Archiver l'information

Jean-Luc SABOURIN
Enseignant en informatique à l'Université de la Rochelle.
UNJF

Légende

 Entrée du glossaire

 Sigle et acronyme

 Référence Bibliographique

 Jurispridence

 Texte de loi

Table des matières

Avant-propos

I

A. Fiche descriptive

1. Informations générales

Domaine

L'établissement, la transmission et la conservation des informations juridiques

Titre du module

Archiver l'information

Auteur

Jean-Luc SABOURIN
Enseignant en informatique à l'Université de la Rochelle.

Code référentiel

D4-4

Durée

10 heures

2. Prérequis

Avoir déjà parcouru l'item D4-3.

3. Mots clés

Archivage, cryptographie, preuve littérale, force probante, stockage, dématérialisation, délai de conservation, document numérique, métadonnées, environnement de confiance, signature.

Savoir

II

A. L'archivage en général

1. Qu'est-ce qu'une archive ?

Avant tout, il faut définir ce qu'est une archive. Si l'on interroge le commun des mortels, on obtient le plus souvent une réponse à la conception ordinaire et la plus usuelle : « Une archive, c'est un document ancien, et essentiellement sous forme papier ! C'est un document administratif, de la "paperasse" dont on n'a plus besoin, mais qu'on est obligé de garder... Alors on le stocke...»

Cette définition simpliste est évidemment très réductrice et ne résiste pas à l'analyse.

La notion traditionnelle de document a totalement évolué depuis l'avènement de l'informatique : Un fichier texte ou un e-mail est-il un document ? Oui, si l'on se réfère à l'usage qu'on en fera, mais évidemment non dans sa forme !

Une archive n'est pas nécessairement ancienne. En fait dès lors qu'il n'est plus appelé à évoluer, un document est éligible au statut d'archive. Par exemple, une facture émise n'évoluera plus jamais. Même si elle comporte des erreurs, on émettra un avoir, ou une autre facture, mais la facture initiale ne sera pas modifiée pour autant et devra être conservée.

Définition: Définition informelle de la notion d'archive

Les archives sont l'ensemble des documents produits dans l'exercice d'une activité pour garder trace des actions d'une personne, ou d'une organisation publique ou privée à travers des supports variés tels des papiers, des photographies, des données électroniques... mais aussi des films sur support photographique, ou encore des données électroniques stockées sur une disquette ou sur un cédérom...

Bien qu'il n'existe pas de définition « universelle » de la notion d'archive, on peut néanmoins, en prenant en considération ces différents points et au regard de la loi française (Code du Patrimoine), en proposer une bien plus satisfaisante :

Définition: Définition de la notion d'archive tirée du code du patrimoine

...Les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité...

A cette définition, il faut ajouter le texte de référence qui organise le régime des archives constitué par la loi du 3 janvier 1979 sur les archives, intégrée dans le code du patrimoine.

2. Terminologie

Dans l'usage courant, les termes *enregistrer, sauvegarder* ou *archiver*, qui traitent du stockage de l'information, sont souvent utilisés de façon globalement équivalente. Or ces termes ont des sens bien précis dans le domaine de l'informatique :

- *Enregistrer* : action qui consiste à stocker l'information sur la mémoire de masse de son ordinateur (disque dur, disque SSD, etc.) ;
- *Sauvegarder* : action qui consiste à dupliquer l'information (par exemple sur un disque dur externe) afin de pouvoir la restaurer en cas de problème ;
- *Archiver* : action qui consiste à conserver les données de manière fiable et fidèle dans le temps.

Dans le domaine juridique, une distinction est importante par rapport au domaine de l'informatique : le stockage de l'information est un acte matériel alors que l'archivage est un acte juridique.

3. Qu'est ce que l'archivage ?

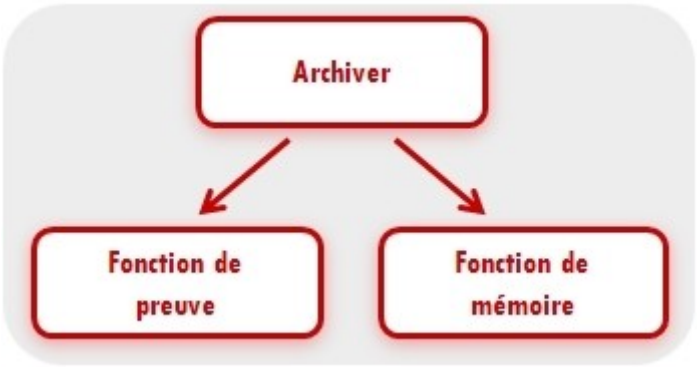
Le Code du Patrimoine français en propose une définition assez généraliste :

Définition: Définition du code du patrimoine

« ...L'ensemble des actions, outils et méthodes mises en œuvre pour conserver à moyen ou long terme des informations, dans le but de les exploiter éventuellement ultérieurement... »

4. Pourquoi archiver ?

Il va sans dire que la mise en œuvre de l'archivage représente un effort pour toute organisation. Des investissements humains et matériels, parfois lourds, peuvent s'avérer nécessaires, et doivent donc trouver une réelle justification. Chaque organisation peut avoir ses spécificités, mais on peut considérer que les deux principales motivations pour archiver sont les suivantes : répondre à la fonction de mémoire et de preuve.



