.1.4. POSITION DE LA CNIL SUR L'ARCHIVAGE ET SA DURÉE

#### 1.1.4.1. Principes

Les Entreprises sont contraintes par diverses obligations légales de conserver des informations détaillées sur leur activité passée, comme nous avons pu le constater lors des développements précédents, en particulier au sujet des opérations effectuées avec leurs clients, fournisseurs ou salariés. Ces informations (documents internes, pièces comptables, déclarations sociales et fiscales, transactions bancaires, contrats, etc.) comportent généralement des données personnelles et se retrouvent, dès lors, protégées par la loi du 6 janvier 1978 modifiée.

- La Commission Nationale de l'Informatique et des Libertés (CNIL) n'impose pas d'une façon générale, de règles ou de délais précis concernant la conservation ou l'archivage des données personnelles.

  Elle précise que les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Reprenant les principes fondateurs de la loi du 6 janvier 1978 modifiée, elle rappelle que la conservation de données doit être limitée, légitime et proportionnée à la finalité poursuivie.

  Elle rappelle également le principe du « droit à l'oubli », (art. 6-5° et 24 de la loi du 6 janvier 1978 modifiée).

  En conséquence, les données archivées sur les clients, fournisseurs ou salariés ne doivent pas être conservées, dans les Entreprises, pour des durées qui pourraient apparaître comme excessives.

  Par ailleurs, lorsque certaines données sont conservées, de façon légitime, sur de longues durées, les modalités pratiques de l'archivage doivent garantir les personnes contre, notamment, tout détournement de finalité.

- La CNIL préconise certaines durées de conservation dans quelques cas particuliers, sans toutefois que ces préconisations revêtent un caractère obligatoire.

  Pour les archives courantes (données d'utilisation courante par les services concernés dans les Entreprises comme par exemple les données concernant un client dans le cadre de l'exécution d'un contrat) et intermédiaires (données qui présentent pour les services concernés un intérêt administratif, par exemple pour les services contentieux, et dont les durées de conservation sont fixées par les règles de prescription), la CNIL précise que conformément aux articles 6-5° et 24 de la loi du 6 janvier 1978 modifiée, des durées de conservation spécifiques, proportionnées à la finalité poursuivie (par exemple durées de prescription définies par la réglementation commerciale, civile ou fiscale), doivent être indiquées dans la déclaration faite à la CNIL.

  Pour les archives définitives (données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction), elle recommande que celles-ci soient conservées sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives (par exemple la direction des archives de l'Entreprise).

  Pour les données de connexion à l'internet, elle préconise une durée de conservation de six mois. Elle considère que cela est suffisant pour dissuader les salariés de tout usage abusif d'internet[11].

  En cas d'archivage automatique des messages électroniques, les salariés doivent en outre être informés des modalités de l'archivage et de la durée de conservation des messages (CNIL Guide pratique pour les employeurs).

- D'une façon générale, la CNIL considère que le responsable de traitement devrait établir, dans le cadre de ses moyens d'archivage, des procédures aptes à gérer des durées de conservation distinctes selon les catégories de données qu'il collecte et être en mesure d'effectuer, le cas échéant, toute purge ou destruction sélective de données.
  Par exemple, elle recommande que l'accès aux archives intermédiaires soit limité à un service spécifique (par exemple un service du contentieux) et qu'il soit procédé, a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations).

- La CNIL recommande enfin, quel que soit le type d'archives, afin de garantir l'intégrité des données archivées, de mettre en œuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées, et de disposer de dispositifs de traçabilité des consultations des données archivées[12].

  Par ailleurs, si les données archivées relèvent de l'application des législations de plusieurs États (dans le cadre par exemple d'une centralisation de l'archivage d'un groupe international), il faudra concilier :

  - les législations relatives aux données personnelles de chacun des États concernés,
  - les interprétations éventuellement divergentes de ces lois par les Régulateurs nationaux de protection des données,
  - les obligations de conservation telles que mentionnées plus haut et qui peuvent être différentes selon le pays concerné (champ d'application, durée, etc.).

11 Nous renvoyons le lecteur, intéressé par ces questions du contrôle de l'usage abusif par le salarié des infrastructures mises à sa disposition par son employeur, vers le vade mecum du Forum des Compétences « la charte informatique par l'exemple » publié en février 2007.

12 Délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

#### 1.1.4.2. Sanctions du non respect de la loi informatique et libertés

**Sanctions administratives**

La CNIL dispose du pouvoir d'enquêter et d'intervenir sur place. Elle peut prononcer un avertissement à l'égard du responsable de traitement, rendu public ou non. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne.

Après une mise en demeure non respectée par le responsable de traitement, la CNIL peut prononcer à son encontre différentes sanctions : interruption du traitement, verrouillage de certaines données, sanctions pécuniaires proportionnelles à la gravité des manquements (150 000 EUR au maximum pour le premier manquement à 300 000 EUR au maximum en cas de réitération dans les cinq années suivantes).

Il faut se rappeler que toute sanction prononcée par la CNIL peut aussi entraîner un risque de réputation, lorsque ces sanctions font l'objet d'une publication.

**Sanctions pénales**

Est notamment puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende le fait de :

- mettre en œuvre des traitements de données personnelles sans respecter les formalités préalables y compris par négligence (art. 226-16 du Code pénal),
- conserver des données personnelles au-delà de la durée prévue par les textes, par la demande d'autorisation préalable ou d'avis, par la déclaration préalable adressée à la CNIL, ou hors des cas prévus par la loi, excepté si la conservation est réalisée à des fins historiques, statistiques ou scientifiques dans le respect de la loi (art. 226-20 du Code pénal).

## *1.2. CONSERVATION DES INFORMATIONS DANS UN CADRE OPÉRATIONNEL*

Comme nous l'avons vu précédemment (cf. paragraphe 1.1.1.1) l'Entreprise conserve de très nombreuses informations qui lui sont nécessaires pour exercer ou pour justifier de son activité tant à l'égard des tiers (clients, prestataires, etc.) que dans le cadre des procédures internes (contrôle interne).

Ces informations conservées par l'Entreprise sont susceptibles d'intéresser également les autorités administratives ou judiciaires dans le cadre des enquêtes qu'elles diligentent (cf. paragraphe 3.2).

Alors qu'aucun texte légal ou réglementaire n'oblige dans certains cas l'Entreprise à conserver des informations, cette dernière aura malgré tout souvent intérêt à mettre en place une politique ou procédure interne d'archivage qu'elle appliquera à tout document, afin de justifier sa bonne foi en cas de destruction de certaines informations qui pourraient être demandées par la suite (ex. de la conservation de la messagerie).

## *1.3. VALEUR AJOUTÉE DE L'ARCHIVAGE ÉLECTRONIQUE*

Le secteur bancaire reste une industrie « papivore ». En effet les établissements financiers produisent et sont amenés à conserver de manière croissante des volumes de documents importants, caractérisant les relations commerciales avec leurs clients et/ou les activités pour compte propre, en vue de satisfaire les obligations légales, réglementaires ou professionnelles et pour des durées de conservation variables.
La restitution des preuves documentaires est rendue particulièrement complexe si les documents restent au format papier, nécessitant des temps de recherches et des besoins en espaces de stockage physique en constante évolution.

L'arrivée du numérique apporte ainsi une réponse pertinente aux enjeux majeurs que nous rencontrons, à savoir :

- *identification des documents (indexation),*
- *gestion du cycle de vie du document,*
- *délais de conservation variables,*
- *partage des informations et sécurité d'accès,*
- *lisibilité, intégrité et pérennité des documents,*
- *archivage (documents dématérialisés et/ou nativement électroniques),*
- *délai de restitution / recherches,*
- *espaces de stockage,*
- *coût de conservation.*

## 1.3.1. ENVIRONNEMENT JURIDIQUE

### 1.3.1.1. L'écrit sous forme électronique - La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

La loi n° 2000-230 du 13 mars 2000[13] « portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique » a apporté une avancée considérable dans le domaine de la preuve.

Elle a modifié l'article 1316 du Code civil, donnant ainsi une nouvelle définition de l'écrit : *« 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 »*. Cette définition englobe les documents établis sur support électronique.

La loi a créé les articles 1316-1 à 1316-4 et 1317 alinéa 2 du Code civil.

L'article 1316-1 met sur le même plan, dans le domaine de la preuve (« *ad probationem* »), l'écrit sur support papier et l'écrit sous forme électronique, sous réserve, pour ce dernier :

- 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[14].

L'article 1316-3 du Code civil prévoit que « *l'écrit sur support électronique a la même force probante que l'écrit sur support papier* ».

Ainsi, un écrit sous forme électronique peut être admis comme preuve de l'existence ou l'extinction d'un droit ou d'une obligation, au même titre qu'un écrit sur support papier sous réserve de deux exigences cumulatives de l'article 1316-1 :

- l'écrit sous forme électronique doit être signé électroniquement, de façon à pouvoir lier avec certitude l'acte à un contractant nettement identifié,

- l'écrit sous forme électronique doit être archivé de façon à pouvoir garantir l'intégrité de l'acte lors de sa création et de sa conservation.

13 la loi du 13 mars 2000 a été complétée par le décret n° 2001-272 du 30 mars 2001 qui définit les exigences techniques pour établir une signature électronique fiable et par un arrêté sur l'agrément des prestataires techniques, le décret n° 2002-535 du 18 avril 2002 sur l'évaluation et la certification de la sécurité offerte par les produits et les systèmes des nouvelles technologies", un arrêté du 26 juillet 2004, et par le décret n° 2005-973 du 10 août 2005 (modifiant le décret n° 71-941 du 26 nov. 1971) relatif aux actes établis par les notaires.

14 L'article 1316-1 du Code civil dispose 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 en garantir l'intégrité ».

S'agissant de la signature électronique, elle est définie à l'article 1316-4 du Code civil ; 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'État[15].

#### 1.3.1.2. La loi pour la confiance dans l'économie numérique du 21 juin 2004

La loi n° 2004-575 du 21 juin 2004 « pour la confiance dans l'économie numérique » marque une nouvelle avancée en la matière. La loi (art. 25) a créé dans le Code civil un nouvel article 1108-1 du Code civil, qui pose le principe de l'égalité entre écrit papier et écrit électronique lorsque l'écrit est requis comme condition de validité de l'acte juridique ("ad validatem"). L'écrit même lorsqu'il est exigé pour la validité d'un acte juridique, peut être établi et conservé sous la forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 (ou à l'article 1317 al. 2 si l'acte doit être authentique).

Les définitions générales de l'écrit et de la signature adoptées dans les textes sur la preuve s'appliquent donc désormais à tout écrit quelle que soit sa fonction.
Si une mention écrite de la main même d'un contractant est exigée, celui-ci peut l'apposer sous forme électronique mais il faut pouvoir garantir que cette apposition n'a pu être effectuée que par lui-même (art. 1108-1 al. 2 du Code civil).

Rappel : la loi pose une exception : certains documents devront en tout état de cause être constitués sur support papier (art. 1108 2 du Code civil) : c'est le cas des actes sous seing privé relatifs au droit de la famille et des successions et des actes sous seing privé relatifs à des sûretés réelles ou personnelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession.

Enfin, l'article 26 de la loi pour la confiance dans l'économie numérique renvoyait à une ordonnance afin de prévoir des équivalents électroniques pour les formalités propres aux documents papiers exigées pour la conclusion, la validité ou les effets de certains contrats (lettre recommandée, formulaire détachable, etc.). C'est l'objet de l'ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique[16].

Ainsi, l'écrit qu'il soit établi à de simples fins probatoires ou qu'il soit nécessaire à la validité de l'acte peut être rédigé, signé et conservé sous forme électronique, sous réserve de répondre techniquement aux impératifs légaux et réglementaires imposés en la matière.

Rappel : pour les contrats conclus en ligne, la loi pour la confiance dans l'économie numérique de juin 2004 impose au contractant professionnel lorsqu'un contrat est conclu en ligne, d'archiver tout contrat établi sous forme électronique et portant sur une somme supérieure à 120 EUR pendant une durée de dix ans (art. L.134-2 du Code de la consommation - montant et durée fixés par le décret n°2005-137 du 16 février 2005) et de garantir à tout moment l'accès à son co-contractant si celui-ci le demande. Cette disposition, qui concerne en particulier les sites Internet de commerce électronique, vise à faciliter le règlement des litiges.

15 Décret n° 2001-272 du 30 mars 2001

16 L'**ordonnance n° 2005-674 du 16 juin 2005** restructure le chapitre VII du titre III du livre III du Code civil qui traite "Des contrats sous forme électronique" en le subdivisant en quatre sections. La section trois de ce chapitre est constituée par les articles 1369-7 à 1369-9 qui instaurent un régime propre aux lettres et aux remises d'écrit.

### 1.3.2. ENVIRONNEMENT TECHNIQUE ET NORMATIF

L'évolution des technologies du numérique depuis dix ans (Gestion Électronique des Documents (GED), Lecture/Reconnaissance Automatique des Documents (LAD/RAD), Reconnaissance Optique des Caractères (OCR)) et la baisse régulière des prix du disque informatique ont rendu attractif l'archivage électronique, parfois uniquement en complément, mais progressivement en remplacement de l'archivage physique des documents.

Le développement des activités sous forme numérique au travers de l'Internet, l'évolution du débit et la baisse du coût des lignes de communication sont des facteurs favorisant le partage et la performance d'accès aux documents numériques.

Par ailleurs l'évolution du droit français et les travaux de normalisation réalisés sur les formats électroniques des documents et les règles organisationnelles et techniques pour concevoir un Système d'Archivage Électronique (spécifications abordées dans la norme AFNOR NF Z42-013, édition 2009) en vue de conserver la valeur probante des documents stockés, permettent d'envisager la pérennité d'un tel système.

C'est pourquoi le secteur bancaire trouve dans l'archivage électronique fiable une réponse, organisationnelle et technique, pertinente à ses obligations de conservation des documents.

Aussi, il est impératif de concevoir un Système d'Archivage Électronique (SAE) particulièrement fiable pour disposer dans le temps de preuves de qualité, permettant d'envisager de ne plus conserver certains documents originaux manuscrits.

## *1.4. QUELS DOCUMENTS ARCHIVER OU DÉTRUIRE ?*

Les documents répondant à l'un ou l'autre des objectifs cités doivent être conservés (cf. paragraphe 1).

Certains documents peuvent contenir d'autres types d'informations (par ex : orientations stratégiques, événements les plus marquants pour la banque et ses filiales, etc.) Ces documents ne sont pas soumis à des règles de conservation légale ; néanmoins, avant de procéder à leur destruction, il est nécessaire de s'interroger sur leurs valeurs stratégique et historique. Certains documents justifient d'être conservés sans limitation de durée pour répondre à des objectifs qui ne sont pas nécessairement ceux définis ci-dessus (ex. préserver l'histoire de l'Entreprise).

Une politique d'archivage propre à chaque établissement, doit donc déterminer quels documents conserver, à quelles fins et pour quel usage et sur quelle durée.
La politique déterminera par ailleurs la forme de la conservation (papier et/ou numérique).

A noter : au-delà des délais légaux de conservation des documents, et sauf raison objective de conservation (archivage historique) les documents doivent être détruits (cf. paragraphe 1.1.4).

# 2. Deuxième partie : Comment archiver ? . . .

## 2.1. TRANSFORMATION DES DOCUMENTS PAPIER EN DOCUMENTS ÉLECTRONIQUES

Certains documents doivent nécessairement être établis et conservés sur support papier. C'est le cas pour :

- les actes sous seing privé relatifs au droit de la famille et des successions,
- les actes sous seing privé relatifs à des sûretés réelles ou personnelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession[17].

Par ailleurs, s'agissant des actes pour lesquels un écrit est exigé à titre de validité, la numérisation est possible mais dans ce cas la destruction de l'original pourrait faire peser un risque à l'établissement en l'absence de jurisprudence claire sur le sujet.

Pour le reste des documents, la numérisation représente une opportunité intéressante et exploitable. Ainsi la transformation des documents papier en documents numériques est l'un des enjeux majeurs du processus d'archivage électronique, dans la mesure où cette étape de transformation n'altère pas la valeur juridique du document.

En droit français, cette opération transforme un document original manuscrit en une copie numérique : à ce stade le document a changé de nature juridique. Mais l'essentiel est qu'il puisse conserver une force probante identique, en l'application des textes particuliers sur la notion de copie.

Il convient donc de déterminer les conditions / règles de numérisation et d'archivage électronique des documents papier permettant de créer un environnement de confiance renforcée dans la qualité des preuves qui en sont issues, avec pour objectif éventuel de substituer la copie numérique à l'original papier, en cohérence avec une politique de risque calculée.

A ce stade, les dispositifs techniques de numérisation sont considérés fiables et industrialisables, pour traiter des volumes papier conséquents et aux formats variables, mais impliquent des procédures d'exploitation et de contrôles rigoureuses pour apporter toute garantie de bonne exécution et de fidélité.

Les méthodes les plus couramment utilisées consistent à numériser recto/verso les originaux manuscrits, en supprimant éventuellement les pages blanches générées, et à associer à ces documents des méta-données (données structurées caractérisant le document), à l'issue de processus d'indexation (extraction/affectation des méta-données en automatique, semi-automatique ou manuel), permettant l'identification précise de chacun des documents en vue de les retrouver de manière rapide et intuitive.

## 2.2. ARCHIVAGE ÉLECTRONIQUE FIABILISÉ : PAR QUELS MOYENS TECHNIQUES ?

Pour archiver des originaux électroniques et/ou des copies numériques, obtenues par transformation des originaux papier, il convient de disposer d'un système d'archivage électronique particulièrement fiable, compte tenu des durées de conservation appliquées, pour garantir l'intégrité, la qualité et la pérennité des archives.

La mise en place d'un Système d'Archivage Électronique (SAE) fiabilisé repose généralement en France sur des recommandations décrites dans les travaux de normalisation menés par l'AFNOR (norme NF Z42-013) et d'exigences pratiques pour la maîtrise d'un tel système réalisées par la Communauté

Européenne et publiées dans le guide du MoReq (Model Requirements for the management of Electronic Records – version 2 datant de février 2008).

17 Article 1108-2 du Code civil.

Il convient donc d'identifier chaque point permettant de garantir la qualité / fiabilité du SAE et d'apporter des réponses précises expliquant les choix réalisés.

L'ensemble des exigences de nature juridique, fonctionnelle, opérationnelle et technique qu'un système d'archivage doit respecter, au sein de l'Entreprise qui le met en œuvre, sont à recenser dans le cadre d'une « **Politique d'Archivage** ».

Cette Politique d'archivage sera complétée par une présentation détaillée des procédures mises en œuvre, pour respecter les exigences définies, correspondant aux « pratiques d'archivage » retenues.

## 2.2.1. ÉLÉMENTS CONSTITUTIFS D'UN SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE (SAE)

L'objectif du SAE est de garantir l'intégrité et la lisibilité des documents numériques archivés, et d'assurer la traçabilité des opérations réalisées, durant toute leur durée de conservation.

Les documents sont soit des originaux électroniques, pour lesquels il faut assurer la stabilité du contenu informationnel, soit des documents issus d'un procédé de numérisation pour lesquels il convient de garantir la fidélité par rapport à l'original.

L'analyse des recommandations abordées dans les travaux de référence évoqués ci-dessus (norme AFNOR NF Z42-013 ou MoREQ) en matière d'archivage électronique, permet de préciser les éléments constitutifs d'un SAE.

- Éléments communs à tout système d'archivage
  - Politique d'archivage,
  - Déclaration des pratiques d'archivage,
  - Spécifications du système d'archivage,
  - Dossier description technique,
  - Procédures d'exploitation,
  - Sauvegardes.

- Éléments spécifiques
  - Supports d'archivage,
  - Processus de capture des archives,
  - Journalisation,
  - Attestations,
  - Horodatage,
  - Sécurisation,
  - Contrôles.

### *2.2.1.1. Processus de capture des archives*

Pour conserver, à titre de preuve, des copies numériques et envisager à terme, sous certaines conditions, de détruire les originaux papier, il convient de détailler les éléments qui vont apporter le niveau de sécurisation requis pour garantir la fidélité du document numérique par rapport à son original papier, et ainsi renforcer la confiance des tiers dans le SAE.

En vue de créer la version numérique la plus fidèle possible, c'est-à-dire en maîtrisant les traitements sur l'image numérisée du document (risque de dégradation de la qualité), il convient de réaliser cette capture en précisant / validant (plan de contrôle) les procédés utilisés :

- numérisation : mode (recto / verso), qualité, réglage des dispositifs,
- compression : avec ou sans (impacts sur la fidélité et le poids des images lors du stockage et/ou performance d'accès),
- traitement de l'image (risque potentiel de dégradation de la qualité) ;
  - avec ou sans suppression des pages blanches,
  - avec ou sans séparation fonds de page / données,
  - redressement, suppression des tâches et des bords,
  - conversion des images (couleur ou niveaux de gris vers noir et blanc)

Remarque : les éventuelles opérations de traitement sur l'image, telle la suppression des pages blanches et/ou de compression lors de l'enregistrement de l'archive doivent s'apprécier en fonction de critères déterminés par chaque Entreprise. Néanmoins les conditions de vérification de la fidélité par rapport à l'original papier devront être précisées en détail et réalisées de manière à conserver la confiance dans le dispositif (contrôles).

#### 2.2.1.2. Format des fichiers électroniques

Différents formats de fichiers sont utilisés pour la conservation des documents (TIFF, PDF, etc.)

L'enjeu majeur pour un SAE dans lequel les documents sont archivés à long terme est de disposer d'un format stable, sécurisé et pérenne (garantie de lisibilité dans le temps).

La normalisation des formats apporte une réponse pour leur pérennité.

L'un des formats adapté aux problématiques d'archivage est le PDF/A (Portable Document Format / Archive) normalisé ISO 19005 (PDF/A-1) qui apporte des fonctionnalités enrichies pour l'archivage mais en contrepartie implique des tailles de fichier plus importantes (lié à l'incorporation de toutes les polices de caractères nécessaires à l'affichage des textes, etc.)

Le format PDF/A a fait l'objet en 2008 de publications de l'APROGED (Association des Professionnels de la Gestion Électronique des Documents) et de la FedISA (Fédération ILM, Stockage et Archivage).

#### 2.2.1.3. Durées de conservation

Les durées de conservation doivent faire l'objet d'une analyse préalable à l'intégration de tout nouveau document dans un SAE, afin de garantir le respect des durées légales, professionnelles ou internes à l'Entreprise et des recommandations de la CNIL.

Au sein de la profession bancaire, le Comité Français d'Organisation et de Normalisation Bancaires (CFONB) a publié « La banque et les durées de conservation d'archives. Nouvelle édition – octobre 2005 », en cours d'actualisation.

L'information « *durée de conservation* », ou sa déclinaison en « *type de durée* » (ex. : court terme, etc.) est généralement identifiée dans les méta-données, associées à chaque document entrant dans le système d'archivage, permettant d'appliquer des règles de gestion cohérentes pour tous les documents ayant des durées de conservation de même nature.

#### 2.2.1.4. Méta-données

Il s'agit des données caractéristiques de chaque document d'archive, décrivant son contexte de création, le format, le contenu et les règles de gestion associées (ex : durée de conservation).

Elles visent notamment à :

- permettre l'identification et l'unicité de chaque document au sein du SAE,
- garantir l'intégrité et la stabilité du contenu informationnel durant le cycle de vie de l'archive,
- faciliter les recherches,
- assurer la gestion des accès aux documents numériques (limitation, protection, etc.).

Ces données sont alimentées durant le processus de création (ou de capture) du document numérique et parfois enrichies durant le cycle de vie de l'archive, puis stockées / sécurisées au sein du SAE.

A titre d'information, il existe un texte du comité de normalisation ISO (ISO 23081-1 :2006 Technical Specification) « *Information and documentation – Records management process – Méta-data for records* » qui traite des principes et apporte une approche guidée pour définir les meta-données en fonction des objectifs fixés par l'Entreprise.

#### 2.2.1.5. Supports de stockage

L'une des évolutions abordées dans la norme AFNOR Z42-013 (dernière version publiée en 2009) concerne les supports d'archivage garantissant la conformité du système.

En complément des supports informatiques à technologie WORM physique (Write Once Read Many) garantissant l'irréversibilité de l'enregistrement des fichiers sur le support, s'ajoutent également les supports réinscriptibles soit à technologie WORM logique (un dispositif logiciel/matériel interdit toute modification/suppression d'un enregistrement) mais surtout les supports réinscriptibles non WORM, dès lors qu'ils mettent en œuvre des procédés cryptographiques qualifiés avec trois niveaux de sécurité (standard, renforcé, avancé).

Ces procédés cryptographiques reposent sur des fonctions combinées de hachage, d'horodatage et/ou de signature électronique.

L'évolution est majeure car dans un cas (technologie WORM) c'est le support qui porte la sécurité (intégrité, pérennité) alors que dans le cas des supports réinscriptibles non WORM, la sécurité des enregistrements (l'archive et les journaux garantissant la traçabilité des opérations) est garantie par la sécurisation cryptographiques des fichiers informatiques, indépendamment de la nature du support.

#### 2.2.1.6. Traçabilité des opérations

Pour la conformité du dispositif d'archivage électronique, permettant de garantir, dans le temps, la qualité des preuves conservées, il convient de définir les conditions de traçabilité des opérations réalises sur les archives

Cela implique des règles précises concernant la journalisation des opérations qui seront enregistrées dans les journaux assurant la traçabilité :

- du cycle de vie des documents,
- des événements du système d'archivage.

**Journal de cycle de vie**

Ce journal permet de suivre le bon fonctionnement du système d'archivage électronique.

Un journal du cycle de vie stocke couramment les opérations de :

- Création d'archive,
- Suppression d'archive,
- Restitution d'une archive,
- Consultation d'une archive,
- Contrôles.

Afin de renforcer la sécurité du système, des traitements adaptés au niveau de service défini/attendu pour le SAE, doivent être mis en place pour garantir l'intégrité des journaux et assurer la traçabilité dans le temps des opérations réalisées durant le cycle de vie de l'archive.

A titre d'exemple ;

- Chaque document archivé pourrait faire l'objet d'un calcul d'empreinte (intégrité) et chaque empreinte serait alors consignée dans le journal du cycle de vie, afin notamment de vérifier l'intégrité de l'objet lors de sa consultation ou de sa restitution,
- Concernant le journal de cycle de vie, une empreinte pourrait également être calculée par fichier, enregistrée ainsi sur la première ligne du journal. La dernière ligne du journal comprendrait la date de clôture de ce dernier,
- Chaque journal serait archivé dans les mêmes conditions que les documents auxquels il se rapporte et pour une durée au moins équivalente à la durée maximale de conservation des documents,
- Chaque opération journalisée ferait l'objet d'un horodatage (certifié ou non), et pour renforcer la sécurisation du SAE, pourrait être signée au moyen d'une signature électronique avancée.

**Journal des événements**

Le journal des événements est un journal permettant de conserver des traces de l'utilisation du SAE.

Ce journal se décompose généralement en trois parties :

- les événements relatifs à l'application d'archivage,
- les événements relatifs à la sécurité,
- les événements relatifs au système.

Les traces apportent la confirmation du respect des procédures spécifiées et doivent comporter en général les informations suivantes pour chaque événement significatif :

- les dates et heures de l'opération,
- l'opération effectuée,
- l'identification du système et du processus technique utilisé,
- l'identification de l'opérateur.

Pour garantir la qualité du journal des événements archivés, il pourrait être nécessaire de tracer tous les événements au niveau applicatif, sécurité et système, afin d'assurer la maîtrise complète et la traçabilité maximale des opérations réalisées.

Néanmoins la complexité de suivi/enregistrement de l'ensemble des opérations est à mettre au regard de l'exigence défini pour le SAE ou pour le type de documents archivés (original électronique versus copie numérique stockée pour consultation et non pour preuve, par exemple).

### 2.2.2. RÈGLES D'ACCÈS ET CONFIDENTIALITÉ

L'accès aux documents stockés dans le SAE implique de respecter des règles permettant de maîtriser les risques et de garantir des délais de conservation adaptés.

L'accès aux informations archivées peut être limité par l'application du secret bancaire.

Le secret bancaire, issu de la jurisprudence relative au secret professionnel, a été formalisé par la loi bancaire du 24 janvier 1984, codifié depuis dans le Code monétaire et financier ; il est défini par les articles L. 511-33 et L. 511-34 : « *Tout membre d'un conseil d'administration et, selon le cas, d'un conseil de surveillance et toute personne qui à titre quelconque participe à la direction ou à la gestion d'un établissement de crédit (…) ou qui est employée […] est tenue au secret professionnel (…).* »

Le secret bancaire comprend à la fois l'obligation de discrétion, sanctionnée civilement, et l'obligation de respecter le secret professionnel, sanctionnée par l'article 226-13 du Code pénal[18].

La Loi de Modernisation de l'Économie[19] (LME), publiée le 5 août 2008, a modifié les contours du secret bancaire[20]. Celui-ci voit sa levée autorisée dans des cas plus nombreux, par les Entreprises de crédit. Le texte prévoit également la possibilité de transmettre des informations couvertes par le secret professionnel à des entités appartenant au même groupe que l'auteur de la communication, lors de l'étude ou de l'élaboration de tout type de contrats ou d'opérations.

Par ailleurs, la CNIL recommande notamment, pour l'ensemble des documents archivés et afin de garantir l'intégrité de ces derniers, de mettre en œuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées, et de disposer de dispositifs de traçabilité des consultations des données archivées[21].

En application de l'article 34 de la loi du 6 janvier 1978 modifiée, un responsable de traitement (c'est-à-dire la personne qui détermine les finalités et les moyens du traitement des données) doit mettre en place des mesures techniques et d'organisation appropriées pour protéger les données archivées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Le non-respect de l'obligation de sécurité peut être sanctionné par la CNIL (cf. paragraphe 1.1.4) et faire également l'objet d'une sanction pénale de cinq ans d'emprisonnement et de 300 000 EUR d'amende, soit 1 500 000 EUR d'amende pour les personnes morales telles que les Entreprises (art. 226-17 du Code pénal).

La CNIL recommande que les Entreprises définissent, dans le cadre de procédures formalisées, des règles d'archivage répondant à l'ensemble des préconisations décrites ci-dessus et qu'une information puisse être fournie sur ces règles, aux personnes physiques concernées, en cas de demande de leur part.

18 Un an d'emprisonnement et 15 000 Euros d'amende, conformément à l'art. 226-13 du Code pénal.

19 Loi n°2008-776 du 4 août 2008 de modernisation de l'économie, entrée en vigueur le 6 août 2008.

20 Article 154 de la LME.

21 Voir délibération précitée note n°12.

A titre d'exemple, comment appréhender le chiffrement du contenu d'un courrier électronique ?

Comme précisé ci-dessus, l'article 34 de la loi informatique et liberté impose au responsable de traitement d'assurer la confidentialité et la sécurité des données personnelles faisant l'objet d'un traitement.

Peu importe le vecteur par lequel passent ou sont transmises ces données personnelles. Le fait de communiquer des données via un courrier électronique constitue un tel traitement.

Les données doivent donc être suffisamment « protégées » pour ne pas être accessibles par des tiers à l'Entreprise qui ne seraient pas autorisés. Les personnes ne disposant pas d'une habilitation, ne doivent pas avoir accès à des données sans autorisation et surtout personne ne doit pouvoir utiliser des données à des fins préjudiciables. Les obligations de secret professionnel et notamment de secret bancaire applicable aux Entreprises de crédit, ne font que renforcer cette obligation et la complètent.

Une telle obligation de sécurité et de confidentialité a plusieurs conséquences : en l'absence de précisions dans le texte, c'est au responsable de traitement qu'il revient de déterminer dans les données faisant l'objet de communication celles qui seraient plus sensibles que d'autres et qui nécessiteraient alors une protection plus grande (type anonymisation, chiffrement). Il faut donc mettre en place un cadre de sécurité en interne.

Il y a sans doute lieu de distinguer, au niveau de la protection des messages électroniques, ceux qui restent internes à l'Entreprise de ceux qui sont transmis hors des systèmes internes, via l'Internet à un tiers.

## 2.3. OÙ ARCHIVER ?

### 2.3.1. ARCHIVAGE RÉALISÉ EN INTERNE

La question d'internaliser ou d'externaliser la prestation d'archivage se pose tant d'un point de vue économique, organisationnel que juridique.

Une inquiétude est parfois perçue sur le caractère probant des actes juridiques, traces ou documents électroniques conservés par une seule des parties.

Il convient de préciser quelques points majeurs afin que cette idée ne puisse perdurer :

- la règle lors de la conclusion d'acte juridique est que chaque partie en conserve par-devers elle un exemplaire afin de pouvoir les comparer en cas de procès.

- Pour autant, le législateur français a exigé en 2004, dans un but de protection du consommateur, que le cybercommerçant conserve les contrats électroniques conclus avec un consommateur, c'est-à-dire l'ensemble des exemplaires, afin que le consommateur soit déchargé de cette contrainte (cf. paragraphe 1.1.2.4). C'est dire que le législateur considère de façon indubitable que le fait pour une partie de conserver l'ensemble des exemplaires d'un contrat ne fait pas *de facto* reposer sur lui une présomption de mauvaise foi et de falsification.

- Une telle solution a également été dégagée par le législateur européen en ce qui concerne l'archivage des factures électroniques, les deux factures (émises et reçues) pouvant être conservées par la même personne[22].

Enfin, concernant le principe selon lequel « *nul ne peut se pré constituer preuve à soi-même* », il convient de modérer l'interprétation qui pourrait être tirée à tort de cet adage. Ainsi, la Cour de cassation[23] est intervenue en appliquant ce principe afin d'éviter des situations où la preuve des faits allégués contre une

22 Cf. Directive du Conseil n°2001/115 du 20 décembre 2001 dite directive « facture », dont les dispositions ont été reprises par la Directive 2006/112/CE du Conseil du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoutée.

23 Cf. Cour de cassation 11 mai 1999 (pourvoi n°97-41245), 24 septembre 2002 (pourvoi n°00-1944), 14 janvier 2003 (pourvoi n°00-22894).

partie ne reposait exclusivement que sur des éléments déclarés par l'autre partie (attestation, déclaration fiscale pour prouver la réalité d'un paiement effectué, etc.).

Mais, et le point est d'importance concernant une solution interne d'archivage électronique, la Cour de cassation a également eu l'occasion d'affirmer à plusieurs reprises[24] que des listings informatiques établis par la société qui s'en prévaut ou encore des relevés de communications téléphoniques (dans le cas de France Telecom) étaient parfaitement acceptables et bénéficiaient d'une présomption simple (de véracité des faits allégués)[25].

Pour ces raisons, au plan juridique, un système informatique permettant l'enregistrement des journaux d'activité (logs), voire l'archivage de documents électroniques, pourra être utilisé dans les contentieux et présentés par la partie qui l'a réalisé, sans risquer la censure *in fine* de la Cour de cassation. Reste que c'est la fiabilité du système informatique lui-même qui pourra être discutée par la partie à qui on oppose les enregistrements réalisés et qu'il convient en conséquence, afin de donner la plus grande force probante possible à ces enregistrements, de prévoir la possibilité de procéder à des audits, et des politiques claires et transparentes concernant l'enregistrement, le traitement, l'intégrité, la confidentialité ou encore les conditions de conservation des informations stockées.

Par ailleurs, au plan pratique, archiver en interne apparaît la solution la plus simple contractuellement parlant, car ne se posent que dans une bien moindre mesure les questions relatives à la confidentialité des données confiées à un prestataire/sous-traitant, aux transferts de responsabilité, et aux diverses obligations contractuelles qui découlent de l'externalisation, telles que, l'obligation de sécurité, le respect des modalités et délais d'accès aux documents, la réversibilité, le plan de continuité d'activité, etc.

En fonction de la nature des documents archivés, la question de savoir si l'externalisation d'une telle prestation relève du règlement CRBF 97-02 du Comité de la réglementation bancaire et financière du 21 février 1997 relatif au contrôle interne des Entreprises de crédit et des Entreprises d'investissement devra également être posée.

En tout état de cause, l'établissement souhaitant mener à bien en interne un projet d'archivage doit s'assurer notamment de la fidélité, de la durabilité, de l'intégrité et de l'identification des archives. Par ailleurs, il devra le cas échéant déclarer le traitement auprès de la CNIL, créer et faire respecter des procédures d'accès, assurer le respect par son personnel des règles de confidentialité, de sécurité etc.

Enfin, lorsque l'Entreprise envisage de confier la prestation d'archivage auprès d'une entité de son groupe hors de l'Union Européenne, il devra veiller tout particulièrement à respecter les réglementations en vigueur, tant celles du pays d'accueil que celles du pays émetteur (secret bancaire, données personnelles, etc.).

### 2.3.2. ARCHIVAGE EXTERNALISÉ AUPRÈS D'UN PRESTATAIRE TIERS

L'Entreprise a toujours la faculté de recourir à l'externalisation de tout ou partie de l'archivage de ses données. Les motivations peuvent être tant économiques que techniques. En tout état de cause, la responsabilité de l'Entreprise quant à l'intégrité et la sécurité de ses archives reste entière, que l'archivage soit effectué en France ou à l'étranger.