La fonction de mémoire :	La fonction de preuve :
Archiver, c'est assurer, à partir du rassemblement d'éléments antérieurs, une base de référence en vue d'une action opérationnelle et d'une prise de décision éclairée (administration, finance, vente, marketing, etc.). La fonction de mémoire permet donc de répondre aux besoins internes de l'entreprise, de l'organisation ou de l'administration. Elle permet de : • Faire des vérifications et analyses financières ou comptables. • Préserver le savoir interne en vue de prises de décisions et actions opérationnelles. • Retrouver rapidement un document recherché. Cela permet dans la gestion courante d'un service (en administration comme en entreprise) de disposer en permanence des	Archiver, c'est pour l'entreprise ou l'organisation la possibilité d'apporter la preuve de ses engagements et de l'exécution de ses obligations vis-à-vis d'un grand nombre de partenaires : actionnaires, fournisseurs, clients, salariés, administration, justice, etc. Pour cela, elle devra fournir des documents à valeur probante (par exemple devant un juge). Cela implique que le système d'archivage doit ajouter à la conservation stricte du document, les conditions de conservation de sa valeur probante.

La fonction de mémoire :	La fonction de preuve :
informations utiles. • Restituer des documents à l'identique ou dans un format le plus proche possible de l'original.	

B. L'archivage électronique

1. Problématique

Jusqu'à une période extrêmement récente, l'archivage ne reposait que sur la conservation physique de supports documentaires. Grâce au développement des technologies de l'information, on dispose maintenant d'une alternative à ces méthodes : **l'archivage électronique**.

Les motivations et finalités de celle-ci sont bien évidemment les mêmes que celles de l'archivage traditionnel, mais l'utilisation de supports numériques pose plusieurs questions :

- Techniquement, comment faire ? En particulier parce que le contenu archivé est considéré comme figé et ne doit donc pas pouvoir être modifié.
- Les technologies utilisées évoluant très rapidement, que retrouvera-t-on dans dix ou vingt ans ?
- L'utilisation de supports numériques permet-elle de garantir que les documents produits auront la moindre valeur de preuve ?

De plus, la réflexion est différente selon qu'il s'agit de :

- Numériser des documents papier en vue de l'archivage.
- Archiver des documents qui sont numériques dès leur création (mails, factures électroniques...).

2. Définition

« L'archivage de contenus numériques est l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, classer et conserver des contenus électroniques sur un support sécurisé dans le but de les rendre accessibles dans le temps , que ce soit à titre de preuve ou à titre informatif. »

3. Spécificités de l'archivage électronique

L'utilisation de supports numériques offre des avantages tout à fait significatifs par rapport à l'archivage papier traditionnel.

Consultation directe des archives depuis un poste utilisateur	Accès permanent	Concurrence d'accès	Réduction des coûts	Réduction des risques
Dans la majorité des cas, l'accès à un système d'archivage traditionnel passe par la formulation d'une demande auprès d'un service d'archives. Un système d'archivage électronique peut permettre la consultation directe des archives, depuis le poste de travail de l'utilisateur. D'autre part, il permet plus facilement de fédérer, à travers un outil de recherche unique, l'accès à différents fonds.	L'archivage électronique peut permettre un accès permanent (7 jours sur 7, et 24 heures sur 24) aux archives, quelle que soit la localisation du demandeur. De même, dans le cas de l'archivage électronique, la concurrence d'accès à une archive ne pose aucun problème.	Chose impossible dans le cas de l'archivage traditionnel, l'archivage électronique permet à plusieurs personnes de consulter le même document en parallèle.	La gestion d'archives physiques traditionnelles nécessite de la mise en œuvre d'une logistique relativement lourde. Il faut pouvoir disposer de locaux et de personnel dédiés, et souvent de moyens de reprographie. Le passage à un système d'archivage électronique permet de réduire, voire d'éliminer les coûts induits par cette structure.	Ce dernier aspect est certainement le domaine où l'archivage électronique présente les avantages les plus décisifs par rapport aux méthodes traditionnelles : **Confidentialité** : le passage à un archivage électronique permet de mettre en place un contrôle strict des accès (et donc de garantir la confidentialité des documents) et une traçabilité complète des accès aux archives. **Perte :** les risques de perte de documents archivés lors de leur consultation, ou suite à une erreur de reclassement, sont éliminés. **Sinistre :** on pense naturellement à la réduction des risques liés à des sinistres « spectaculaires », tels qu'un incendie ou une inondation, mais des aléas plus insidieux peuvent également mettre en péril un fond d'archive : humidité, insectes, rongeurs, etc., ou plus simplement la mauvaise qualité des papiers ou des encres... On dispose aujourd'hui de tous les moyens techniques nécessaires (backup, réplication, etc.) à la sécurisation de manière satisfaisante du système d'archivage électronique.

4. L'archivage légal n'existe pas

Une clarification s'impose quant à l'utilisation des termes « archivage légal » et « archivage à valeur probatoire ». Le premier est impropre et devrait être banni. Il n'y a pas de loi, pas de label, pas de norme qui confère à un produit ou un service d'archivage l'étiquette « légal ». En cas de conflit sur la valeur probatoire d'un document, c'est le juge qui décidera de sa fiabilité, en vertu des pouvoirs qui lui sont conférés par les textes.

Mais si c'est au juge de décider, il fondera cette décision sur les éléments d'appréciation qui seront portés à sa connaissance. Il faut en conséquence que le système d'archivage réponde aux exigences posées par la loi pour attribuer une valeur probante à un écrit numérique.

Il est fondamental de conserver, au-delà du document lui-même, tous les éléments « probatoires » qui pourront étayer sa validité.

C. Système probatoire français et archivage

1. Organisation

Le système probatoire français s'organise autour de deux concepts : la preuve libre et la preuve légale. La preuve libre signifie que tous les moyens de preuve (témoignages, commencements de preuve, ...) seront recevables par le juge en cas de litige. La preuve légale vise les cas pour lesquels la loi impose certains moyens de preuve comme un écrit, signé le plus souvent.

La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et de la communication et relative à la signature électronique intègre les écrits sous forme électronique dans le **système probatoire légal français**.