En effet, l'article 35 de la loi du 6 janvier 1978 modifiée dispose que le responsable du traitement, lorsque l'archivage est effectué pour son compte par un prestataire / sous-traitant, doit s'assurer que ce dernier

24 Cf. Cour de cassation 28 janvier 2003 (pourvoi n°00-17553, concernant les relevés de communications téléphoniques de France Telecom), 13 juillet 2004 (pourvoi n°01-11729, concernant le listing informatique des opérations d'enregistrement d'Air France).

25 Ainsi, pour le Professeur Pierre Stoffel-Munck, dans le cas par exemple de contrats de fourniture en libre-service, de paiement par mesure de la consommation ou de mesure effectuée par le fournisseur lui-même mais de façon automatisée, les enregistrements, du fait de cetautomatisation et de la réalisation par une machine « a priori » impartiale, pourront valoir comme présomption simple.

présente des garanties suffisantes en matière de sécurité technique, de confidentialité et d'organisation relatives aux traitements à effectuer.

Dans le cadre de cette prestation/sous-traitance de l'archivage, un contrat doit lier le responsable de traitement au prestataire/sous-traitant et prévoir notamment que le prestataire/sous-traitant n'agit que sur

la seule instruction du responsable de traitement et que des obligations en matière de sécurité et de confidentialité lui incombent également.

La question de l'intelligence économique et des risques pour l'Entreprise d'héberger ses données à l'étranger par exemple, doit être abordée[26]. Ainsi, il est important de noter qu'un grand nombre de législations nationales permettent aux États de donner accès à ses forces de l'ordre à l'ensemble des données informatisées stockées sur son sol et ce pour des motifs qui ont tendance à être élargis avec le temps (enquêtes dans le cadre de délit commis ou avéré, simple suspicion de terrorisme aux États-Unis, etc.).

#### 2.3.2.1. En France

Si une Entreprise confie tout ou partie de son archivage à un prestataire/sous-traitant externe, il transfère la réalisation de la réception, la conservation et la restitution de documents à une autre société, tout en conservant pleinement la responsabilité juridique de l'opération vis-à-vis de ses clients et des tiers.

Comme l'activité de tiers archiveur ne fait pas l'objet de réglementation spécifique, sauf en matière d'archives publiques[27] les conditions de l'externalisation de l'archivage reposeront uniquement sur le contrat entre l'Entreprise et son prestataire/sous-traitant.
L'archivage étant une fonction importante, voire sensible, le choix du prestataire/sous-traitant devra être conduit avec prudence, à la lumière de son expérience, de sa solidité, et des garanties qu'il est en mesure d'apporter à ses clients.

Le projet d'externalisation d'archivage pourra donc être conduit avec la méthodologie de conduite de grand projet. La contractualisation établira les conditions juridiques et techniques de l'archivage et notamment les obligations du prestataire/sous-traitant pour assurer la fidélité, la durabilité, l'intégrité et l'identification des archives.

Les clauses les plus sensibles portent sur la responsabilité du prestataire/sous-traitant, les conditions de sécurité et de réversibilité. Il peut être souhaitable que le prestataire/sous-traitant s'engage à une obligation de résultat, plutôt que de moyens, c'est-à-dire qu'il assume la charge de la preuve, en cas de faute présumée.

#### 2.3.2.2. Dans un autre pays

L'Entreprise s'assurera de la localisation de l'archivage externalisé. L'archivage dans un pays étranger peut générer des risques particuliers.

Le risque « pays » sera examiné en fonction des conditions climatiques, politiques, etc. De même, l'aspect législatif et réglementaire devra faire l'objet d'une analyse de risque, à savoir l'application de normes locales peuvent-elles avoir un effet sur l'archivage ? Le transfert de données à l'étranger génère-t-il des obligations particulières pour l'Entreprise ? Les données seront-elles accessibles aux autorités administratives et judiciaires locales ?

26 Cf. Guide précité à la note n° 2.

27 Loi du 15 juillet 2008 relatif aux archives.

Une Entreprise située en France devra veiller au respect de la loi du 6 janvier 1978 modifiée (qui reprend les principes établis par Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données).

Dès lors que des archives contenant des données personnelles sont confiées à un prestataire/sous-traitant et font l'objet d'un transfert en dehors de la France, le régime est différent selon qu'on se situe dans l'Union Européenne (UE) ou hors UE :

- le transfert d'archive de la France vers un pays de l'UE doit faire l'objet d'une simple déclaration à la CNIL,
- le transfert international d'archive hors UE ou hors des pays dont la Commission Européenne a jugé la protection « adéquate »[28] doit faire l'objet d'une demande d'autorisation auprès de la CNIL. Par ailleurs, doivent être insérées dans les contrats de prestation de service des clauses ad hoc rédigées par la Commission Européenne qui ont pour objectif d'encadrer les transferts de données nominatives de responsables de traitement à sous-traitants (ou de responsable de traitement à responsable de traitement) en permettant de considérer que ce transfert se fait en offrant des garanties suffisantes au regard de la protection de la vie privée, des libertés et des droits fondamentaux des personnes ainsi qu'à l'égard de l'exercice de ces droits.

Ces clauses prévoient notamment un grand nombre d'exigences en matière de sécurité et de confidentialité. En outre, une information des personnes doit être envisagée.

En dehors des pays membres de l'UE, seuls quelques pays sont considérés par la Commission Européenne comme offrant une protection « adéquate » des données ce qui implique que le transfert des données vers ces pays ne nécessite pas de formalisme autre que de déclarer ce transfert dans la déclaration d'activité française[28].
Mis à part ces pays, la loi française impose donc que les transferts de données personnelles hors UE, obéissent à différentes obligations.

Les États-Unis constituent une exception du fait des principes internationaux de protection des données au sein du Safe Harbor (sphère de sécurité) : seuls les prestataires/sous-traitants ou les Entreprises ayant adhéré aux principes de « Safe Harbor » auprès de la Federal Trade Commission seront considérés comme « adéquats » au niveau de la protection des données et il ne sera pas nécessaire de demander une autorisation à la CNIL.

Quelque soit la nature des données personnelles communiquées au prestataire/sous-traitant installé hors Union Européenne, il faut que les raisons d'un tel transfert soient légitimes et proportionnées à l'activité envisagée. Doit être mis en place un *process* de sécurité et de confidentialité ainsi que des habilitations ou juridictions d'accès.

Dans tous les pays, la réglementation nationale applicable aux données personnelles dépendra du lieu de traitement (au sens de la directive européenne : collecte, stockage, accès, etc.). Le responsable du traitement devra se conformer à la législation nationale de chaque territoire concerné.

28 cf. supra. Pour une liste des pays, se référer au site internet de la CNIL : http://www.cnil.fr/index.php?id=1154

L'archivage des documents a pour objectif essentiel, de permettre, en cas de besoin, l'accès à leur contenu, durant la période prévue. L'accès peut être nécessaire pour les archives courantes, intermédiaires ou définitives. L'accès permet de consulter l'information, la contrôler, la transmettre ou de l'utiliser à des fins probatoires.

Les archives contiennent des documents qui représentent une partie du patrimoine informationnel de l'Entreprise, un actif à protéger. Certaines informations peuvent être précieuses, avoir une valeur probante et/ou être confidentielles. Certaines informations sont des données à caractère personnel, car elles concernent des clients, des fournisseurs ou des salariés, et sont soumises à la réglementation relative à l'informatique et aux libertés (cf. paragraphe 1.1.4). D'autres informations, enfin, font l'objet de droits de propriété intellectuelle, au profit de l'Entreprise ou de tiers.

Afin préserver la sécurité du système d'archivage et le respect des droits, l'accès aux documents, aux traces et aux pièces jointes est nécessairement encadré par des procédures.
Pour les accès internes, c'est-à-dire par les membres de l'Entreprise, les procédures sont élaborées par les instances internes de l'Entreprise (cf. paragraphe 3.1.1), et selon des limites prévues par la réglementation (cf. paragraphe 3.1.2).

Pour les accès externes, l'accès aux informations de l'Entreprise, ne sera possible, qu'avec l'accord de celle-ci, ou dans le strict respect des procédures judiciaires et administratives.

## 3.1. ACCÈS INTERNE

### 3.1.1. MODALITÉS D'ACCÈS

#### 3.1.1.1. Utilisateurs

Les utilisateurs des systèmes d'information sont susceptibles d'avoir accès aux archives, pour les consulter, les extraire, les modifier et/ou les diffuser.

Afin de protéger le contenu des archives, et les droits des personnes concernées, les accès aux archives doivent faire l'objet de procédures sécurisées, adaptées au niveau de sécurité attendu. Les moyens sécuritaires seront adaptés à la politique de sécurité mise en œuvre pour l'archivage : procédure, suivi, gestion des habilitations, des traces, chiffrement, contrôle, audit, etc.

L'accès aux données archivées par les utilisateurs sera délimité aux actions nécessaires, et encadré par des règles de procédure interne claires, et formalisées dans le règlement intérieur, une charte d'usage des systèmes d'information et/ou une procédure spécifique, engagements de confidentialité.

Au-delà de la formalisation de ces règles, il est naturellement indispensable que les personnes soient informées et formées à l'utilisation de l'outil.

#### 3.1.1.2. Administrateurs

Les administrateurs du système d'information (administrateurs d'archivage de messagerie, de sécurité, de réseaux, etc.) représentent une population spécifique, et disposent, de par leur fonction, d'accès étendu aux données. Ils gèrent le système et participent à la vie de toute application, y compris celle d'archivage : installation, tests, gestion des habilitations, suivi, maintenance et assistance aux utilisateurs.

Les administrateurs peuvent accéder à certaines données archivées non seulement à l'occasion d'opérations courantes de la gestion de l'archivage, mais peuvent être amenés à assister

d'autres collaborateurs de la banque, lors de procédures d'accès spécifiques aux archives (audit, procédures administratives ou judiciaires, etc.).

L'accès aux données archivées par les administrateurs doit être restreint aux actions propres à leur mission, et encadré par des règles de procédure interne claires. Au-delà de la formalisation de ces règles, il est important que les administrateurs soient formés à l'utilisation des outils à leur disposition et au caractère sensible de leur mission.

Si les administrateurs intervenant dans les locaux de l'Entreprise sont des prestataires externes, des règles similaires de sécurité et de confidentialité doivent se trouver dans le contrat de prestation établi avec l'Entreprise qui les emploie, afin de formaliser les obligations de chaque partie.

#### 3.1.1.3. Auditeurs et contrôleurs internes

Les différents corps d'audit et de contrôle de l'Entreprise doivent pouvoir accéder aux données archivées, dans le cadre de leur mission. Dans les établissements financiers, cet accès s'applique aux fonctions d'inspection. La motivation de l'accès est double : prendre connaissance des documents archivés et des traces d'accès à ces documents.

L'accès aux données archivées par les auditeurs et contrôleurs doit être adapté aux actions propres à leur mission, et encadré, comme pour les autres acteurs, par des règles de procédure interne claires. Les procédures d'accès et d'analyse peuvent être manuelles ou automatisées par des outils logiciels, qui permettront de faciliter les tâches de recherche et de conserver les traces des recherches.

Si les auditeurs et contrôleurs intervenant dans les locaux de l'Entreprise sont des prestataires externes (auditeur externe, commissaire aux comptes, etc.), au-delà de leur déontologie professionnelle, des règles de sécurité et de confidentialité doivent se trouver dans le contrat de prestation, afin de sécuriser l'Entreprise et de lui permettre de mettre en œuvre la responsabilité de son prestataire, en cas de non-respect.

#### 3.1.1.4. Personnes concernées par les données

Les personnes physiques disposent de droits sur les données personnelles qui les concernent (droits issus de la loi n°78-17 du 6 janvier 1978 modifiée) : droit d'accès (art. 39 ) et de rectification (art. 40) et droit d'opposition (art. 38) – (cf. paragraphe 3.1.2.2).

### 3.1.2. LIMITATIONS D'ACCÈS

#### 3.1.2.1. Muraille de Chine

L'expression « muraille de Chine » est utilisée dans l'organisation bancaire. Elle signifie l'obligation, pour l'établissement, de mettre en œuvre une séparation organisationnelle et matérielle entre les activités de financement ou de conseil et les activités d'analyse financière, de vente et de trading intervenant sur les marchés d'instruments financiers. L'activité du prestataire de services d'investissement le conduit à avoir connaissance d'informations confidentielles ou privilégiées qui, si elles étaient rendues publiques, seraient susceptibles d'avoir une influence sensible sur le cours des instruments financiers concernés ou qui leur sont liés. Le Règlement général de l'AMF[29] impose au professionnel de prévoir des procédures visant à éviter la circulation indue de ce type d'information.

29 Art 315-15 du Règlement Général de l'AMF.

En pratique, le « côté public de la muraille de Chine » concerne les personnes *« ayant connaissance d'ordres dont l'exécution est susceptible d'avoir une influence sensible sur le cours des instruments financiers concernés et le cours d'instruments financiers qui leur sont liés »*. Ces personnes sont détentrices d'informations privilégiées sur de courtes durées. Le « côté privé de la muraille de Chine » inclut notamment les fonctions de fusion-acquisition, de financement, de gestion de portefeuille et de conseil.

Certains collaborateurs de la banque sont identifiés comme étant placés de manière permanente au dessus de la muraille de Chine (membres du comité de direction, fonctions juridiques, risque, contrôle permanent, etc.).

Dans le but d'assurer la protection de ces informations confidentielles ou privilégiées, cette muraille de Chine devra se retrouver dans la gestion et l'organisation des archives.

### *3.1.2.2. Préconisations de la CNIL*

**Modalités d'accès dans les Entreprises**

Comme nous l'avons déjà dit, le responsable de traitement, en application de l'article 34 de la loi du 6 janvier 1978 modifiée doit mettre en œuvre des mesures techniques et d'organisation appropriées pour protéger les données archivées notamment contre la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite.

De telles mesures doivent permettre d'assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

La CNIL recommande notamment que l'accès aux archives intermédiaires (cf. paragraphe 1.1.4) soit limité à un service spécifique (par exemple un service du contentieux) et qu'il soit procédé, a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations).

Elle recommande également que les archives définitives (cf. paragraphe 1.1.4) soient conservées sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives, par exemple la direction des archives de l'Entreprise.

Elle recommande enfin de mettre en œuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées ainsi que de mettre en œuvre des dispositifs de traçabilité des consultations des données archivées.

Elle préconise également d'utiliser des procédés d'anonymisation en cas de conservation à long terme de documents d'archives, notamment pour les données sensibles.

**Droit d'accès des personnes**

Les archives courantes et intermédiaires sont soumises au droit d'accès des personnes en application de l'article 39-I-4° de la loi du 6 janvier 1978 modifiée.

Le responsable de traitement doit, par conséquent, prévoir la possibilité d'une demande de droit d'accès aux données archivées et doit être en mesure d'y répondre favorablement.
L'article 39 II de la loi du 6 janvier 1978 modifiée admet un tempérament selon lequel les dispositions de cet article ne s'appliquent pas lorsque les données personnelles *« sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des*

*personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique* ». De telles dérogations doivent être mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la CNIL.

Concernant le traitement des archives définitives dans le but d'assurer la conservation à long terme de documents d'archives, le responsable du traitement n'est pas tenu de donner suite aux demandes de droit d'accès concernant les informations archivées et n'a pas à le notifier préalablement à la CNIL.

Néanmoins le responsable de traitement doit, dans ce cas, être en mesure de justifier que les moyens d'archivage employés sont de nature à exclure manifestement tout risque d'atteinte à la vie privée des personnes concernées.

C'est la raison pour laquelle la CNIL recommande d'utiliser, en particulier en cas de données sensibles, des procédés d'anonymisation.

## 3.2. ACCÈS EXTERNE - MODALITÉS D'ACCÈS

### 3.2.1. PROCÉDURES ADMINISTRATIVES ET JUDICIAIRES FRANÇAISES

Les entreprises sont soumises, en France, à différentes procédures administratives et judiciaires. Les exemples suivants, non exhaustifs, visent à donner quelques indications permettant à l'entreprise d'anticiper l'accès aux documents archivés dans ce cadre, et d'intégrer cette dimension dans sa politique d'archivage. Ces présentations succinctes sont complétées par des tableaux figurant en annexe IV.

#### 3.2.1.1. La DGCCRF

**Pouvoirs en matière de concurrence**

***Enquête simple de la DGCCRF***

Les enquêteurs peuvent demander la communication des livres, factures et tous autres documents professionnels et en obtenir ou en prendre copie par tous moyens et sur tous supports (art. L.450-3 du Code de commerce).

Dans le cadre d'une enquête simple, les enquêteurs n'ont pas de droit de saisie et ne peuvent que consulter les documents ou en prendre copie. La demande des enquêteurs doit être précise et ciblée. Une entrave à l'enquête est constitutive d'un délit correctionnel (art. L.450-8 du Code de commerce).

***Enquête lourde de la DGCCRF avec visite et saisie***

Cette enquête a lieu sur autorisation judiciaire rendue par ordonnance du Juge des libertés et de la détention (JLD) du Tribunal de grande instance (TGI) du lieu de visite (art. L.450-4 du Code de Commerce). Les enquêteurs doivent notifier l'ordonnance du Juge des libertés et de la détention (JLD) autorisant la perquisition.

Dans ce cas, les enquêteurs ont le droit de rechercher et peuvent saisir tous documents utiles à leur enquête.

Les enquêteurs doivent notifier l'ordonnance du Juge des libertés et de la détention (JLD) autorisant la perquisition. Pour ce qui est de la messagerie, ils peuvent accéder à l'intégralité des messages et saisir tous documents. L'enquêté peut prendre copie des documents saisis. Si des saisies lui paraissent litigieuses, il peut noter des réserves dans le PV de fin de visite.

**Pouvoirs en matière de réglementation de la consommation**

*Contrôle de la conformité des produits et services*

Les agents peuvent exiger la communication et obtenir ou prendre copie par tous moyens et sur tous supports ou procéder à la copie des documents de toute nature, entre quelques mains qu'ils se trouvent. Ils ont accès aux logiciels et aux données stockées.

Les enquêteurs peuvent exiger communication de documents et les saisir « *en quelques mains qu'ils se trouvent* ». Faire obstacle à la DGCCRF est sanctionné par l'article L.217-10 du Code de la consommation.

### 3.2.1.2. La HALDE

#### Demande de communication de documents

La HALDE[30] peut demander dans le cadre formel de l'enquête, communication de tous documents quel qu'en soit le support, nécessaires à apprécier la situation.

Dans l'exercice de ce droit de communication, les demandes de la HALDE sont assez larges, puisque les documents demandés ont pour but d'effectuer des comparaisons afin de savoir s'il existe des discriminations.