Premier exemple, *l'article 1341 du Code civil*[1] impose de recourir à un écrit signé pour tout acte sous seing privé (acte qui n'est pas conclu devant un officier ministériel) dont le montant est supérieur à 1.500 euros.

Deuxième exemple, en cas de litige, l'entreprise doit pouvoir arguer d'une preuve et notamment d'un écrit signé. La preuve est essentielle en droit car toute prétention juridique passe par une exigence de **justification des droits**.

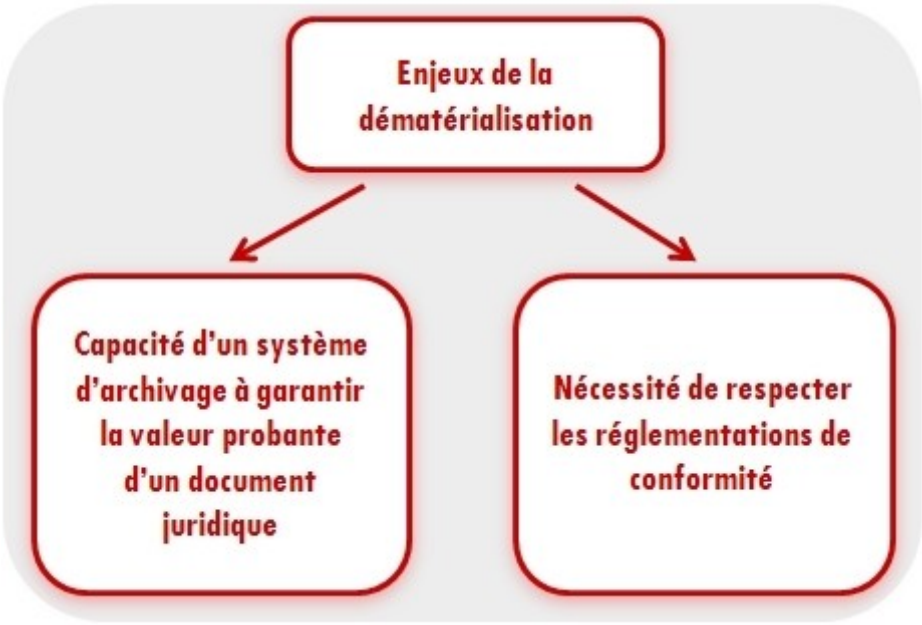
1 - http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006438186&cidTexte=LEGITEXT000006070721&dateTexte=20100503&oldAction=rechCodeArticle

Conseils, trucs et astuces

L'entreprise aura intérêt à mettre en place un système d'archivage électronique sécurisé pour l'ensemble de ses documents.

La difficulté majeure de l'archivage électronique réside dans l'absence de règles uniformes de conservation.

2. Les deux enjeux du système d'archivage



Toute opération de dématérialisation comporte deux enjeux bien différents, que l'on a parfois tendance à confondre :

- **Le premier enjeu** est celui de la **capacité d'un système d'archivage à garantir la valeur probante d'un document dématérialisé**. Il peut s'agir du contenu d'un contrat conclu en ligne entre un établissement financier et son client ou du montant des créances cédées sous forme électronique. Dans cette hypothèse, le risque se résume en un adage latin bien connu : *« Ne pas avoir de preuve revient à ne pas avoir de droit »*.

Conseils, trucs et astuces

Il est donc nécessaire de trouver des procédés et des organisations qui permettront d'avoir avec une assurance raisonnable que des documents restitués plusieurs années après leur création, sous forme papier à partir des enregistrements numériques, ou tout simplement visualisés à l'écran, sont bien fidèles à leur état original, et ce sans recourir systématiquement à une expertise.

Remarque

S'offrir un système d' « archivage à valeur probatoire », a un certain prix. Et ce prix sera d'autant plus élevé que le système sera plus fiable et que la durée de conservation sera longue. Cette réflexion sur l'analyse de la valeur doit être faite au moment de la conception du système d'archivage car elle est structurante : compte tenu de l'envahissement endémique des entreprises par l'information numérique, ce serait un pur non sens de conserver de la même façon une messagerie d'entreprise et des contrats d'assurance vie.

- **Le second enjeu** est lié à la **nécessité de respecter les réglementations de conformité** qui se sont multipliées récemment : Sarbanes Oxley Act, Loi de Sécurité Finnaière, Bâle II et règlement CRBF 97, Loi Informatique et Liberté, Contrôle fiscal de comptabilité informatisée, facturation électronique, CFR 21 Part 11, etc.

Exemple

Ces réglementations sont soit sectorielles, soit réservées à un type de données particulier. Certaines concernent les établissements bancaires, d'autres l'industrie pharmaceutique. Certaines portent sur les données à caractère personnel et d'autres sur les factures.

A chacune de ces règles sont associées des sanctions, en cas de non respect de celles-ci. Lors de la conception d'un système d'archivage, il faut se demander si les documents à conserver tombent sous le coup de l'une de ces règles et si oui quelles sont les contraintes qui en découlent et les risques encourus à les ignorer ?

Exemple

A titre d'exemple, dématérialiser les factures sans respecter les préconisations de l'administration fiscale en termes de signature électronique et d'archivage expose l'entreprise à un risque de redressement sur l'assiette de la TVA.

3. La valeur probatoire d'un document numérique

Quelle est la valeur probatoire d'un document numérique ?

Cette question est celle à laquelle il faut répondre pour établir les spécifications fonctionnelles de base du système d'archivage. Car à tout document numérique est associé un enjeu probatoire, qui sera plus ou moins important.

L'écrit numérique est fondamentalement différent de l'écrit papier en ce que **l'information est dissociée du support**. L'écrit papier est un objet statique et intangible, dans lequel l'information et le support sont intimement liés.

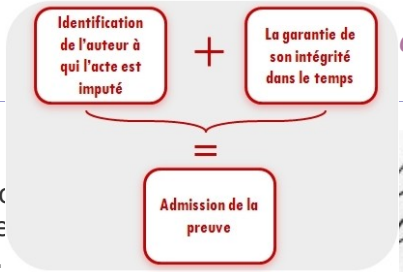
L'information signifiante s'induit de l'apparence visuelle du support (date, signature, papier à en tête, contenu). Dans un écrit numérique composé de données structurées, ces éléments sont épars, et le système d'archivage devra les gérer d'une façon telle que l'information signifiante portée par un tel écrit puisse être conservée et reconstituée fidèlement.

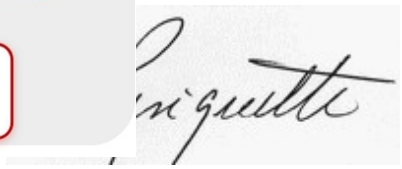
L' « écrit numérique » est un concept récent, introduit dans le droit français par la loi n°2000-230 du 13 mars 2000 à travers l'article 1316 du Code civil. Cet article, et en particulier *l'article 1316-1 du Code civil*[2] affirme l'équivalence de force probante entre les écrits sous forme papier et les écrits sous forme électronique. La preuve littérale sous forme électronique est admise à une double condition : **l'identification** de l'auteur à qui l'acte est imputé et la **garantie de son intégrité** dans le temps. Les conditions propres à son établissement y sont donc posées :

Etre capable de connaître son origine.	**Etre établi et conservé dans des conditions de nature à en garantir l'intégrité.**
Cette condition doit être comprise au sens de savoir qui est la ou les personne(s) physique(s) ou morale(s) qui portent les engagements, ou la responsabilité, du document en question.	Cela signifie que l'objet archivé n'a pu en aucune manière, être modifié, altéré ou dénaturé depuis qu'il a été créé. Cette condition ne fait que traduire un critère qui était assuré de façon naturelle par le support matériel du papier, et qui est tout sauf naturel dans le monde numérique.

2 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=53C8C633186BF34891765D832D6E10D8.tpdjo02v_1?idArticle=LEGIARTI000006437813&cidTexte=LEGITEXT000006070721&dateTexte=20100503

En savoir plus: Etre capable de connaître son origine.





Pour identifier de manière ou les personne(s) à l'o document, les procédés de électronique sont utilisés. rentrerons pas ici dans l'explication détaillée du fonctionnement de ces procédés. Vous trouverez, en effet, toutes les informations utiles dans le cours du domaine .... A compléter... du C2I niveau 2 métiers du droit.

Telle que définie par les textes, c'est-à-dire délivrée par un Prestataire de Service de Certification Electronique, la signature électronique permet à la fois d'identifier les personnes à l'origine d'un document, mais permet aussi de garantir l'intégrité de ce document. En effet, le mécanisme de signature électronique intègre un calcul préalable d'empreinte sur le document à signer. Concrètement, c'est cette empreinte qui va être signée. Ce mode de fonctionnement permet d'identifier les auteurs (les signatures utilisées appartenant bien aux signataires) et de garantir l'intégrité du document (l'empreinte calculée sur un document modifié serait différente de l'empreinte signée initiale).

La signature permet donc, à elle seule, d'assurer de façon complète et fiable les fonctionnalités qui permettent d'accorder une valeur probante à un écrit numérique.

Elle présente un intérêt évident lors de transactions distantes. Elle n'est pas néanmoins un passage obligé de l' « archivage à valeur probatoire », dès lors que le processus mis en œuvre donne des garanties suffisantes de pouvoir identifier l'origine de l'information et d'assurer son intégrité.

En savoir plus: Etre établi et conservé dans des conditions de nature à en garantir l'intégrité.

On voit là apparaître un élément fondamental de la compréhension de l'écrit numérique. Contrairement à l'écrit papier, figé une fois pour toute sous forme d'un « original », l'écrit numérique va vivre, se transformer, changer de support et parfois même de format, au cours des différents cycles de son existence depuis sa création, son stockage, son versement en système d'archivage et jusqu'à sa restitution ou sa destruction. Les deux conditions posées par l'article 1316-1 du Code Civil devront être assurées pour l'ensemble du cycle de vie de l'écrit numérique, ce qui impose de voir l'archivage numérique, eu sens large, non pas comme une action ponctuelle mais comme la mise en œuvre d'un processus pérenne au cours du temps.

Tous les événements survenant sur une archive doivent donc être tracés et contrôlés pour éviter le moindre doute quant à sa validité.

Bien que le principe de la conservation soit inscrit dans la loi, aucune modalité précise d'archivage n'y est détaillée.

Exemple: Actes

Lorsqu'un écrit est requis à des fins de validité pour un acte (ex : offre préalable de crédit...), *l'article 1108-1 du Code civil*[3] renvoie aux articles 1316-1 et 1316-4 du Code civil en ce qui concerne les conditions à respecter. Ces actes devront être établis et conservés dans les mêmes conditions que celles exigées en matière de preuve des actes sous forme électronique. En conséquence, l'archivage électronique ne doit pas se limiter au seul écrit mais doit prendre en compte l'ensemble des éléments qui participent à la légalité du document.

L'ordonnance du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique a précisé les conditions dans lesquelles certaines formes exigées à titre de validité des actes juridiques (par exemple : LRAR, formulaire de rétractation) peuvent être dématérialisées.