Les personnes soumises au secret professionnel ne peuvent être poursuivies pour les informations à caractère secret qu'elles auraient pu révéler à la Haute Autorité.

En cas de refus de collaborer, la HALDE peut saisir le juge des référés afin qu'il ordonne toute mesure d'instruction qu'il estime utile pour la poursuite de l'enquête.

#### Les vérifications sur place

Les vérifications sur place ne peuvent avoir lieu que dans les locaux exclusivement consacrés à un usage professionnel et sous réserve d'obtenir au préalable l'accord de la personne contrôlée.

Seuls les agents de la HALDE ayant reçu une habilitation spécifique du procureur général de la Cour d'appel peuvent procéder à ces vérifications.

A l'occasion de ces vérifications sur place, les agents de la HALDE peuvent entendre toutes personnes susceptibles de fournir des informations.

La HALDE n'a pas le pouvoir d'effectuer les recherches et ne peut avoir accès à la messagerie d'un salarié.

### 3.2.1.3. L'AMF

Le secret professionnel ne peut être opposé à l'AMF (art. L.621-9-3 du Code monétaire et financier).

Les obstacles au bon déroulement d'une mission de contrôle ou d'enquête sont constitutifs d'un délit sanctionné pénalement (art. L.642-2 du Code monétaire et financier).

#### Communication de documents

L'AMF peut se faire communiquer tous documents nécessaires à l'enquête, quel qu'en soit le support et en obtenir copie.

30 Haute Autorité de Lutte contre les Discriminations et pour l'Egalité, cf. loi du 30 décembre 2004.

**Vérifications sur place**

Les agents de l'AMF peuvent accéder aux locaux professionnels.

L'AMF n'a pas le pouvoir de consulter ni de saisir d'office les documents, mais seulement d'en demander copie s'ils lui paraissent utiles pour la poursuite de son enquête. Les agents de l'AMF n'ont pas accès à l'ensemble de la messagerie d'un salarié.

#### *3.2.1.4. La Commission bancaire*

La Commission bancaire contrôle le respect des dispositions législatives et réglementaires par les Entreprises de crédit et les Entreprises d'investissement.

Le secret professionnel ne peut être opposé à la Commission bancaire (art. L.511-33 du Code monétaire et financier). Le fait d'entraver la mission de contrôle de la Commission bancaire est sanctionné pénalement.

**Le contrôle sur pièces**

La Commission bancaire peut demander aux personnes soumises à son contrôle tous renseignements, documents quel qu'en soit le support et en obtenir copie. Elle peut demander les rapports des Commissaires aux comptes et de manière générale tous documents comptables.

**Le contrôle sur place**

La Commission bancaire peut procéder à des interrogatoires et se faire communiquer tous documents nécessaires à l'enquête. Les contrôles peuvent être étendus aux filiales d'un établissement financier.

Comme la HALDE et l'AMF, la Commission bancaire ne dispose pas d'un droit de perquisition. Elle demande communication des documents et prend copie de ceux qu'elle estime nécessaire pour l'accomplissement de sa mission. La Commission bancaire ne peut donc accéder à l'intégralité de la messagerie d'un salarié.

#### *3.2.1.5. La CNIL*

Les agents de la CNIL peuvent avoir accès aux locaux professionnels. Ils peuvent, en application de l'article 11 2° f) de la loi du 6 janvier 1978 modifiée, demander « *communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Les membres de la délégation peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle* ».

Dans le cadre de leur mission, les agents de la CNIL ne peuvent rechercher des informations sur la messagerie d'un salarié de l'Entreprise.

Selon l'article 11 2° f), ils doivent avant tout « *procéder à des vérifications sur tout traitement* ». Ils vérifient si les traitements de données personnelles mis en œuvre dans l'Entreprise ont bien été déclarés et sont conformes à la loi du 6 janvier 1978 modifiée.

Durant l'inspection, il convient de prendre toutes mesures utiles afin de faciliter la mission de la CNIL. Le responsable du traitement peut être puni d'un an d'emprisonnement et de 15 000 EUR d'amende en cas d'entrave à l'action de la CNIL (art. 51 de la loi informatique et libertés du 6 janvier 1978 modifiée).

Toutefois, conformément à l'article 21 de la loi « *sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées par la CNIL sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions* ». La CNIL peut donc se voir opposer le secret bancaire.

#### *3.2.1.6. Les Douanes*

En vue de la recherche de la fraude, les agents des Douanes disposent « de pouvoirs de visite » des personnes, des locaux et des biens, ainsi que des droits de communication. Ces droits s'exercent sur l'ensemble du territoire national.

**Droit de visite**

Les agents des Douanes peuvent exercer un droit de visite sur les marchandises et les moyens de transport ainsi que sur les personnes, sans que ces dernières ne puissent à cette occasion être retenues contre leur gré, ni faire l'objet d'aucune mesure coercitive.

Les agents des Douanes peuvent accéder aux locaux et lieux à usage professionnel, ainsi qu'aux moyens de transport à usage professionnel et à leur chargement, si des marchandises ou documents se rapportant à des infractions au Code des Douanes sont susceptibles d'y être détenus. Au cours du contrôle les agents des Douanes peuvent retenir des documents ou en prendre copie.

Lors d'un contrôle, les agents des Douanes pourront avoir accès au disque dur d'un portable et donc à une messagerie électronique. Dans ce sens, la Douane a été autorisée à « fouiller » et saisir un agenda (C. cass. Crim. 18 avril 1988).

Les agents des Douanes doivent être autorisés par ordonnance du Juge des libertés et de la détention (JLD) à procéder à des perquisitions et saisies en tous lieux, même privés, où des marchandises ou des documents se rapportant à des délits douaniers ou des infractions à la législation sur les relations financières avec l'étranger sont susceptibles d'être détenus (art.64 du Code des Douanes). En cas de flagrant délit, ils peuvent procéder directement à la perquisition.

**Droit de communication**

Les agents des Douanes peuvent exiger la communication de documents de toute nature et sur tous supports (comptabilité, factures, compte en banque…,etc.) relatifs à leur mission, sans que le secret bancaire ne puisse leur être opposé. Le droit de communication s'exerce sur les documents pendant trois ans (art. 65 du Code des Douanes).

#### *3.2.1.7. Les Autorités fiscales*

**Droit de communication de l'Administration fiscale**

L'Administration fiscale dispose d'un droit de communication (sur place ou par correspondance) sur tous documents comptables, contrats, relevés de comptes, bordereaux de remises de valeurs, documents de service, quel qu'en soit le support.

Ce droit de communication s'exerce sur les documents professionnels pendant six ans (art. L.102 B du Livre des Procédures Fiscales).

Si ces documents sont établis ou reçus sur support informatique, ils doivent être conservés pour une durée d'au moins trois ans. Les contrats de fiducie doivent être conservés pendant dix ans.

**Pouvoir de perquisition**

En cas de présomption de fraude, l'Administration fiscale peut, par ordonnance du Juge des libertés et de la détention (JLD) qui fixe les limites de la mission des agents de l'Administration fiscale procéder à des perquisitions en tous lieux, mêmes privés, de toutes pièces ou documents, et procéder à leur saisie quel qu'en soit le support. L'Entreprise est alors déliée de son obligation au secret professionnel.

Cette procédure ne s'applique que pour la recherche d'infractions aux impôts directs et à la T.V.A. Dans le cadre de cette procédure, les agents de l'Administration fiscale peuvent accéder à l'ensemble de la messagerie d'un salarié de l'Entreprise.

### *3.2.1.8. Les Autorités judiciaires*

**Enquête de flagrance (art.53 et suivants du Code de procédure pénale)**

Elle concerne les crimes et délits qui sont en train de se commettre ou qui viennent de l'être (bref délai). Les opérations menées dans le cadre de l'enquête de flagrance ne peuvent excéder huit jours, période pouvant être renouvelée une fois par le Procureur de la République lorsque l'infraction en cause est punissable de plus de cinq ans d'emprisonnement et que des éléments nécessaires à l'enquête le justifient. Les diligences menées par les officiers de police judiciaires lors de l'enquête s'imposent à toutes personnes pouvant contribuer à l'établissement de la vérité.

Les perquisitions et saisies sont possibles sans l'accord des personnes intéressées par les faits poursuivis. L'officier de police judiciaire a seul le droit de prendre connaissance des documents et a l'obligation de mettre en place toutes mesures utiles pour assurer le respect du secret professionnel et des droits de la défense, c'est-à-dire de veiller à ce que la perquisition et la saisie ne concernent que les faits poursuivis.

**Enquête préliminaire (art. 75 et suivants du Code de procédure pénale)**

L'enquête préliminaire permet de rassembler les preuves sans mettre en œuvre l'instruction. Elle est décidée par les officiers de police judiciaires, soit d'office, soit sur instruction du procureur de la République. En enquête préliminaire, l'officier de police judiciaire ne peut requérir les documents ou informations couverts par le secret professionnel qu'avec l'autorisation du Parquet (art. 77-1-1 du Code de procédure pénal). Le secret professionnel peut toujours être opposé aux officiers de police judiciaires qui agissent d'office (ces enquêtes peuvent durer jusqu'à six mois sans qu'ils rendent compte au Parquet ; art.75-1 du Code de procédure pénal). L'absence de réponse est punissable d'une amende de 3 750 EUR.

**Commission rogatoire du juge d'instruction (art. 151 du Code de procédure pénale)**

Le juge d'instruction lorsqu'il est saisi pour des faits dénommés, fixés par le Procureur de la République dans son réquisitoire introductif peut mener l'enquête seul mais le plus souvent, il agit par commissions rogatoires. Les commissions rogatoires sont des délégations de pouvoirs octroyées à un autre magistrat ou à un officier de police judiciaire. Elles doivent indiquer la nature de l'infraction recherchée et être signées du juge et ne peuvent prescrire que des actes d'instruction se rattachant aux faits qui y sont visés.

Elles lèvent le secret bancaire en application de l'article 511-23 du Code monétaire et financier aux termes duquel « *il ne peut être opposé à l'autorité judiciaire agissant dans le cadre d'une procédure pénale* ». La police judiciaire ayant reçu délégation de l'autorité judiciaire par la commission rogatoire peut donc obtenir des informations, renseignements et documents couverts par le secret bancaire dans la limite des faits visés dans la commission rogatoire.

Elles lèvent le secret bancaire en application de l'article 511-23 du Code monétaire et financier aux termes duquel « *il ne peut être opposé à l'autorité judiciaire agissant dans le cadre d'une procédure pénale* ». La police judiciaire ayant reçu délégation de l'autorité judiciaire par la commission rogatoire peut donc obtenir des informations, renseignements et documents couverts par le secret bancaire dans la limite des faits visés dans la commission rogatoire.

**Réquisitions électroniques**

Ces réquisitions s'effectuent sur demande d'un officier de police judiciaire sur présentation d'un procès verbal. Le secret professionnel leur est opposable (art. 60-2 1er alinéa du Code de procédure pénale). Toutefois, le fait de refuser sans motifs légitime est sanctionné par une amende prévue au 4e alinéa de l'article 60-2 du Code de procédure pénale.

Les informations sollicitées sont mises à disposition de l'officier de police judiciaire au moyen d'un ficher spécifique ou par accès temporaire et limité à la base de données de la personne morale contrôlée.

Dans le cadre de cette procédure, l'officier de police judiciaire ne peut avoir directement accès à la messagerie d'un salarié.

**La saisie-contrefaçon**

Les commissaires de police, à la demande de tout auteur d'une œuvre protégée peuvent saisir les reproductions illicites d'une œuvre. Un huissier de justice peut également procéder à une saisie-contrefaçon sur ordonnance du président du Tribunal de grande instance (TGI) du lieu de la contrefaçon.

Il peut y avoir accès indirect à une messagerie si la contrefaçon porte sur un logiciel de messagerie : il y a alors saisie dudit logiciel de messagerie.

### 3.2.2. PROCÉDURES JUDICIAIRES ET ADMINISTRATIVES ÉTRANGÈRES

Les Entreprises françaises doivent faire face à des procédures administratives ou judiciaires émanant d'autorités étrangères, notamment lorsqu'elles ont des activités commerciales dans certains pays, (par exemple *Common law*).

Dans le cadre de procédures sur la constitution de preuves électroniques, les autorités étrangères sont susceptibles de demander à des Entreprises françaises de produire un certain nombre de documents électroniques. Dans les pays de *Common law*, les preuves destinées à être produites devant la justice civile ou administrative sont collectées par les parties elles-mêmes et non recueillies, comme en droit français par une autorité publique, dirigée ou contrôlée par le juge. Pendant une phase préparatoire portant le nom de *pre-trial discovery*, les parties peuvent saisir le juge pour contraindre l'autre partie, ou un tiers, à leur livrer des informations. Comme la communication d'informations électroniques, dans le cadre des procédures internationales, représente un coût important, du temps passé et des risques de divulgation des informations privilégiées, confidentielles ou protégées par d'autres textes, nous recommandons de traiter ces demandes avec prudence et de les transmettre aux services internes compétents (Direction Juridique, Direction de la Déontologie, etc.).

L'administration d'éléments de preuve sur support électronique ne représente plus un phénomène exceptionnel dans le cadre de litiges commerciaux internationaux, comme une majorité d'informations sont désormais sur support électronique.

Aujourd'hui, les concepts de *discovery,* ou de *disclosure* en Angleterre, désignent le processus consistant à satisfaire une demande légale de production de messages électroniques archivés et d'autres éléments : traces de connexion, outils d'archivage et d'accès, etc.

**Quelques exemples de procédures étrangères**

Aux Etats-Unis, les règles relatives au processus de discovery sont issues de la procédure civile fédérale[31] et du Code Fédéral de la preuve[32]. Selon ces règles, lors de la *pre-trial discovery* , les parties doivent communiquer à leur adversaire toutes les pièces qui sont utiles au soutien de leur demande. Il ressort de la jurisprudence[33] qu'une partie a l'obligation de préserver les preuves potentielles lorsqu'elle a connaissance qu'un procès lui est intenté *(litigation hold).*

Le dispositif de la procédure civile fédérale a fait l'objet d'une réforme en 2006, pour permettre aux parties d'échanger quant aux problématiques de préservation des informations, notamment au coût de la *e-discovery*, à sa durée et au caractère confidentiel[34] de l'information comme moyen de défense. Par ailleurs, l'accessibilité des preuves électroniques est prise en compte par ces récents amendements. En effet, si les sources ne sont pas « raisonnablement accessibles », elles n'ont pas à être produites, à moins que la partie qui est à l'origine de la requête prouve qu'elle est fondée[35]. Il existe d'autres limites à la production des documents : les correspondances avocats-clients et certains avis d'experts.

En Grande-Bretagne, il existe une procédure similaire, désignée sous le terme de *disclosure*[36], qui requiert d'une partie de divulguer à la partie adverse tous les éléments pertinents de preuve dont elle dispose, au cours de l'instruction d'une affaire. Plusieurs restrictions[37] s'appliquent à la communication d'informations : lorsque la production de document risque de porter atteinte à l'ordre public ou aux informations protégées par le secret professionnel, lorsque la pièce ne se trouve plus sous le contrôle d'une partie et lorsque l'accès demandé est disproportionné, par rapport à la demande.

Au Canada, ce sont diverses normes fédérales et provinciales qui réglementent l'administration de la preuve. Il en ressort qu'elles prévoient toutes une obligation de communiquer les documents pertinents, sauf au Québec qui est civiliste.

Dans tous les cas, il sera nécessaire d'examiner les critères de recherches (période, sujets, destinataires, émetteurs, etc.) en perspective avec le litige, de prendre des mesures techniques, organisationnelles voire judiciaires, pour protéger les informations privilégiées, les données à caractère personnel et les secrets, notamment le secret bancaire.

Outre les restrictions spécifiques à l'application des procédures judiciaires étrangères, plus globalement la loi française veut interdire la transmission d'informations à l'étranger, en imposant aux autorités étrangères l'usage des traités et conventions internationales d'entraide judiciaire, notamment par l'application de la loi de blocage.

## 3.3. LIMITATIONS D'ACCÈS

### 3.3.1. LOI DE BLOCAGE

#### 3.3.1.1. Le principe

Les Entreprises sont parfois sollicitées par des autorités étrangères en vue de l'obtention d'informations dans le cadre de leurs procédures administratives ou d'éléments de preuve dans le cadre de procédures judiciaires.

31 Federal Rules of Civil Evidence, Amendments, December 1, 2006.

32 Federal Rules of Evidence.

33 West v. Goodyear Tire and Rubber Co., 167F.3rd 776 (2dCir.1999).

34 Rules 16(b) & 26(f).

35 Rule 26 (b) & (f).

36 « Civil Procedures Rules, SI 1998/3132 », entrée en vigueur le 26 avril 1999.

37 Articles 31.19, 31.3(1) & 31.3(2).

Or la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique, à des personnes physiques ou morales étrangères est interdite dès lors que :

- cette communication est de nature à constituer une menace notamment à l'égard des intérêts économiques essentiels « sensibles » de la France,
- ou qu'elle tend à la constitution de preuve dans le cadre d'une procédure judiciaire ou administrative étrangère[38].

Le texte posant cette interdiction est appelée « loi de blocage »

#### 3.3.1.2. Les dérogations

Si la loi de blocage énonce un principe général d'interdiction, il peut y être dérogé et des dispositions légales autorisent la communication d'informations à des autorités publiques étrangères, fondée sur la mise en place de systèmes de coopération entre autorités de supervision publique dans une logique de reconnaissance mutuelle des contrôles réalisés au niveau national.
Ainsi pour ce qui concerne l'activité bancaire, la Commission bancaire française a signé de nombreux accords avec des autorités de contrôle des pays tiers. Ces accords ont pour objectif de faciliter l'échange des informations entre autorités de contrôle bancaire.

Dans le domaine judiciaire, la convention de la Haye du 18 mars 1970 sur l'obtention des preuves à l'étranger et le Règlement 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des Etats membres dans le domaine de l'obtention des preuves en matière civile ou commerciale, déterminent les procédures de communication de pièces en vue d'une utilisation dans un procès à l'étranger.

#### 3.3.1.3. Les sanctions

Toute infraction aux dispositions de la loi de blocage peut faire l'objet d'un emprisonnement de six mois et/ou d'une amende de 18 000 EUR.

La Cour de cassation a récemment fait application des sanctions[39] à l'encontre d'un avocat français reconnu coupable d'avoir tenté d'obtenir des renseignements d'ordre économique en vue d'une utilisation dans un procès aux États-Unis, en dehors des procédures de la Convention de La Haye, et donc en violation de la loi de blocage. Il a été condamné au versement d'une amende de 10 000 EUR sur le fondement de cette loi.