3 - http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006436118&cidTexte=LEGITEXT000006070721&dateTexte=20100503&oldAction=rechCodeArticle

Exemple: Commandes en ligne

Pour les commandes en ligne (écrits non signés), *l'article L.134-2 du Code de la consommation*[4] dispose que *« lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel* **assure la conservation de l'écrit** *qui le constate pendant un délai déterminé par ce même décret et en* **garantit à tout moment l'accès** *à son cocontractant si celui-ci en fait la demande. »*

Cet article met à la charge du professionnel une obligation de conserver le contrat conclu par voie électronique avec un consommateur. Le décret n° 2005-137 du 16 février 2005 a également fixé un montant et un délai lorsque la livraison du bien ou l'exécution de la prestation est immédiate. Le cocontractant professionnel doit en outre garantir l'accès et donc la copie à son cocontractant, à tout moment, si celui-ci formule une demande en ce sens.

Durées de conservation

Documents	années
Actes notariés	illimité
Bons de commande	10
Bons de livraison	10
Commandes clients	10
Contrats commerciaux	10
Documents fiscaux	6
Documents d'assurance	30
Factures client	10
Fiches de paye	5
Images-chèques	10
Ordres de bourse	5
Pièces comptables	10

Comme exposé, le cadre juridique propre à l'archivage électronique pose des exigences disparates en termes de contenu (documents à archiver), de durées de conservation... En effet, ces dernières sont très variables selon les domaines concernés. En France, la durée de conservation de droit commun en droit civil est de 30 ans. Toutefois, il existe de nombreuses exceptions pouvant réduire cette durée jusqu'à 6 mois.

Par ailleurs, l'archivage électronique doit respecter la durée de conservation des actes authentiques électroniques, c'est-à-dire une **durée illimitée**.

4. Archives publiques et archives privées

4 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=8664EB78A8622625650C57B137E352AA.tpdjo02v_1?idArticle=LEGIARTI000006292189&cidTexte=LEGITEXT000006069565&dateTexte=20100503

Définition

Le Code du Patrimoine (Article L 211-4) opère une distinction riche de conséquences entre archives publiques et archives privées. Le code définit ce que sont les archives publiques de manière assez simple : constituent des archives publiques l'ensemble des documents produits par les collectivités et établissements publics. Il pose comme principe que tout ce qui n'en relève pas relève des archives privées.Ces dernières sont, en substance, l'ensemble des documents des personnes physiques ou morales de droit privé.

Les archives publiques sont imprescriptibles, comme le précise l'article L. 212-1 du code du patrimoine et le législateur a admis les supports électroniques avec l'article 1er de la loi du 3 janvier 1979 :

« Les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, (...) ».

a) Différences

L'intérêt de cette distinction entre public et privé n'est pas mineur et induit des différences sur l'organisation du service des archives.

Quand ils sont gérés par des collectivités publiques, les services des archives sont présumés neutres. A condition qu'ils respectent les principes généraux posés par les textes, ces services n'ont pas à démontrer le sérieux ni la validité de leur organisation. En revanche, quand ils sont gérés par des organismes privés, les services privés d'archives doivent démontrer leur neutralité. En d'autres termes, la nature publique ou privée des personnes qui conservent les documents fait peser sur lesdits documents soit un préjugé favorable de neutralité, soit un soupçon de partialité.

Exemple

Par exemple en droit public, la passation de marchés publics par voie électronique implique de recourir à l'archivage électronique.

Dans ce cas, c'est la signature électronique de ce marché par la personne publique qui lui conférera le caractère de seul exemplaire de référence. Les autres pièces relatives aux marchés publics destinées à être archivées devront être attestées ou certifiées par la personne responsable du marché.

b) Spécificités de l'archivage public

Les archives publiques ne font pas l'objet de prescriptions juridiques particulières quant à leur forme, date et support. L'archivage électronique est donc compatible avec le cadre juridique applicable aux archives publiques.

L'archivage public présente toutefois une finalité orientée vers l'information du public. L'objectif est dans ce cas la conservation historique (conservation de la mémoire des informations comprises dans le patrimoine national d'où le caractère imprescriptible), mais aussi la réalisation de statistiques.

Ainsi dans le domaine public, il existe une obligation d'archiver certains documents à des fins informationnelles, historiques ou statistiques qui vient s'ajouter à l'archivage dont la finalité est juridique.

Les conditions de réalisation de l'archivage n'ont pas vocation à être identiques dans les deux cas, même si dans tous les cas les documents doivent être conservés de nature à en garantir l'intégrité et organiser son accessibilité.

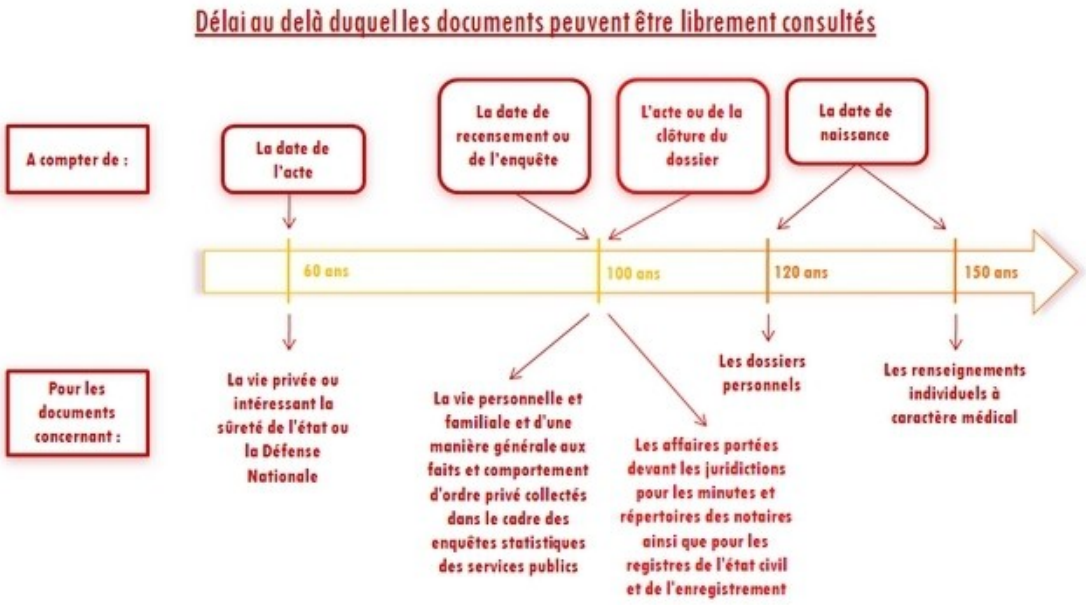
Aux termes de l'article 2 du décret 79-1037 du 3 décembre 1979 modifié, précisé par la circulaire du 2 novembre 2001, il convient de distinguer :