### 3.3.2. POSITION DE LA CNIL

Concernant les différentes possibilités d'accès à des données archivées traitées ci-dessus, la CNIL ne pourra s'y opposer dès lors qu'un texte légal encadre ces accès.

Elle veillera toutefois, à ce que ne soit pas communiquées plus de données que nécessaire.

---

38 Loi n° 68-678 du 26 juillet 1968 (modifiée par la loi n° 80-538 du 16 juillet 1980). Article 1 : « sous réserve des traités ou accords internationaux, il est interdit à toute personne de nationalité française, ou résidant habituellement sur le territoire français, et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement, de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisé par l'autorité administrative en tant que de besoin ».

Article 1 bis : « sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement, ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères, ou dans le cadre de celles-ci ».

39 arrêt du 12 décembre 2007 rendu par la Chambre Criminelle de la Cour de Cassation

# 4 Quatrième partie : Cas pratique :

# Archivage électronique appliqué à la messagerie d'Entreprise.

## 4.1 *Définition du courriel et des éléments qui le composent*

### 4.1.1 DÉFINITION DU COURRIEL

Le courrier électronique, auquel le terme courriel a été choisi comme équivalent par la Commission de Néologie et de Terminologie de la Langue Française, est spécifiquement défini à l'article 1 IV de la Loi pour la Confiance dans l'Économie Numérique (LCEN) du 21 juin 2004 comme *« 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 ».*

Cette définition a été voulue comme étant très large car encadrant une réalité très hétérogène en pratique. Ainsi, elle englobe par exemple les messages vocaux laissés sur les répondeurs téléphoniques.
Dans son acception la plus courante, le terme de courrier électronique est toutefois utilisé pour désigner de façon plus limitative un *« service de transfert de messages envoyés par un système de messagerie électronique via un réseau informatique (principalement l'Internet) dans la boîte aux lettres électronique d'un destinataire choisi par l'émetteur »*[40].

Le courriel peut contenir des pièces jointes de différentes tailles, de différents formats. Il peut contenir une certaine mise en page et/ou des pièces jointes. Il peut être envoyé à une ou plusieurs personnes simultanément voire à de nombreux destinataires, via des listes de diffusion, de façon apparente ou en « copie cachée ».

### 4.1.2 QUELS SONT LES ENJEUX DE LA MESSAGERIE ÉLECTRONIQUE DANS L'ENTREPRISE ?

La messagerie est un vecteur de communication performant, simple d'utilisation et rapide.

Déployée dans la quasi-totalité des Entreprises, la messagerie est un outil mis à la disposition de tous les collaborateurs de l'Entreprise, et destiné à échanger et conserver des informations à caractère professionnel mais peut également le cas échéant servir à échanger des informations à caractère privé.

La question de l'usage privé de la messagerie au sein de l'Entreprise reste un sujet délicat malgré les évolutions récentes de la jurisprudence de la Cour de cassation. Cette question avait déjà fait l'objet de développements exhaustifs dans le précédent livrable du Groupe Informatique et Juridique du ***Forum des Compétences*** publié en février 2007 : « *La charte Informatique » par l'exemple*[41]. Le paragraphe 4.3 de ce guide revient de manière plus détaillée sur les aspects juridiques du sujet.

### 4.1.3 QUELLES PRÉCAUTIONS L'UTILISATION DE LA MESSAGERIE REQUIERT-ELLE ?

L'utilisation de la messagerie est soumise au respect d'un certain nombre de bonnes pratiques qu'il appartient à chacun de connaître et de respecter au travers du règlement intérieur ou d'un document autonome (charte de l'Entreprise).
Comme précédemment abordé par le Groupe Informatique et Juridique dans « *La charte Informatique* » *par l'exemple*, les chartes font partie du dispositif de sécurité des Entreprises, mais représentent également un instrument de sensibilisation et de responsabilisation des utilisateurs.

Elles permettent notamment d'informer les divers utilisateurs sur les règles qui régissent au sein de l'Entreprise l'utilisation du système d'information, de les responsabiliser, de rappeler la réglementation

40 Définition Wikipedia http://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique. Ce transfert de courrier électronique s'opère grâce au protocole d'échange « Simple Mail Transfer Protocol » (littéralement « Protocole simple de transfert de courrier »), généralement abrégé en « SMTP ».

41 Document disponible sur http://www.forumdescompetences.com/index.php?section=205.

applicable, de fixer les règles d'une surveillance de l'utilisation, de protéger l'Entreprise en cas de non-respect des règles par les utilisateurs.

La rédaction de la charte pourra utilement s'accompagner d'actions de sensibilisation et de formation.

Par ailleurs, il conviendra de faire évoluer cette charte dans le temps en fonction des changements intervenus dans l'Entreprise, de l'évolution des technologies, des règles juridiques applicables et de la jurisprudence, à l'aide d'audits techniques et juridiques.

Le statut juridique de la charte dépendra de son intégration ou non dans le règlement intérieur :

- si elle est intégrée à ce dernier, la charte s'impose au salarié de telle sorte que le non-respect des obligations qui y figurent pourra exposer le salarié à des sanctions disciplinaires. Cette charte, intégrée au règlement intérieur, aura été préalablement présentée aux instances représentatives du personnel,
- si elle constitue un document autonome non intégré au règlement intérieur, la charte revêt alors une simple valeur informative, pédagogique, morale, et le non respect des obligations qui y figurent ne pourra pas entraîner de manière directe l'application de sanctions.

### 4.1.4 FAUT-IL LIMITER LA VOLUMÉTRIE DES ÉCHANGES ?

Le volume des boîtes aux lettres a un impact direct sur les performances des serveurs de messagerie et des systèmes de sécurité. Par répercussion, il y aura aussi un impact sur la rapidité et l'efficacité des recherches effectuées, que ce soit dans les bases « vivantes » des courriels ou bien dans les bases d'archives.

Le fait de restreindre la taille des messages et des boîtes aux lettres est une pratique courante. Elle doit toutefois être encadrée par des règles clairement communiquées aux utilisateurs.

A titre d'exemple :

- L'utilisateur veillera à limiter au maximum la taille des fichiers attachés à des messages et vérifier que la taille maximale autorisée n'est pas atteinte,
- D'autres types de formulation peuvent être ajoutés sur ce sujet, telle que par exemple :

  L'utilisateur ne doit pas utiliser sa boîte aux lettres comme un espace de stockage. Il est recommandé de détacher dans l'espace de travail utilisateur ou sur un serveur de fichiers les fichiers reçus qui doivent être conservés, en appliquant les consignes du département de l'Entreprise le cas échéant.

Nous renvoyons le lecteur intéressé par les possibilités juridiques d'interdiction ou d'utilisation encadrée, ainsi que par ledit encadrement imaginable, à « *La Charte Informatique par l'exemple* ».

### 4.1.5 QUELLE VALEUR L'INFORMATION VÉHICULÉE PAR LA MESSAGERIE A-T-ELLE ?

Toute information ou instruction diffusée par l'intermédiaire de la messagerie doit être considérée comme ayant autant de portée qu'une information ou instruction diffusée par d'autres voies (courrier, téléphone et fax).

Le paragraphe 4.2 de ce guide traite de l'analyse de la valeur probante des courriels. Pour effectuer cette analyse, il convient tout d'abord de déterminer quels sont les éléments qui composent un courriel.

### 4.1.6 ÉLÉMENTS COMPOSANT LE COURRIEL

Un message est composé de plusieurs rubriques qui requièrent d'être valorisées chacune de façon appropriée : une en-tête, un objet, un contenu, des pièces jointes et une liste de destinataires. Il peut être personnalisé grâce à des options de distribution.

Des règles internes d'utilisation de la messagerie électronique peuvent être mises en places et techniquement encadrées, compte tenu de l'organisation interne de chaque Entreprise et eu égard à l'importance qu'à pris ce média dans la vie des affaires.

#### *4.1.6.1 L'en-tête*

Ainsi, il est souvent préférable que les solutions techniques choisies permettent d'identifier sans ambiguïté l'émetteur de chaque message. De même, il est utile que l'en-tête des messages comporte les coordonnées internes de l'utilisateur permettant de le joindre (mais compte tenu également des risques en terme d'intelligence économique si les messages à destination de l'extérieur de l'Entreprise comportent les mêmes informations).

Autre exemple, une mention particulière mettant en avant le caractère externe de l'intervenant dans l'Entreprise (« Assistant Extérieur » ou « Prestataire ») évite toute ambiguïté vis-à-vis des règles strictes du droit social.

Pour des besoins techniques et de sécurité, les échanges réalisés au niveau des différents serveurs participant à l'acheminement des messages font l'objet d'un enregistrement dans des journaux d'activité (appelés *« logs »*), qui peut être conservé pendant une durée donnée et éventuellement exploité, dans le respect des règles de droit social et en fonction des formalités observées antérieurement à cette fin (information des partenaires sociaux, etc.). Chaque journal est constitué d'un ensemble de traces techniques composées des informations suivantes : l'horodatage, l'émetteur, le(s) destinataire(s) et l'objet du message.

#### *4.1.6.2 L'objet*

L'objet d'un message permet d'identifier rapidement de quoi il traite, que ce soit lors de sa première lecture, ou lors d'une recherche ultérieure, dans une archive par exemple. A ce titre, il peut être utile de recommander aux utilisateurs d'indiquer un titre court et explicite en objet, pour renseigner objectivement le destinataire sur le propos du message, ou encore de reformuler l'objet du message en cas de re-routage, pour focaliser l'attention sur le complément d'information fourni. En fonction des usages internes, le fait même de re-router certains messages peut aussi :

- être rendu impossible pour des raisons de confidentialité,

- entraîner l'insertion en copie de l'émetteur pour des raisons de courtoisie.

Chaque Entreprise, afin d'optimiser l'utilisation par ses salariés et donc sa propre gestion de cet outil informatique, aura ainsi intérêt à définir ses propres usages.

#### 4.1.6.3 Le contenu

De même, attirer l'attention des utilisateurs quant au contenu des messages échangés est toujours utile, celui-ci n'étant efficace en pratique que si son contenu est clair et concis. A ce titre, il peut être rappelé l'intérêt :

- de soigner le contenu aussi bien sur le fond (niveau de langage approprié) que sur la forme (texte structuré et aéré),
- d'éviter les termes flous ou excessifs qui pourraient entraîner une mauvaise interprétation de son message,
- de prendre garde à ce que l'on envoie, les messages électroniques étant écrits et pouvant plus tard être opposés au rédacteur, à l'Entreprise ou à ses employés (cf. remarques supra sur la *e-discovery*, etc.),
- etc.

#### 4.1.6.4 Les pièces jointes

Les pièces jointes d'un courriel ont souvent une valeur informationnelle bien plus importante que le contenu du message lui-même, surtout si le message est réduit à sa plus simple expression, à l'image d'une carte de visite qui accompagne un colis transportant des objets de valeur.

C'est pourquoi il est important que des consignes particulières soient communiquées aux utilisateurs.

A titre d'exemple :

- Les messages doivent être de taille raisonnable et ne comporter qu'un nombre restreint de pièces jointes, surtout s'ils sont adressés à plusieurs destinataires (encombrement de la messagerie),
- En cas d'envoi d'un document volumineux, utiliser un outil de compression de fichier,
- Ne pas choisir systématiquement « Répondre avec historique ». En cas de réponse avec historique, se poser la question de l'utilité de transmettre les pièces jointes au message d'origine.

## 4.2 Messagerie électronique et preuve

La loi du 13 mars 2000 permet d'affirmer qu'un écrit électronique a la même force probante qu'un écrit papier, sous réserve que soient respectées un certain nombre de conditions posées par les articles 1316-1 et 1316-3 du Code Civil.

Ainsi, selon l'article 1316-1 du Code civil, 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. La force probante du courriel dépendra donc de la fiabilité du système en garantissant les critères d'identification et d'intégrité.

Or le courriel est, en pratique dans les Entreprises, envoyé de manière non sécurisée et très aisément falsifiable, que ce soit son contenu ou son émetteur. Il n'est ainsi très souvent pas signé électroniquement par des moyens de signatures à clé publique qui seraient de nature à apporter une preuve fiable de l'identité du signataire et de l'intégrité du message. Les moyens nécessaires à sa véritable sécurisation réclament une organisation lourde et souvent spécifique, liée à un cercle fermé d'utilisateur.

A défaut de remplir les conditions énoncées par la loi du 13 mars 2000, le courriel ne constitue donc a priori qu'un commencement de preuve par écrit au plan du droit civil et donc un élément parmi d'autres de traçabilité des opérations.

Sa force probante pourra être renforcée par d'autres éléments de preuve (autres courriers électroniques concordants échangés, etc.), mais c'est le juge qui au final tranchera entre la force probante des différents moyens de preuve qui lui seront soumis par les parties.

Suivant le type de preuve qu'il conviendra d'apporter en cas de contentieux ultérieur (va-t-on exiger un écrit à titre de preuve ? de validité ? Est-ce une simple preuve d'un envoi ou fait juridique ?), il conviendra alors de concevoir, en liaison avec le service informatique, une solution garantissant le cas échéant leur intégrité et leur imputabilité.[42]

Enfin, la messagerie électronique n'offre généralement pas dans tous les cas des garanties d'origine, de bon acheminement et de confidentialité des messages reçus et/ou envoyés (hypothèse de messages filtrés par le biais de filtres anti-spam possibles en tout point du réseau, etc.). Ces notions sont fondamentales doivent être prises en compte par l'émetteur compte tenu de la sensibilité du contenu ou de la nécessité d'une réception correcte de l'information envoyée.

C'est pourquoi, sur ce sujet, il est préconisé de communiquer des consignes particulières aux utilisateurs dans une charte et/ou dans le règlement intérieur.

Ainsi, à titre d'exemple :

- Il ne faut pas considérer comme garantie l'identité de l'expéditeur ou l'intégrité du contenu d'un message reçu d'Internet. Les usurpations d'identité et les modifications du contenu de messages transmis via Internet sont fréquentes.
- Il ne faut pas tenir compte des accusés de réception automatiques de messages envoyés via Internet. Pour vérifier la bonne réception d'un message important transmis via Internet il est recommandé d'utiliser tout autre moyen de communication (téléphone par exemple).
- Ne mettre en destinataire principal que les personnes dont on attend une action ou qui sont directement concernées par l'information.

## 4.3 Courrier électronique professionnel et privé

### 4.3.1 ÉTAT DE LA JURISPRUDENCE

La jurisprudence est longtemps restée sur l'application stricte du respect du secret des correspondances à la messagerie professionnelle d'Entreprise (Cass. soc., 2 octobre 2001, Nikon c/ M. O., n° 99-42942, Bull. civ. 2001, V, n° 291).

Il faut noter que cela s'accordait mal avec les nécessités pratiques, techniques et organisationnelles de l'Entreprise (continuité d'activité, rôles et pouvoirs des administrateurs de messagerie, etc.).

42 On pourra utilement se référer, à ce sujet, au livre blanc « Conserver les courriers électroniques ? Ou comment résoudre la problématique de l'archivage des e-mails ? », édité par FedISA.

C'est pourquoi, dès 2005, ce principe a connu des tempéraments. Ainsi, un jugement du Conseil de Prud'hommes de Nanterre du 15 septembre 2005 a reconnu la validité d'un principe de labellisation obligatoire du contenu privé des courriels par le salarié.

C'est un arrêt du 18 octobre 2006 (Cass. soc., 18 octobre 2006, Bull. civ. 2006, V, n° 308, p. 294) qui a franchi une étape essentielle en indiquant que « *les dossiers et fichiers créés par le salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors de sa présence* ».

Cette jurisprudence a ensuite été étendue à la messagerie électronique en 2007. La Cour de cassation (30 mai 2007, The Phone House c/ M.X, n° 05-43102) reconnaît en effet la possibilité pour un employeur d'accéder sans aucune formalité particulière à une messagerie électronique d'un salarié. Elle a précisé qu'il convenait de vérifier si les courriers électroniques avaient expressément été identifiés par le salarié comme personnels, avant d'en déduire que l'employeur avait outrepassé ses droits, en effectuant un contrôle à l'insu du salarié, sur le disque dur de son ordinateur.

Par ailleurs dans des décisions rendues à propos de la validité d'une mesure d'expertise (Cass. soc., 23 mai 2007, Datacep c/ Lionel X, 10 juin 2008, n° 06-19229), elle admet que « *le respect de la vie personnelle du salarié ne constitue pas en lui-même un obstacle à l'application des dispositions de l'article 145 du Nouveau Code de procédure civile dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicitées* ». Par conséquent, le recours à l'huissier est possible, l'employeur ayant justifié d'un intérêt légitime puisque ce dernier « *avait des raisons légitimes et sérieuses de craindre que l'ordinateur avait été utilisé pour favoriser des actes de concurrence déloyale* ». Il faut noter toutefois que dans l'une de ces décisions, l'accès avait été réalisé en présence du salarié.

### 4.3.2 MESSAGES AU CONTENU PRIVÉ

Si un usage privé de la messagerie est possible, et indépendamment du point de savoir si ce simple usage peut être sanctionné, il est en pratique nécessaire de mettre en place des règles concernant la position à tenir en présence de messages au contenu privé.

L'utilisateur doit être informé de ces règles et de ses droits.
Ainsi il conviendra de lui préciser le cas échéant quel est l'usage privé « raisonnable » de la messagerie (nécessité de la vie courante et familiale, usage limité et de courte durée afin de ne pas affecter l'exploitation normale du système informatique de l'employeur, agissements considérés comme fautifs ou prohibés tels que l'envoi de messages ou fichiers au contenu illicite de l'ordinateur de l'Entreprise, etc.). Ces règles devront être communiquées aux destinataires de l'utilisateur.

Il conviendra également d'édicter des règles concernant les conditions d'émission de ces courriels : labellisation (type de labellisation à déterminer), taille des pièces jointes…

Il conviendra enfin d'informer l'utilisateur des procédures de contrôle mises en place : mesures de filtrage de spams, des messages infectés par des virus ou comportant des logiciels malveillants, des pièces jointes dépassant la limite autorisée par l'Entreprise, de certains types de fichiers (exécutables notamment).

Concernant la question de la gestion des accès aux postes de travail et aux réseaux, le lecteur pourra se reporter pour des exemples de clauses, à « *La charte Informatique par l'exemple* », éditée par le ***Forum des Compétences*** en février 2007.

### 4.3.3 POSITION DE LA CNIL

Selon la CNIL[43], il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'Entreprise revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où le message peut être archivé lui conférant alors la nature et le caractère d'une correspondance privée protégée par le secret des correspondances.

Elle considère que le respect de l'intimité de la vie privée doit rester un principe. Elle estime que *« l'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, un message à caractère personnel correspond à un usage généralement et socialement admis »* (La Cyber surveillance sur les lieux de travail, rapport de la CNIL 2004).

Elle rappelle que le salarié doit exécuter son contrat de travail de bonne foi et en toute loyauté, il ne doit pas essayer de transmettre le contenu de messages de nature professionnelle sous l'apparence de correspondances privées, par exemple en communiquant des documents confidentiels après avoir identifié ses messages comme étant personnels.

Dans ce même rapport, la CNIL reconnaît que l'employeur peut mettre en place des outils de contrôle et de mesure de la taille, de la fréquence des messages échangés et de leurs pièces jointes ainsi que prévoir l'archivage des messages échangés. La CNIL précise que tout contrôle des salariés doit être loyal, transparent et proportionné.

D'une façon générale, la CNIL rappelle que les traitements de données personnelles, y compris celles des collaborateurs, doivent être déclarés à la CNIL et respecter les principes de droit commun de la loi du 6 janvier 1978 modifiée :

- collecte et traitement des données réalisés pour un usage légitime et déterminé,
- atteinte aux droits fondamentaux (comme le respect de la vie privée) ni excessive ni disproportionnée par rapport au but recherché,
- pertinence des données collectées,
- durée de conservation limitée, légitime et proportionnée à la finalité poursuivie,
- sécurité et confidentialité des données,
- information des personnes concernées claire, précise et objective,
- respect des droits d'accès, de rectification, de suppression et d'opposition.

Elle reconnaît enfin la nécessité de mettre en place ou modifier un règlement intérieur/règles de bonne conduite, afin d'encadrer l'utilisation de la messagerie par les collaborateurs.

## 4.4 Problématique du classement

### 4.4.1 QUELLES MESURES DE CLASSEMENT PRENDRE EN AMONT, POUR FACILITER L'ARCHIVAGE EN AVAL ?

Le classement et l'archivage des courriels peuvent être organisés au niveau de chaque département utilisateur, qui identifie et communique les règles applicables en terme d'utilisation des outils de messagerie et d'archivage, en cohérence avec les dispositions internes relatives à l'archivage des dossiers papier et électroniques.

La multiplicité des situations découlant d'impératifs techniques et/ou organisationnels explique qu'il n'est pas possible de recommander de façon générale un type de consigne à suivre pour cet archivage.

43 Cf. sur son site le Guide Pratique pour les employeurs éd. novembre 2008.

Ainsi, à titre d'exemple, l'utilisateur pourra avoir à se conformer à certaines règles, notamment concernant :

- les règles de classement et de suppression / conservation des courriels (boîte aux lettres et système de messagerie),
- l'utilisation de boîtes aux lettres génériques partagées au sein des équipes pour le suivi en permanence de la réception de certains messages « métiers ».

Afin de permettre la poursuite de l'activité en cas d'absence, les délégations d'accès à la messagerie pourront être confiées à un collaborateur désigné en back up.

### 4.4.2 QUELLE EST LA DIFFÉRENCE ENTRE SAUVEGARDE ET ARCHIVAGE ?

La sauvegarde permet de restaurer le système informatique dans un état de fonctionnement suite à un incident. Elle permet aussi la restauration d'une partie du système informatique à la suite d'une suppression ou d'une modification accidentelles de données.

L'archivage consiste à conserver les données à des fins juridiques, opérationnelles ou historiques selon des critères et des durées définies dans un tableau d'archivage.

Il convient de distinguer la durée maximale de conservation des messages électroniques dans les outils de sauvegarde de la messagerie, de la durée maximale de conservation des archives, nécessairement plus longue.

### 4.4.3 L'ARCHIVAGE DES COURRIELS PEUT-IL ÊTRE MANUEL ?

L'archivage des courriels peut être laissé à la main des utilisateurs (sauf dans certains cas : cf. paragraphe 4.4.4), à charge pour l'Entreprise de leur fournir les moyens de le faire, et surtout de leur communiquer les consignes pour le faire.

La multiplicité des situations découlant d'impératifs techniques et/ou organisationnels explique qu'il n'est pas possible de recommander de façon générale un type de consigne à suivre pour cet archivage.

A titre indicatif, les moyens et consignes qui suivent sont mis en place dans certaines entreprises :

- L'utilisateur de messagerie dispose d'une boîte d'archives, située sur son poste ou sur un serveur local. Cette boîte d'archive est sauvegardée périodiquement,

- L'archivage manuel résulte d'une action volontaire du titulaire de la boîte de messagerie. Il lui appartient d'apprécier l'incidence qu'aurait pour son activité ou pour l'Entreprise la perte de tels documents, avant de procéder à leur archivage,

- Compte tenu du fait que les messages professionnels émis, reçus ou stockés sont et demeurent la propriété de l'Entreprise, l'Entreprise a la possibilité d'accéder à ces archives,

- Cette opération s'effectue sans intervention de l'utilisateur titulaire de celles-ci, en cas de demandes motivées et avec l'accord de l'Audit Interne ou du Responsable de la Conformité de l'entité d'appartenance de l'utilisateur.

### 4.4.4 COMMENT L'ARCHIVAGE DES COURRIELS PEUT-IL ÊTRE AUTOMATISÉ ?

L'espace de messagerie peut être organisé en un certain nombre de répertoires « normalisés ». Des règles automatisées d'archivage peuvent être définies pour tout ou partie de ces répertoires, en fonction des besoins des métiers.

Une bonne pratique consiste à mettre en place un dispositif d'enregistrement systématique des messages envoyés/reçus pour les profils d'utilisateurs les plus exposés à l'utilisation de la messagerie électronique (exemples : opérateurs de marchés, dirigeants).

### 4.4.5 QUELLES RÈGLES DOIVENT ENCADRER L'ACCÈS À LA MESSAGERIE ÉLECTRONIQUE POUR LES ADMINISTRATEURS ?

Les administrateurs des messageries assurent l'administration, le bon fonctionnement et la sécurité de l'outil de messagerie électronique de la Banque. Les droits techniques qui leur sont attribués sont encadrés par des procédures, une obligation de confidentialité et nécessitent d'être limités au strict nécessaire pour assurer leur mission.

## *4.5 Destruction*

### 4.5.1 LA DESTRUCTION DE MESSAGES POUR PRÉSERVER L'INTÉGRITÉ DU RÉSEAU

Les systèmes d'information, d'autant plus s'ils sont connectés à l'Internet, peuvent être la cible d'attaques informatiques, de contamination, de tentative de vol d'information, etc.

En pratique, les usagers sont de plus en plus sollicités par le biais de messages comportant des contenus préjudiciables, illicites, dangereux, mensongers ou parfois simplement inutiles, envoyés par des tiers, que ceux-ci soient malintentionnés ou inattentifs, négligents ou qu'ils pensent tout simplement bien faire. Ainsi, il est utile de préconiser aux utilisateurs recevant des messages électroniques provenant de l'extérieur de l'établissement de détruire, avant même son ouverture, tout message reçu dont la provenance et/ou l'objet sont suspects, pour éviter toute atteinte et surcharge des réseaux locaux (Virus, « *hoax* » ou canulars, messages publicitaires, ...) et toute évasion de données personnelles (Chevaux de Troie, …).

L'intégrité du réseau peut également être compromise lorsque les usagers reçoivent de l'extérieur des courriels comprenant des pièces jointes de grande taille et notamment des fichiers vidéos. Sous réserve des habitudes et de l'activité propres à chaque Entreprise, ces fichiers véhiculent des informations qui ne devraient pas, a priori, relever du domaine professionnel. Là encore, les utilisateurs devraient être sensibilisés au fait que dans ce cas, ces courriels et leur(s) pièce(s) jointe(s) risquent la destruction automatique éventuelle (encombrement du réseau, propagation de virus possible, etc.).

Plus particulièrement, le volume de courriers publicitaires non sollicités, souvent envoyés à des millions d'exemplaires à la fois et sans respecter les règles juridiques existantes (les « spams »[44]), a atteint de nos jours un tel seuil qu'il convient de prendre en compte spécifiquement cette problématique dans le cadre d'une politique d'archivage des courriels. En effet, 150 milliards de spams par jour sont échangés, soit

44 En pratique, envoi de messages électroniques adressés sur la base d'une collecte irrégulière d'adresses de courriels, sans adresse valide d'expédition ou de réponse et dont l'adresse de désinscription est inexistante, invalide ou détournée de sa finalité (permettant notamment de valider l'adresse de courriel d'un tiers). Ces messages contiennent pour l'essentiel des sollicitations de type commercial, souvent pour des produits dont la distribution est illicite (contrefaçons, médicaments). Le terme anglais de SPAM provient d'un sketch des Monty Python où le terme SPAM (marque déposée : "Spiced Pork And Ham") était répété de manière constante.

entre 75 et 85 % de l'ensemble des courriels. Dès lors, les archiver à l'égal des autres messages conduit à surdimensionné inutilement son infrastructure.

Une procédure automatisée de destruction et/ou de non-conservation des messages apparaît dès lors utile à mettre en place. Reste que pour atteindre sa pleine efficacité, il convient de positionner cette procédure en entrée du système d'information de l'Entreprise.

Ainsi, les messages suspects, non consultés et traités par les utilisateurs, pourront être détruits sans incidence particulière, même s'il peut être utile de laisser une période probatoire, de quarantaine, durant laquelle les utilisateurs le souhaitant peuvent « sauver » des messages filtrés à tort, les faire alors rentrer dans le système d'information de l'Entreprise et donc dans la procédure d'archivage classique.

Pour mettre en œuvre ce type de procédure automatisée, il existe aujourd'hui sur le marché des outils, appelés « filtres de réputation », dont la fonction est de filtrer en entrée de réseau les flux provenant des serveurs de messagerie connus comme « pollueurs » sur Internet (envoi massif de courriels non sollicités, messages émis ne respectant pas les standards techniques d'Internet[45], …).

Cette fonction est destinée à ne pas surcharger les relais de messagerie dans du traitement inutile de messages envoyés par des serveurs de messagerie de mauvaise réputation qui, dans la majeure partie des cas, sont assimilables à du spam.

### 4.5.2 COMMENT GÉRER LA DESTRUCTION ACCIDENTELLE DE MESSAGES ?

Comme tout élément d'information géré dans un processus de traitement automatisé, la question de la destruction accidentelle de courriels se pose, et nécessite un traitement adéquat.

A titre indicatif, les moyens et consignes qui suivent (mises en place dans des Entreprises ayant participé à ce document) sont à considérer dans l'organisation du recouvrement de courriels détruits accidentellement :

- Tout d'abord, communiquer clairement aux utilisateurs les règles et procédures en vigueur, notamment les durées maximales de rétention des sauvegardes ou des archives.
- Dans le cas d'une action malencontreuse d'un utilisateur, celui-ci peut demander la restauration de tout ou partie de sa boîte de messagerie aux équipes concernées.

### 4.5.3 QUAND UN COURRIEL PEUT-IL ÊTRE DÉFINITIVEMENT SUPPRIMÉ ?

La prescription ou date à laquelle un courriel archivé peut être supprimé répond avant tout à un impératif légal ou réglementaire (ex : durée de prescription selon la nature du dossier client, dont le courriel constitue un des éléments, exigence de la CNIL en matière de protection des données personnelles et du « droit à l'oubli »).

Le courriel doit en principe être attaché à un dossier et sa durée de conservation doit être définie en fonction de son objet. La durée de conservation sera donc celle fixée pour le dossier dans le tableau d'archivage, en fonction des contraintes légales ou opérationnelles. Toutefois, il peut être utile, au niveau de l'Entreprise, de fixer une durée de conservation des messages électroniques dans l'outil d'archivage électronique, au-delà de laquelle les messages seront supprimés.

La destruction du message est alors irréversible, sans possibilité de le retrouver ou de le reconstituer. Reste que l'effacement avant le terme prévu n'est évidemment pas possible dans le cas de l'utilisation de supports WORM, que ceux ceux-ci soient logiques ou physiques.

45 Notamment : RFC 822 (Request For Comment n° 822 -STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES).

A noter que les régulateurs dans le domaine financier sont de plus en plus nombreux dans le monde à exiger des Entreprises de crédit l'usage de telles technologies pour l'archivage de leurs documents électroniques et notamment les courriels (SEC aux Etats-Unis par exemple).

Dans ces hypothèses, la destruction avant terme prévu des données n'apparaît pas possible sans, soit compromettre l'existence d'autres données stockées sur le même support (WORM physique), soit altérer l'intégrité du processus dans son ensemble dans le cas du WORM logique (la non destruction étant sa raison d'être).

Une politique d'archivage devra dès lors intégrer ces impératifs, prévoir si possible un regroupement des données et surtout, en l'absence de possibilité réelle d'effacement avant le terme prévu à l'origine, mettre en place au minimum un processus permettant la non restitution de la donnée « oubliée » par le dispositif qui ne permettra plus alors de l'extraire et de l'afficher.

La « destruction » sera alors virtuelle, la donnée étant toujours présente physiquement, mais tout aussi efficace (le système empêchant de pouvoir la désarchiver).

### 4.5.4 QUE FAIRE EN CAS DE DÉPART / MOBILITÉ PROFESSIONNELLE / ABSENCE PROLONGÉE?

L'Entreprise doit prendre en compte l'ensemble des processus liés à son activité, et son mode d'organisation aussi bien technique que fonctionnel afin de prévoir les hypothèses de mobilité professionnelle et plus spécifiquement l'archivage des données et messages du collaborateur concerné.

Ainsi, la question du transfert automatique ou non des messages et du devenir des archives doit absolument être envisagée.

## *4.6 Cas des « Webmail »*

Les Webmails sont des clients de messagerie accessibles depuis un navigateur Internet, au contraire des clients de messagerie installés en local sur un poste de travail.

L'accès à ces Webmails se fait via des protocoles de sécurité qui sont au choix de l'hébergeur de l'application distante. Ainsi, certains Webmails peuvent être accessibles via un simple login/mot de passe, tandis que d'autres peuvent faire appel à des processus d'authentification forte garantissant l'intégrité de leur contenu et l'identité de leur émetteur.

A l'instar de ce qui a été dit sur le courriel, de la chaîne créée autour du Webmail (authentification, garantie de l'intégrité des messages, de leur horodatage, sécurisation de la liaison et de l'accès au site) dépendra la valeur probante du message ainsi émis. De la même manière, la conservation de cette valeur probante dépendra des conditions d'archivage du courriel.

Ce type de solution de messagerie en ligne peut être un moyen pour l'Entreprise de réserver la mise à disposition de la messagerie à des fins uniquement professionnelles, l'utilisation du Webmail étant tolérée pour les envois de messages privés.

L'utilisation de Webmails constitue toutefois un risque en matière de sécurité des systèmes d'information, principalement car il affranchit l'utilisateur des contrôles antivirus qui auraient été effectués en messagerie classique sur les serveurs de messagerie de l'Entreprise. D'autant que les systèmes de sécurité intégrés auxdits Webmails (antivirus, etc.) échappent au contrôle de l'Entreprise, qui ne maîtrise pas les solutions utilisées ni la fréquence de leurs mises à jour.

Une Entreprise ne souhaitant pas que ses employés consultent des Webmails pourra dès lors mettre en place de filtres interdisant l'accès auxdites URL.

Nous renvoyons à ce propos le lecteur au document « *La charte informatique par l'exemple* » précité.

## 4.7 Cas des messageries professionnelles instantanées

La messagerie instantanée permet l'échange immédiat de messages textuels entre plusieurs utilisateurs du même réseau.

A la différence de la messagerie traditionnelle, les messages s'affichent en quasi-temps réel et permettent un dialogue interactif, par ordinateurs ou smart-phones interposés. Les messages instantanés, courts et peu formels, présentent ainsi quelques similitudes avec les conversations téléphoniques professionnelles.
Cet outil de travail collaboratif se développe au sein des organisations, inspiré par les pratiques de chat[46] du grand public. L'outil logiciel peut être interne à l'Entreprise ou externe (type Bloomberg, etc.), réservé à un groupe d'utilisateurs désignés ou ouvert vers l'extérieur. Seules les messageries électroniques instantanées autorisées par l'Entreprise doivent être utilisées au sein de celle-ci.

Les règles d'utilisation et les principes de précaution associés énumérés précédemment s'appliquent également. Nous renvoyons le lecteur intéressé par les possibilités juridiques d'interdiction ou d'utilisation encadrée (ainsi que par ledit encadrement imaginable) à « *La Charte Informatique* » *par l'exemple* précitée note n°41.

### Ce type d'échanges électroniques peut-il ou doit-il être enregistré par l'employeur ?

Des principes identiques à ceux des courriels pourraient s'appliquer a priori, avec des modalités d'application particulière compte tenu de l'absence de possibilité de labellisation par exemple. Ainsi, ces contenus sont concernés par les réglementations existantes, notamment celles de l'AMF en ce qui concerne la preuve des instructions émises et des informations échangées.

46 Discussion entre deux ou plusieurs personnes sur internet, du verbe anglais to chat, [tʃat], bavarder. Le nom chat et le verbe chatter sont souvent utilisés en franglais pour désigner la messagerie instantanée.

# Conclusion

La conservation des documents électroniques représente l'une des questions importantes de l'économie numérique. La gestion optimale et l'accès à l'information, au sein de volumes de données croissants, suppose une organisation efficace de l'archivage électronique, notamment au moyen d'une politique adaptée à l'organisation.

Ce guide soulève les questions principales à examiner pour construire ou améliorer la politique d'archivage électronique des organismes confrontés à cet enjeu. Pourquoi et comment archiver ? Quelles procédures d'accès aux documents ? Afin de construire une politique adaptée à l'Entreprise et évolutive, ces questions seront utilement complétées par d'autres, propres à chaque métier et à chaque mode d'organisation. Les réponses à ces questions seront dictées par l'objectif recherché, c'est-à-dire la conservation fiable et durable du patrimoine informationnel.

L'une des problématiques consistera à concilier les choix techniques et organisationnels d'archivage avec l'environnement juridique. La politique d'archivage va intégrer l'évolution des règles nationales, voire internationales, notamment en matière de preuve et de délais de prescription. L'organisation du système de conservation devra également concilier des impératifs qui peuvent apparaître contradictoires, comme l'obligation de conservation des documents dans le temps et le respect des préconisations des régulateurs en matière de données personnelles (« droit à l'oubli »)

S'il est évident que la problématique de l'archivage n'est pas nouvelle et que l'archivistique traditionnelle, pour les documents sous forme papier, dispose de méthodologies éprouvées, l'archivage électronique nécessite une nouvelle approche. Construire une politique d'archivage électronique implique aujourd'hui davantage d'acteurs que l'archivage traditionnel. Une approche globale et unifiée est rendue nécessaire par la complexité de l'environnement et l'intégration des systèmes d'information. Cette approche sera pluridisciplinaire, elle intégrera les expertises organisationnelles, techniques, déontologiques, juridiques et sécuritaires, y compris du point de vue de la continuité d'activité, et naturellement la participation de tous les métiers concernés. Il sera utile également de prévoir dès la rédaction de la politique d'archivage, l'auditabilité du système et de la politique elle-même.