- les **archives courantes** qui correspondent aux documents utilisés pour le traitement quotidien des affaires dont la conservation est assurée dans le service d'origine ;
- les **archives intermédiaires** qui correspondent aux documents qui, n'étant plus d'un usage courant, doivent néanmoins être conservés temporairement à proximité des services d'origine pour les besoins administratifs ou juridiques ;
- les **archives définitives** qui correspondent aux documents qui sont conservés indéfiniment, pour les besoins de la gestion et de la justification des droits des personnes pour la documentation historique de la recherche. Ces archives définitives ou historiques sont constituées après tri et élimination, à partir des archives intermédiaires.

Les documents passent d'une des périodes précités à une autre, en fonction de leur **Durée d'Utilité administrative (DUA).** Cette durée correspond au délai minimal durant lequel les documents doivent être conservées dans les locaux des établissements ou services producteurs, en tant qu'archive courante ou intermédiaire. Elle est déterminée en fonction des besoins du service producteur ou des délais de recours légaux. La DUA d'un document est déterminée au moyen d'un acte réglementaire ou par le biais de tableau de gestion adopté conjointement par le service producteur et l'administration des archives.

De fait, les DUA peuvent correspondre à des délais parfois très courts (un an pour un acte d'extrait d'acte civil) ou aller jusqu'à l'infini en cas d'archive définitive. Le délai de communication publique de droit commun des archives publiques est de 30 ans. Par ailleurs et de surcroît, il doit être précisé que le délai au-delà duquel les documents d'archives peuvent être librement consultés est de :

- 150 ans à compter de la date de naissance des documents comportant les renseignements individuels à caractère médical ;
- 120 ans à compter de la date de naissance pour les dossiers personnels ;
- 100 ans à compter de la date de l'acte ou de la clôture du dossier pour les éléments relatifs aux affaires portées devant les juridictions pour les minutes et répertoires des notaires ainsi que pour les registres de l'état civil et de l'enregistrement ;
- 100 ans à compter de la date de recensement ou de l'enquête pour les documents contenant des renseignements personnels ayant trait à la vie personnelle et familiale et d'une manière générale aux faits et comportement d'ordre privé collectés dans le cadre des enquêtes statistiques des services publics ;
- 60 ans à compter de la date de l'acte pour les documents qui contiennent des informations mettant en cause la vie privée ou intéressant la sûreté de l'état ou la Défense Nationale et dont la liste est fixée par décret en Conseil d'État.



c) Contraintes du droit privé

Attention

L'archivage privé concerne les documents des personnes physiques ou morales.

Il s'agit soit d'un acte juridique ou d'un fait juridique. Selon la nature de l'opération, la qualification aura une incidence sur le système de preuve applicable.

Afin de rapporter la preuve d'un acte juridique, il est en principe nécessaire de produire un écrit passé devant notaire ou signé des parties. Une exception existe cependant pour les actes portant sur un montant inférieur à 1500 €. Comme vu précédemment, L'article 1316-1 du Code civil pose certaines exigences à finalité probatoire pour l'établissement et la conservation d'un acte juridique. L'écrit sous forme électronique sera ainsi admis à titre de preuve s'il vérifie ces exigences.

Leur preuve étant libre, tous les moyens de preuve sont donc recevables par le juge (présomptions, témoignages, aveux, serments, commencement de preuve écrite, etc.).

Conseils, trucs et astuces

Néanmoins, afin de convaincre le juge, il faudra établir la fiabilité du procédé utilisé pour archiver les moyens de preuve des faits juridiques.

Dans un souci de sécurité juridique, il est alors recommandé de s'appuyer sur les modalités d'archivage s'appliquant aux actes juridiques. Les personnes archivant des documents auraient alors la possibilité, au préalable, de s'assurer de la valeur juridique de ceux-ci. Comme en matière de fait juridique, le principe de la liberté de la preuve s'applique entre commerçants. En effet, le Code de commerce prévoit que « les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi».

N'étant pas d'ordre public, les règles déterminant les moyens de preuve ou encore la charge de la preuve peuvent faire l'objet de conventions. Celles-ci sont un gage de sécurité juridique puisqu'elles vont permettre aux parties de régler à l'avance la question de la force probante des contrats qu'elles concluent en ligne.

Exemple

Dans les contrats de consommation, il est possible d'insérer des clauses aménageant le système de preuve sous réserve, pour le professionnel, de respecter la législation en matière de clauses abusives.

L'*article L. 134-2 du Code de la consommation*[5] impose au professionnel de conserver pendant 10 ans, l'écrit constatant un contrat en ligne portant sur un montant supérieur à 120 € et de le tenir à disposition du consommateur lorsque celui-ci en fait la demande.