De plus, la méthodologie et la politique d'archivage électronique seront établies, à la différence de l'archivage classique, dès la mise en œuvre des systèmes, et non en fin de cycle de vie des documents.

Enfin, comme la politique d'archivage vise à la protection, au partage de l'information, et à la traçabilité des produits complexes, la politique d'archivage électronique sera aussi pluridisciplinaire et anticipative que possible.

**Archivage électronique**

L'archivage de contenus électroniques est l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, sélectionner, classer et conserver des contenus électroniques, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (en cas d'obligations légales notamment ou de litiges) ou à titre informatif. Le contenu archivé est considéré comme figé et ne peut donc être modifié. La durée de l'archivage est fonction de la valeur du contenu et porte le plus souvent sur du moyen ou long terme.

**Certificat électronique**

Il s'agit d'un élément permettant la vérification d'une signature électronique. Pour que le procédé de signature électronique soit présumé fiable, le certificat électronique doit être qualifié. Un certificat délivré par un prestataire reconnu qualifié sera présumé qualifié.

**Chiffrement ou cryptographie**

Le chiffrement vise à transformer à l'aide de conventions secrètes appelées clés, des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers n'ayant pas la connaissance du secret, ou à réaliser l'opération inverse grâce à des moyens, matériels ou logiciels conçus à cet effet. Le chiffrement permet de détecter la perte d'intégrité d'informations, d'authentifier des interlocuteurs et de protéger la confidentialité des informations.

**Conservation**

La conservation est l'ensemble des moyens mis en œuvre pour stocker, sécuriser, pérenniser, restituer, tracer, transférer voire détruire, les contenus électroniques archivés.

**Dématérialisation**

La dématérialisation est le transfert sur un support numérique des types d'informations qui existaient jusque là sous forme analogique (papier, film, etc.).

**Document**

Un document est généralement défini comme le support physique d'une information.

**Document informatique ou fichier**

Un document informatique est l'ensemble des données informatives présentes sur un support, sous une forme permanente et lisible par l'homme ou par une machine (permanent par opposition à volatil).

**Donnée**

Description élémentaire, souvent codée, d'une chose, d'une transaction d'affaire, d'un événement, etc. Les données peuvent être conservées et classées sous différentes formes : papier, numérique, alphabétique, images, sons, etc.

**Donnée à caractère personnel**

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à

un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. (art 2, loi du 6 janvier 1978 relative à l'informatique et aux libertés)

**Information**

Source de connaissance sur un sujet donné, susceptible d'être représentée afin d'être conservée, traitée, communiquée.

**Métadonnées**

Données décrivant le contexte, le contenu et la structure des documents ainsi que leur gestion dans le temps.

**Sauvegarde**

La sauvegarde est l'ensemble des actions, outils et méthodes destinés à dupliquer des contenus électroniques d'origine dans un but sécuritaire pour éviter leur perte en cas de dysfonctionnement du dispositif sur lequel ils sont enregistrés (dans le cas de plans de reprise d'activité ou de continuité d'activité - PRA/PCA). Le contenu sauvegardé n'est pas considéré comme figé et peut donc être modifié ou remplacé. La durée de la sauvegarde est fonction de sa périodicité et porte le plus souvent sur du court terme.

**Signature électronique**

La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache (art 1316-4 du Code Civil).
Toutes les signatures électroniques sont recevables en justice dès lors qu'elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et l'intégrité de l'acte. Le décret 2001-272 du 30 mars 2001 décrit les conditions sous lesquelles le procédé de signature électronique est présumé fiable. Si ces conditions ne sont pas remplies, il est nécessaire en cas de contestation de prouver la fiabilité du procédé de signature électronique utilisé.

**Signature électronique sécurisée**

Il s'agit d'une signature électronique qui est propre au signataire, qui est créée par des moyens que le signataire puisse garder sous son contrôle exclusif et qui garantit avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

**Stockage**

Le stockage s'apparente aux actions, outils et méthodes permettant d'entreposer des contenus électroniques et servant de base au traitement ultérieur des contenus.

**Traitement de données à caractère personnel**

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. (Art 2, loi du 6 janvier 1978 relative à l'informatique et aux libertés).

# *Annexe II : Tableau sur le régime de la preuve en droit français. . .*

## 1 – **Le régime de la preuve en droit français**

| **PREUVE RÉGLEMENTÉE**<br>**écrit sur support papier ou électronique** | **PREUVE RÉGLEMENTÉE**<br>**écrit sur support papier** | **PREUVE LIBRE** |
|---|---|---|
| **Tout acte supérieur à 1 500 EUR.**<br>(art. 1341 Code civil.) | Les actes sous seing privé relatifs au droit de la **famille et des successions** (art. 1108 2 du Code civil) | Acte **en dessous du seuil de 1 500 EUR.** |
| Les actes sous seing privé relatifs à des **sûretés réelles ou personnelles**, de nature civile ou commerciale, s'ils sont passés par une personne pour les **besoins de sa profession** (art. 1108 2 du Code civil) | Les actes sous seing privé relatifs à des **sûretés réelles ou personnelles**, de nature civile ou commerciale s'ils ne sont pas conclus pour des besoins professionnels (art. 1108 2 du Code civil) | **A l'égard des commerçants**, les actes de commerce peuvent se prouver par tous moyens (art. L.110-3 du Code de commerce.) |
| Tout acte pour lequel l'écrit est requis comme **condition de validité** de l'acte juridique (ad validationem) (art. 1108 1 du Code civil). | | **Contrats conclus avec un non commerçant** : à défaut d'écrit, production d'un commencement de preuve par écrit (lettre, chèque, acte non signé …) complété par un autre mode de preuve extérieur à l'acte (témoignage, présomption) (art. 1347 *Code civil*). |
| | | Obligation née d'un **quasi contrat**, d'un **délit ou d'un quasi-délit** (*art. 1348 al. 1er Code. civil.*). |
| | | **Perte du titre** par suite d'un cas fortuit ou d'une force majeure (*art. 1348 al. 1er Code. civil*.). |
| | | **A défaut de conservation du titre original** par une partie ou par le dépositaire, production d'une **copie qui en est la reproduction fidèle et durable** (*art. 1348 al. 2 du Code. civil.*) |

## 2 – *Les solutions*

1) Les conventions sur la preuve

La validité de ces conventions est consacrée par l'article 1316-2 du Code civil : *« à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable ».*

Les conventions sur la preuve vont permettre l'admission « *d'écrits électroniques* » comme preuve sans que ces derniers répondent aux exigences des articles 1316-1 et 1316-4 du Code civil. Il en est ainsi, par exemple, pour les enregistrements informatiques qui constatent les opérations réalisées par cartes bancaires.

2) Les normes en vigueur

La norme la plus connue en la matière est la norme NF Z 42-013 sur l'archivage électronique, élaborée par l'Association Française de Normalisation (AFNOR). Elle contient un ensemble de spécifications concernant les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer leur conservation et leur intégrité.

3) Le recours à un prestataire externe (tiers archiveur)

L' *« externalisation »* de l'archivage électronique peut représenter le moyen de sécuriser la procédure d'archivage électronique en mettant en avant l'indépendance de ce prestataire.

## *PHOTOCOPIE*

**Cass. Civ.1, du 21 mars 2006 :** pour admettre comme preuve de l'existence d'un prêt bancaire, dont l'existence était contestée par le défendeur, **la photocopie de l'offre de prêt** invoquée par la banque, la cour d'appel, devant laquelle le défendeur avait exigé la production de l'original de ce document, qu'il déniait avoir signé, retient que la banque s'est trouvé dans l'impossibilité matérielle de verser celui-ci aux débats. La Cour de cassation casse l'arrêt d'appel sur le fondement des articles 1334 et 1348 du Code civil : « (…) ***à défaut de production de l'original du document litigieux,*** il lui incombait de rechercher si la ***photocopie retenue, qui n'avait par elle-même aucune valeur juridique*** et ne pouvait suppléer à ce défaut de production, constituait une ***reproduction fidèle et durable*** de cet original ou si ce dernier avait été perdu par suite d'un cas fortuit ou de force majeure ».

**Cass. Civ.1, 30 mai 2000** : S'agissant d'un contrat d'assurance complémentaire dont l'original a été égaré par l'assureur c'est dans **l'exercice de son pouvoir souverain d'appréciation de la valeur et de la portée de la photocopie** qui lui était soumise, que la cour d'appel a jugé que la photocopie, qui ne révélait aucune trace de falsification par montage de plusieurs documents et permettait de constater que les caractéristiques d'ordre général de l'écriture du bulletin complémentaire de 1992 présentaient de grandes similitudes avec celles du bulletin d'adhésion de 1990, **constituait une copie sincère et fidèle du document original**, au sens de l'article 1348, alinéa 2, du Code civil.

**CA Paris, 17 mars 1998 :** la preuve de l'étendue d'une obligation née d'un contrat doit être établie par écrit, conformément à l'article 1341 du Code civil. Cette règle reçoit exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente **une copie, qui en est la reproduction non seulement fidèle mais aussi durable,** en application de l'article 1348 alinéa 2 du Code civil. En l'espèce, **selon l'expertise judiciaire,** la photocopie du bulletin de versement complémentaire, produite par l'assureur, et qui modifie l'identité des bénéficiaires du contrat d'assurance vie, ne montre pas de trace de falsification par montage de plusieurs documents et les caractéristiques générales de l'écriture, présentant de grandes similitudes avec celles de l'écriture du bulletin d'adhésion lui-même si en raison d'une mauvaise qualité de la photocopie, elle-même reproduite à partir d'une autre photocopie, il n'est pas possible de procéder à une comparaison d'écriture plus approfondie. Par conséquent, **la photocopie constitue une copie sincère et fidèle** du bulletin rempli par l'assuré, au sens de l'article 1348 alinéa 2 du Code civil.

**Cass. Civ. 1, 25 juin 1996 : la photocopie produite étant une reproduction durable et fidèle** du mandat établi, ce document ne constituait pas un commencement de preuve par écrit, mais faisait pleinement preuve de l'existence d'un mandat de vente confié à un commissaire-priseur, conformément à l'article 1348 du Code civil.

**Cass. Civ. 1, 9 mai 1996 :** après avoir constaté **l'impossibilité de production de l'original** du bulletin de transfert de l'assurance décès, la cour d'appel faisant justement application de l'article 1348 du Code civil, retient que la **photocopie de ce bulletin en constitue une reproduction fidèle et durable,** ses énonciations se trouvant corroborées par les témoignages de la volonté du souscripteur de transférer le bénéfice de l'assurance à telle personne, et par les instructions données, en vue de la transmission à l'assureur du bulletin signé.

**Cass. Civ.1, 14 février 1995 :** la cour d'appel a retenu comme commencement de preuve par écrit **la photocopie** de la reconnaissance de dette écrite et signée par le débiteur, qui ne contestait ni l'existence de l'acte ni la conformité de la photocopie à l'original, selon lui détruit. Mais si la photocopie de la reconnaissance de dette comportait la stipulation de l'intérêt conventionnel, **cet acte ne pouvait concerner que la preuve,** le taux d'intérêt devant selon l'article 1907 du Code civil être fixé par écrit.

## *TELECOPIE*

**Cass. Civ. 1, 28 mars 2000 : une copie, à laquelle est assimilable une télécopie, peut être invoquée comme moyen de preuve en cas d'impossibilité de production de l'original.** Ayant retenu que la télécopie que le créancier entendait utiliser comme preuve d'un acte de cautionnement était contestée par le défendeur qui soutenait que celle-ci était un mont**age d**estiné à faire croire à l'existence d'un original qu'il n'avait pas établi, c'est dans **l'exercice de son pouvoir souverain d'appréciation** que la cour d'appel a décidé que la preuve du cautionnement n'était pas rapportée.

**CA, Aix en Provence, 26 mai 1997 :** en droit, le créancier qui invoque au soutien de son action l'engagement d'un tiers au titre de caution, normalement considéré comme un engagement civil, doit en rapporter la preuve en fournissant un acte original émané de son adversaire, conforme aux exigences légales ou encore un commencement de preuve écrite complété par tout autre moyen admissible ; si ces règles reçoivent exception notamment **lorsque le créancier prouve qu'il n'a pas conservé le titre original et présente une copie de celui-ci qui en est la reproduction fidèle et durable, tel n'est pas le cas en l'espèce où le créancier,** qui ne dispose ni de l'original du cautionnement allégué, ni même d'un commencement de preuve écrite original entend utiliser directement comme preuve la télécopie qu'il possède de l'acte original de cautionnement. En conséquence, ne pouvant établir, conformément à l'article 1348 du Code civil qui permet l'utilisation de la copie qu'au seul cas où le titre original n'a pas été conservé, qu'il aurait à un moment donné disposé de cet original, le créancier ne peut affirmer que **la télécopie** dont il dispose serait ne reproduction fidèle d'un titre original qu'il n'a jamais vu et que son adversaire affirme ne pas avoir établi.

**Cass. Civ. 1, 2 décembre 1997 :** l'écrit constituant aux termes de l'article 6 de la loi du 2 janvier 1981, l'acte d'acceptation de la cession ou du nantissement d'une créance professionnelle, **peut être établi et conservé sur tout support, y compris par télécopies,** dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées
ou ne sont pas contestées. Analysant les circonstances dans lesquelles a été émise la télécopie litigieuse, dont le caractère mensonger n'avait pas été allégué, la cour d'appel a pu en déduire que la preuve écrite de l'acceptation de la cession de créance était établie.

## *DIVERS*

**Cass. Civ. 1, 14 février 1990 :** C'est dans l'exercice de son **pouvoir souverain d'appréciation de la valeur probante du document** qui lui était soumis que la cour d'appel a estimé insuffisante l'attestation selon laquelle le commissaire aux comptes de la banque certifiait « avoir la conviction » que l'ensemble des personnes s'étant portées cautions et figurant sur **les « listings » informatiques** avaient bien reçu l'information conformément aux prescriptions légales.

**Cass. Civ. 1, 28 juin 1989 :** les juges du fond ont valablement pris en compte une lettre de la banque mandataire d'époux acquéreurs d'un immeuble, qui rendait vraisemblable leur non paiement d'une partie du prix et d'avoir donc, sur cette base, permis à la société venderesse de **prouver la réalité de sa créance par témoignages et présomptions complémentaires.**

**Cass. Civ. 1, 27 mai 1986 : les copies pouvant valoir comme commencement de preuve par écrit,** justifie sa décision la cour d'appel qui fonde sa conviction **sur les doubles d'une facture obtenus à l'aide de papiers carbone** insérés dans un carnet à souche, joints à d'autres indices qu'ils confortaient.
Dès lors qu'ils ont fait application de dispositions de l'article 1347 du Code civil, les juges ont pu se fonder sur des écrits qui ne comportaient pas toutes les mentions requises par l'article 1326 du même code.

# *Annexe IV : Modalités d'accès dans le cadre des procédures administratives et judiciaires françaises, Principales autorités pouvant intervenir dans le secteur bancaire et financier*