5 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=8664EB78A8622625650C57B137E352AA.tpdjo02v_1?idArticle=LEGIARTI000006292189&cidTexte=LEGITEXT000006069565&dateTexte=20100503

Remarque

On peut néanmoins s'interroger sur les éléments que le professionnel est tenu d'archiver en pratique (conditions générales de vente, commande, signature électronique, etc.) ou encore sur les modalités permettant au consommateur d'exercer son droit d'accès.

Exemple: Cas des factures électroniques

La loi pose le principe du recours aux factures électroniques signées dès le moment où le destinataire accepte ces factures. Celles-ci doivent être émises et transmises par voie électronique « dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique ». La durée de conservation des factures électronique dépendra de la matière et des délais de prescription qui s'y rattachent.

Le C.G.I. prévoit en outre que les factures, la signature électronique à laquelle elles sont liées ainsi que le certificat électronique attaché aux données de vérification de la signature électronique doivent être conservés dans leur contenu originel par l'émetteur et le destinataire. En matière commerciale, la durée de conservation des factures électronique sera de 10 ans, c'est-à-dire la durée à partir de laquelle se prescrivent.

Exemple: Cas des documents comptables

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

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

D. Archives publiques et archives privées

1. Introduction

Remarque

Il faut aussi rappeler que les collectivités territoriales sont propriétaires de leurs archives et qu'elles en assurent elles-mêmes la conservation et la mise en valeur avec le concours financier de l'État.

2. Différences

La problématique de la preuve en droit administratif est très différente de celle du droit civil. En effet, en droit administratif, le juge peut recevoir tous les moyens de preuve qui lui sont présentés par les parties au litige (écrit, témoignage,...).

Attention

Pour convaincre le juge, il faut que cette preuve soit fiable.

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

Par exemple en droit public, la passation de marchés publics par voie électronique implique de recourir à l'archivage électronique.

Attention

La fiabilité des documents archivés réside dans la confiance accordée à la personne publique.

Exemple

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

3. Intérêt de la distinction

a) Introduction

L'intérêt de cette distinction entre public et privé n'est pas mineur pour répondre au moins à deux questions très concrètes relatives au "comment conserver ?" : l'organisation du service des archives et la durée de conservation.

b) Organisation du service des archives

Quand ils sont gérés par des collectivités publiques, les services des archives sont présumés neutres. A condition qu'ils respectent les principes généraux posés par les textes, ces services n'ont pas à démontrer le sérieux ni la validité de leur organisation. En revanche, quand ils sont gérés par des organismes privés, les services privés d'archives doivent démontrer leur neutralité. En d'autres termes, la nature publique ou privée des personnes qui conservent les documents fait peser sur lesdits documents soit un préjugé favorable de neutralité, soit un soupçon de partialité.

c) Durée du délai de conservation des archives

4. L'archivage public et le droit

Les archives publiques ne font pas l'objet de prescriptions juridiques particulières quant à leur forme, date et support. L'archivage électronique est donc compatible avec le cadre juridique applicable aux archives publiques. L'archivage public présente également une finalité orientée vers l'information du public. Il s'agit de conservation historique ainsi que celle tournée vers la réalisation de statistiques. En ce sens, il s'agit d'assurer la conservation du patrimoine informationnel du pays. L'objet de l'archivage est ainsi la conservation de la mémoire des informations comprises dans le patrimoine national d'où le caractère imprescriptible.

Ainsi dans le domaine public, il existe une obligation d'archiver certains documents à des fins informationnelles, historiques ou statistiques qui vient s'ajouter à l'archivage dont la finalité est juridique.

Les conditions de réalisation de l'archivage n'ont pas vocation à être identiques dans les deux cas même si dans tous les cas, les documents doivent être conservés de nature à en garantir l'intégrité et organiser son accessibilité.

Aux termes de l'article 2 du décret 79-1037 du 3 décembre 1979 modifié, précisé

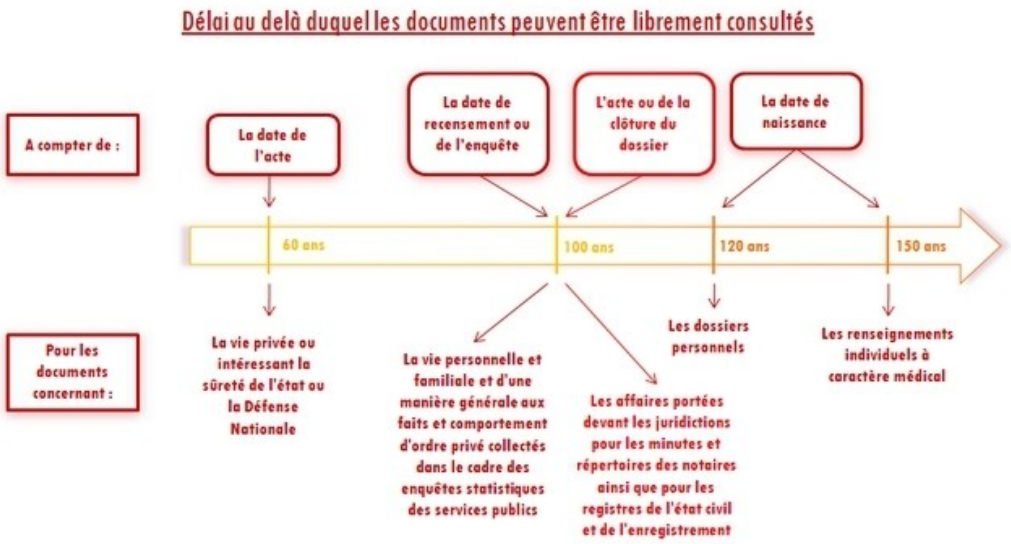
par la circulaire du 2 novembre 2001, il convient de distinguer :

- les **archives courantes** qui correspondent aux documents utilisés pour le traitement quotidien des affaires dont la conservation est assurée dans le service d'origine ;
- les **archives intermédiaires** qui correspondent aux documents qui, n'étant plus d'un usage courant, doivent néanmoins être conservés temporairement à proximité des services d'origine pour les besoins administratifs ou juridiques ;
- les **archives définitives** qui correspondent aux documents qui sont conservés indéfiniment, pour les besoins de la gestion et de la justification des droits des personnes pour la documentation historique de la recherche. Ces archives définitives ou historiques sont constituées après tri et élimination, à partir des archives intermédiaires.