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **DGCCRF** | <u>Pouvoirs en matière de concurrence</u><br>- Enquête simple : Les enquêteurs peuvent demander la communication des livres, factures et tous autres documents professionnels et en obtenir ou en prendre copie par tous moyens et sur tous supports. Une entrave à l'enquête est constitutive d'un délit correctionnel (article L.450-8 du Code Comm.)<br>- Enquête lourde ou coercitive: cette enquête a lieu sur autorisation judiciaire rendu par ordonnance du JLD du TGI du lieu de visite. Dans ce cas, les enquêteurs ont le droit de rechercher et de saisir tous documents utiles à leur enquête.<br>Ils peuvent accéder à l'intégralité de la messagerie et saisir tous documents.<br>L'enquêté peut prendre copie des documents saisis et si des saisies lui paraissent litigieuses, noter des réserves dans le PV de fin de visite.<br><br><u>Pouvoirs en matière de réglementation de la consommation</u><br>- Contrôle de la conformité des produits et services: "Les agents peuvent exiger la communication et obtenir ou prendre copie par tous moyens et sur tous supports ou procéder à la saisie des documents de toute nature, entre quelques mains qu'ils se trouvent". Ils ont accès "aux logiciels et aux données stockées". Faire obstacle à la DGCCRF est sanctionné (article L.217-10 du Code Cons.). | *Dans le cadre d'une* ***<u>enquête simple</u>*** :<br><br>Les enquêteurs ne peuvent que consulter les documents ou en prendre copie. Ils n'ont pas de pouvoir de perquisition et **ne peuvent accéder directement à une messagerie**. En l'absence de commission rogatoire, le <u>secret professionnel</u> est opposable pour les comptes des clients.<br><br>**<u>Dans tous les cas</u>**, les enquêteurs ne peuvent saisir les correspondances entre l'Entreprise et ses avocats (décret de juillet 2005).. | ***<u>Pour les enquêtes simples et lourdes</u>***<u>:</u> Article L.141-1 du Code de la consommation pour la recherche et constatation d'infraction et articles L.450-1 à L. 450-8 du Code de commerce (article L.450-3 pour l'enquête simple et L.450-4 pour l'enquête coercitive).<br><br>***<u>Pour le contrôle de conformité des produits et services</u>***<u>:</u> article L.215-1 et suivants du Code de la consommation. | Dans le cadre d'une **<u>enquête lourde</u>** : les enquêteurs notifient l'ordonnance du JLD autorisant la perquisition<br><br>**<u>A l'issue de l'enquête:</u>** un procès verbal doit être établi. |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **HALDE** | ***Demande de communication de documents***: La HALDE peut demander dans le cadre de son enquête tous documents quels qu'en soit le support.<br><br>Les personnes soumises au secret professionnel ne peuvent être poursuivies pour les informations à caractère secret qu'elles auraient pu révéler à la Haute Autorité.<br>En cas de refus de collaborer, la HALDE peut saisir le juge des référés afin qu'il ordonne toute mesure d'instruction qu'il juge utile pour la poursuite du dossier.<br><br>***Les vérifications sur place:*** dans les locaux exclusivement consacrés à un usage professionnel et sous réserve d'obtenir au préalable l'accord de la personne contrôlée. Seuls les agents de la HALDE ayant reçu habilitation spécifique du procureur général près la Cour d'appel peuvent procéder à ces vérifications. | **Demande de communication de documents:**<br><br>La HALDE ne peut effectuer les recherches et n'a pas accès à l'ensemble de la messagerie d'un salarié.<br><br>Le secret bancaire ne peut lui être opposé dès lors que les demandes d'informations respectent le principe de spécialité des pouvoirs qui lui sont propres<br><br>***Les vérifications sur place:***<br><br>Les agents de la HALDE peuvent entendre toutes personnes susceptibles de fournir des informations, mais n'ont pas accès directement aux documents et ne peuvent effectuer de saisies.<br><br>Les agents de la HALDE ne peuvent accéder à l'intégralité de la messagerie d'un salarié de l'Entreprise. | Articles 5, 6, 8 et 10 de la loi du 30 décembre 2004<br>portant création de la Haute Autorité de lutte contre les discriminations et pour l'égalité. | ***Les vérifications sur place:***<br><br>Au début de l'enquête**:**<br><br>Une fois saisie, la HALDE adresse un avis aux personnes intéressées et recueille leurs accords.<br><br>Au cours de l'enquête:<br><br>la HALDE est habilitée à enquêter dans les locaux accessibles au public et les locaux professionnels.<br><br>Les documents demandés ont pour but d'effectuer des comparaisons afin de savoir s'il existe des discriminations. Dans cette optique, les demandes sont assez large.<br><br>A l'issue de l'enquête: La HALDE rédige un procès verbal constatant les résultats de son enquête. Ce rapport est adressé aux personnes intéressées qui peuvent adresser leurs observations sous 10 jours |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **AMF** | Le <u>secret professionnel</u> ne peut être opposé à l'AMF.<br><br>Faire obstacle à une mission de l'AMF est constitutif d'un délit sanctionné par l'article L.642-2 du Code monétaire financier.<br><br>***<u>Demande de communication de documents</u>*:**<br>L'AMF peut se faire communiquer tous documents nécessaires à son enquête, quel qu'en soit le support et en obtenir une copie.<br><br>***<u>Vérifications sur place:</u>***<br>Les agents de l'AMF peuvent accéder aux locaux professionnels. | ***<u>Demande de communication de documents</u>*:**<br>L'AMF n'a pas le pouvoir d'effectuer les recherches, ni de saisir d'office les documents.<br>Les agents de l'AMF n'ont pas accès à l'ensemble de la messagerie d'un salarié.<br><br>***<u>Les vérifications sur place</u>:*** Ces vérifications permettent **d'interroger** les personnes susceptibles de fournir des informations à l'AMF.<br>Les agents de l'AMF n'ont pas accès directement aux documents et ne peuvent effectuer de saisies.<br>Les agents de l'AMF ne peuvent accéder à l'intégralité d'une messagerie | Article L.621-9-3 (pour le secret professionnel).<br><br>Article L.621-10 du Code monétaire et financier. | **En cas de vérification sur place:**<br><br><u>Au début de l'enquête</u>: L'AMF présente son ordre de mission, nominatif et valable pendant toute la mission. Une copie peut être remise à la personne concernée par le contrôle sur place. L'objet du contrôle figurant sur l'ordre de mission encadre le périmètre des investigations.<br><br><u>Au cours de l'enquête:</u> Si nécessaire, le secrétaire général de l'AMF peut modifier le périmètre des investigations en émettant un ordre de mission complémentaire. Les inspecteurs examinent les documents qui leur sont communiqués et en demandent copie s'ils le jugent utile. Ils peuvent ordonner la conservation de toute information, via une confirmation écrite.<br><br><u>A l'issue de l'enquête:</u> Un rapport de contrôle est rédigé.<br>. |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **Douanes** | **Droit de communication**<br>Les agents des douanes peuvent exiger la communication de documents de toute nature et sur tous supports (comptabilité, factures, compte en banque…) relatifs à leur mission, sans que le secret bancaire ne puisse leur être opposé. Le droit de communication s'exerce sur les documents pendant trois ans (article 65 du Code des Douanes) et dix ans pour les contrats de fiducie.<br><br>**Droit de visite et de saisie**<br><br>Les agents des douanes ont un droit de visite sur les marchandises et les moyens de transport ainsi que sur les personnes.<br>Ils ont accès aux locaux et lieux à usage professionnel, ainsi qu'aux moyens de transport à usage professionnel et à leur chargement, si des marchandises ou documents se rapportant à des infractions au code des douanes sont susceptibles d'y être détenus. Au cours du contrôle les agents des douanes peuvent retenir des documents ou en prendre copie.<br><br>Lors d'un contrôle, les agents des douanes pourront avoir accès au disque dur d'un portable et donc à une messagerie électronique. Dans ce sens, la douane a été autorisée à « fouiller » et saisir un agenda (C. cass. Crim. 18 avril 1988). | **Droit de communication**<br><br>L'article 65 n'autorise pas l'administration des douanes à effectuer les recherches : elle peut demander communication des documents et saisir les originaux qui lui paraissent utiles. Les agents des douanes ne pourront pas accéder à la messagerie d'un salarié de l'Entreprise.<br><br>**Droit de visite et de saisie**<br><br>Les personnes ne peuvent être retenues contre leur gré, ni faire l'objet d'aucune mesure coercitive.<br><br>Les agents des douanes doivent être autorisés par ordonnance du JLD pour procéder à des perquisitions et saisies en tous lieux, même privés, où des marchandises ou des documents se rapportant à des délits douaniers ou des infractions à la législation sur les relations financières avec l'étranger sont susceptibles d'être détenus (art.64 du CD).<br><br>En cas de flagrant délit, ils peuvent procéder directement à la perquisition. | Articles 63 ter, 65 et 65 bis du Code des Douanes: droit d'accès de communication et de saisie.<br><br>Articles 60 à 63 bis du Code des douanes: droit de visite des marchandises, des moyens de transport et des personnes.<br><br>Article 64 du Code des douanes droit de perquisition. | **Au début de l'enquête:**<br><br>Pour une perquisition, seuls peuvent y procéder les agents des douanes spécialement habilités par le directeur général des douanes et droits indirects. Ils présentent d'abord une ordonnance du JLD.<br><br>**Au cours de l'enquête:** Aucun délai autre que la prescription ne limite la durée de l'enquête. Pour accéder à un local à usage professionnel, l'agent des douanes doit avoir au moins le grade de contrôleur. Le droit de communication est exercé par les agents ayant au moins le grade d'inspecteur ou d'officier et ceux chargés des fonctions de receveur; la remise des documents doit être volontaire: un refus constitue une contravention douanière (article 43 bis du Code des douanes).<br><br>**A l'issue de l'enquête:** Les agents des douanes rédigent un procès verbal. |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **Commission bancaire** | La Commission bancaire contrôle le respect des dispositions législatives et réglementaires par les Entreprises de crédit et les Entreprises d'investissement.<br><br>Le secret professionnel ne peut être opposé à la Commission bancaire<br><br>***Le contrôle sur pièces***:<br><br>La Commission bancaire peut "demander aux personnes soumises à son contrôle tous renseignements, documents quel qu'en soit le support et en obtenir la copie".Elle peut demander les rapports des Commissaires aux comptes et de manière générale tous documents comptables.<br><br>***Le contrôle sur place:***<br><br>Dans le cadre de ce contrôle, la Commission bancaire peut procéder à des interrogatoires et se faire communiquer tous documents nécessaires à son enquête.<br>Ces contrôles peuvent être étendues aux filiales d'un établissement financier. | ***Contrôle sur pièces***<br><br>la Commission bancaire demande communication de documents. Il s'agit d'une procédure écrite, les agents de la commission bancaire ne peuvent dans ce cadre accéder à la messagerie électronique d'un salarié de l'Entreprise.<br><br>***Contrôle sur place:***<br><br>Comme la HALDE et l'AMF, la Commission bancaire ne dispose pas d'un droit de perquisition. Elle demande communication de documents et prend copie de ceux qu'elle estime nécessaire pour l'accomplissement de sa mission.<br><br>La Commission bancaire ne peut donc accéder à l'intégralité de la messagerie d'un salarié. | Article L.511-33 du Code monétaire et financier pour la levée du secret professionnel.<br><br>Article L.613-1 et L.613-6 à L.613-20 du Code monétaire et financier. | ***Au début de l'enquête :*** La Commission Bancaire (CB) peut se saisir elle-même. Elle détermine la liste, le mode et les délais de transmission des documents et informations qui doivent lui être remis. Pour un contrôle sur place dans un établissement affilié à un organe central, la CB en informe ce dernier.<br><br>***Au cours de l'enquête***: Dans le cadre d'un contrôle sur place, la Commission prend copie des documents qu'elle estime nécessaire.<br><br>***A l'issue de l'enquête*:** Dans le cadre d'un contrôle sur place, les résultats du contrôle sont communiqués aux dirigeants de la personne morale contrôlée et aux commissaires aux comptes concernés. |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **Autorités fiscales** | ***Droit de communication de l'administration fiscale*:**<br><br>Ce droit s'exerce sur tout type de support.<br><br>Documents recherchés par l'administration fiscale: documents comptables, contrats, relevés de comptes, bordereaux de remises de valeurs, documents de service.<br><br>Le droit de communication s'exerce sur les documents pendant six ans.<br><br>***Pouvoir de perquisition*:**<br><br>En cas de présomption de fraude l'administration fiscale peut procéder à des perquisitions : "rechercher la preuve en effectuant des visites en tous lieux mêmes privés, où les pièces ou documents sont susceptibles d'être détenus et procéder à leur saisie quel qu'en soit le support".<br><br>Les banques sont alors déliées du secret professionnel. | ***Droit de communication :***<br><br>En application de ce droit, l'administration fiscale ne peut effectuer les recherches. Elle demande communication de documents comptables qui lui permettront de remplir sa mission. Elle ne sera pas amenée ici à prendre connaissance de la messagerie d'un salarié.<br><br>***Pouvoir de perquisition :***<br><br>Cette procédure ne s'applique que pour la recherche d'infractions aux impôts directs et à la TVA. Elle doit être autorisée par ordonnance du JLD qui fixe les limites de la mission des agents de l'administration fiscale.<br><br>Les correspondances entre l'Entreprise et ses avocats ne peuvent être saisis (décret du 12/07/2005). | Article L.16 B du Livre des procédures fiscales (perquisition). Articles L.81 et suivants du Livre des procédures fiscales (droit de communication). | ***Au début de l'enquête:***<br><br>En cas de perquisition : notification de l'ordonnance du JLD indiquant les noms et qualités de l'agent enquêteur (ayant au moins le grade d'inspecteur) et de l'OPJ assistant aux opérations et précisant le cadre de la mission.<br><br>***Au cours de l'enquête:***<br><br>*Droit de communication:* L'administration fiscale n'a droit à communication des pièces que sur une affaire déterminée **(**elle ne parait pas pouvoir obtenir communication de la liste nominative des titulaires de coffres par exemple)<br><br>*Pour la perquisition*, tous les documents peuvent être saisis. Une nouvelle autorisation judiciaire est nécessaire en cas de découverte de nouveaux lieux (ou d'un coffre dont l'occupant des lieux est titulaire).<br><br>***A l'issue de l'enquête*:** Rédaction d'un PV obligatoire à l'issue d'une perquisition ou à l'occasion d'une saisie. |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **CNIL** | Les agents de la CNIL ont accès aux locaux professionnels.<br>Les agents de la CNIL peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie.<br><br>Les membres de la délégation peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.<br><br>Durant l'inspection, il convient de prendre toutes mesures utiles afin de faciliter la mission de la CNIL, sous réserve du secret professionnel.<br><br>*Est puni d'un an d'emprisonnement et de 15.000 EUR. d'amende le fait d'entraver l'action de la CNIL (article 51 loi IL)*. | Selon l'article 11 2° f) les agents de la CNIL doivent avant tout procéder à des vérifications sur tout traitement. Ils vérifient si les traitements de données personnels mis en oeuvre dans l'Entreprise ont bien été déclarés et sont conformes à la loi Informatique et Liberté.<br>Ces investigations ne doivent pas les amener à effectuer des recherches dans une messagerie électronique.<br><br>Le secret professionnel est opposable à la CNIL (mention de cette opposition sera faite au PV: article 69 du décret de 2005). | Article 11 et 44 de la loi Informatique et Libertés.<br><br>Pour le secret professionnel: article 21, 3e alinéa de la loi Informatique et Liberté et article 69 du décret du 20 octobre 2005. | ***Au début de l'enquête*:**<br><br>Il peut être demandé communication préalable de documents.<br>La décision de prévenir le responsable du traitement contrôlé est prise au regard de la mission envisagée. Cette décision est notifiée au responsable des lieux où se situe le contrôle contre signature d'un AR; en cas d'opposition la CNIL doit demander une ordonnance au président du TGI (articles 493 à 498 du CPC).<br><br>***Au cours de l'enquête:***<br><br>L'objectif est d'obtenir copie d'informations pour apprécier les conditions de mise en oeuvre d'un traitement.<br><br>***A l'issue de l'enquête:***<br><br>Un procès verbal indiquant les documents copiés est établi à l'issue de l'inspection |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| **Autorités judiciaires** | **<u>Au Pénal</u>**<br><br>***<u>Enquête de flagrance</u>*** *:*<br><br>Les diligences menées par les OPJ lors de l'enquête s'imposent à toute personne pouvant contribuer à l'établissement de la vérité.<br>Les perquisitions et saisies sont possibles sans l'accord des personnes intéressées par les faits poursuivis. L'OPJ a seul le droit de prendre connaissance des documents et a l'obligation de mettre en place toutes mesures utiles pour assurer le respect du secret professionnel et des droits de la défense, c'est-à-dire de veiller à ce que la perquisition et la saisie ne concernent que les faits poursuivis.<br><br>***<u>Enquête préliminaire :</u>***<br><br>L'enquête préliminaire permet de rassembler les preuves sans mettre en œuvre l'instruction. Elle est décidée par les OPJ , soit d'office soit sur instruction du procureur de la République. L'absence de réponse est punissable d'une amende de 3 750 EUR..<br><br>***<u>Commission rogatoire du juge d'instruction:</u>***<br><br>Elle doit indiquer la nature de l'infraction recherchée et être signée du juge et ne peut prescrire que des actes d'instruction se rattachant aux faits qui y sont visés. Elle lève le secret bancaire en application de l'article 57 de la loi bancaire selon lequel il ne peut être opposé à l'autorité judiciaire agissant dans le cadre d'une procédure pénale. La police judiciaire ayant reçu délégation de l'autorité judiciaire par la commission rogatoire peut donc obtenir des informations, renseignements et documents couverts par le secret bancaire dans la limite des faits visés dans la commission rogatoire. | Le secret professionnel est opposable au juge civil.<br><br>***<u>En enquête préliminaire</u>*** , l'OPJ ne peut requérir les documents ou informations couverts par le secret professionnel qu'avec l'autorisation du Parquet (art. 77-1-1 du CPP)<br><br>A contrario le secret professionnel peut toujours être opposé aux <u>OPJ qui agissent d'office</u> (ces enquêtes peuvent durer jusqu'à six mois sans qu'ils rendent compte au Parquet ; art.75-1 du CPP).<br><br>***<u>Réquisitions électroniques:</u>***<br>Le secret professionnel est opposable (1er alinéa de l'article 60-2 du Code de Proc. | <u>Article L.511-33</u> du Code Monétaire et Financier (levée du secret bancaire).<br><br><u>Article 60-1</u> du Code de Proc. Pénale (réquisitions en matière d'infractions pénales).<br><br><u>Enquête de flagrance</u><br>Art.53 et suivants du CPP et art. 60-1 du CPP pour le secret bancaire<br><br><u>Enquête préliminaire</u><br>*Art. 75 et suivants du CPP et art.77-1-1 du CPP pour le secret bancaire*<br><br><u>*Commission rogatoires*</u><br>*art. 151 et suivants du CPP*<br><br><u>Pour la réquisition électronique:</u> article 60-2 et R.15-33-67 à R.15-33-75 du Code de Proc. pénale. | ***<u>Au début de l'enquête</u>*:** Présentation de la réquisition, de l'ordonnance ou de la commission rogatoire qui **délimite** l'étendue des pouvoirs d'investigations.<br><br>***<u>A l'issue de l'enquête</u>*:** La rédaction d'un procès verbal est obligatoire à l'issue d'une perquisition ou à l'occasion d'une saisie. |

| Nom des Autorités | Pouvoirs de l'autorité | Limitations des pouvoirs | Textes | Déroulement de l'enquête |
|---|---|---|---|---|
| | ***Réquisitions électroniques*:** Un officier de police judiciaire peut faire une demande de mise à disposition par procès verbal. Les informations ainsi sollicitées sont mises à disposition de l'OPJ soit dans un fichier spécifique soit par un accès temporaire et limité à la base de données de la personne morale sollicitée. Le fait de refuser sans motif légitime est sanctionné par une amende.<br><br>***La saisie contrefaçon*** *:*<br>Les commissaires de police, à la demande de tout auteur d'une œuvre protégée saisissent les reproductions illicites d'une œuvre. Un huissier de justice peut également procéder à une saisie contrefaçon sur ordonnance du président du TGI du lieu de la contrefaçon.<br>Il peut y avoir accès indirect à une messagerie si la contrefaçon porte sur un logiciel de messagerie : il y a alors saisie dudit logiciel de messagerie. | Pénale.<br>Il s'agit ici d'une demande de communication, l'OPJ ne pourra avoir directement accès à la messagerie d'un salarié. | Pour la saisie contrefaçon : art.L.332-1 du CPI | |

# *Annexe V : Liste des membres du groupe de travail.*

## *VERS UNE POLITIQUE*

## *D'ARCHIVAGE ÉLECTRONIQUE*

## *DES DOCUMENTS*

| | | | |
|---|---|---|---|
| Martine | BOCCARA | *Juriste* | BNP PARIBAS |
| Xavier | BOIDART | *Consultant en sécurité de l'information* | CREDIT AGRICOLE SA |
| Agnès | CHATELIER | *Juriste Protection des Données Personnelles* | BNP PARIBAS |
| François | COUPEZ | *Responsable Adjoint du Droit des Nouvelles Technologies* | SOCIETE GENERALE |
| Eric | COURTAIN | *Responsable Déontologie et Procédures IT* | BNP PARIBAS |
| Bertrand | EUGENIE* | *Responsable Conservation Documentaire* | CREDIT MUTUEL ARKEA |
| Stéphane | HENRY | *Responsable de la Division Informatique et NTIC* | CREDIT AGRICOLE SA |
| Yves-Marie | LECOCQ | *Juriste Nouvelles Technologies-Achats au sein de la Direction des Affaires Juridiques* | SOCIETE GENERALE |
| Sabine | MARCELLIN* | *Juriste / Co-directeur de la rédaction du Guide Lamy Droit de l'Informatique et des Réseaux* | CALYON CREDIT AGRICOLE CIB |

### *Avec la contribution de :*

| | | | |
|---|---|---|---|
| Wilfrid | GHIDALIA | *Secrétaire général* | FORUM DES COMPETENCES |

* Animateurs du groupe de travail