Les documents passent d'une des périodes précités à une autre, en fonction de leur **Durée d'Utilité administrative (DUA).** Cette durée correspond au délai minimal durant lequel les documents doivent être conservées dan s les locaux des établissements ou services producteurs, en tant qu'archive courante ou intermédiaire. Elle est déterminée en fonction des besoins du service producteur ou des délais de recours légaux. La DUA d'un document est déterminée au moyen d'un acte réglementaire ou par le biais de tableau de gestion adopté conjointement par le service producteur et l'administration des archives.

De fait, les DUA peuvent correspondre à des délais parfois très courts (un an pour un acte d'extrait d'acte civil) ou aller jusqu'à l'infini en cas d'archive définitive. Le délai de communication publique de droit commun des archives publiques est de 30 ans. Par ailleurs et de surcroît, il doit être précisé que le délai au-delà duquel les documents d'archives peuvent être librement consultés est de :

- 150 ans à compter de la date de naissance des documents comportant les renseignements individuels à caractère médical ;
- 120 ans à compter de la date de naissance pour les dossiers personnels ;
- 100 ans à compter de la date de l'acte ou de la clôture du dossier pour les éléments relatifs aux affaires portées devant les juridictions pour les minutes et répertoires des notaires ainsi que pour les registres de l'état civil et de l'enregistrement ;
- 100 ans à compter de la date de recensement ou de l'enquête pour les documents contenant des renseignements personnels ayant trait à la vie personnelle et familiale et d'une manière générale aux faits et comportement d'ordre privé collectés dans le cadre des enquêtes statistiques des services publics ;
- 60 ans à compter de la date de l'acte pour les documents qui contiennent des informations mettant en cause la vie privée ou intéressant la sûreté de l'état ou la Défense Nationale et dont la liste est fixée par décret en Conseil d'État.


Délai au delà duquel les documents peuvent être librement consultés
A compter de :
La date de l'acte
La date de recensement ou de l'enquête
L'acte ou de la clôture du dossier
La date de naissance
60 ans
100 ans
120 ans
150 ans
Pour les documents concernant :
La vie privée ou intéressant la sûreté de l'état ou la Défense Nationale
La vie personnelle et familiale et d'une manière générale aux faits et comportement d'ordre privé collectés dans le cadre des enquêtes statistiques des services publics
Les affaires portées devant les juridictions pour les minutes et répertoires des notaires ainsi que pour les registres de l'état civil et de l'enregistrement
Les dossiers personnels
Les renseignements individuels à caractère médical

5. Contraintes du droit privé

Attention

L'archivage privé concerne les documents des personnes physiques ou morales.

Il s'agit soit d'un acte juridique ou d'un fait juridique. Selon la nature de l'opération, la qualification aura une incidence sur le système de preuve applicable.

Afin de rapporter la preuve d'un acte juridique, il est en principe nécessaire de produire un écrit passé devant notaire ou signé des parties. Une exception existe cependant pour les actes portant sur un montant inférieur à 1500 €. L'article 1316-1 du Code civil pose certaines exigences à finalité probatoire pour l'établissement et la conservation d'un acte juridique. L'écrit sous forme électronique sera ainsi admis à titre de preuve si l'auteur est identifié (dans les conditions posées par l'article 1316-4 du Code civil) et l'intégrité de l'acte est garanti. L'utilisation de la signature électronique est définie à *l'article 1316-4 du Code civil*[6] comme « un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

6 - http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006437841&cidTexte=LEGITEXT000006070721&dateTexte=20100503&fastPos=2&fastReqId=451097471&oldAction=rechCodeArticle

Attention

Concernant les faits juridiques, rien n'est précisé quant à leur conservation.

Leur preuve est libre. Tous les moyens de preuve sont donc recevables par le juge (présomptions, témoignages, aveux, serments, commencement de preuve écrite, etc.).

Conseils, trucs et astuces

Néanmoins, afin de convaincre le juge, il faudra établir la fiabilité du procédé utilisé pour archiver les moyens de preuve des faits juridiques.

Dans un souci de sécurité juridique, il est alors recommandé de s'appuyer sur les modalités d'archivage s'appliquant aux actes juridiques. Les personnes archivant des documents auraient alors la possibilité, au préalable, de s'assurer de la valeur juridique de ceux-ci. Comme en matière de fait juridique, le principe de la liberté de la preuve s'applique entre commerçants. En effet, le Code de commerce prévoit que « les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi».

N'étant pas d'ordre public, les règles déterminant les moyens de preuve ou encore la charge de la preuve peuvent faire l'objet de conventions. Celles-ci sont un gage de sécurité juridique puisqu'elles vont permettre aux parties de régler à l'avance la question de la force probante des contrats qu'elles concluent en ligne.

Exemple

Dans les contrats de consommation, il est possible d'insérer des clauses aménageant le système de preuve sous réserve, pour le professionnel, de respecter la législation en matière de clauses abusives.

Cette qualification pourra en effet être retenue, et la clause susceptible par voie de conséquence d'être réputée non écrite, dès lors qu'elle aura « pour objet ou pour effet de créer au détriment du consommateur un déséquilibre significatif entre les droits et obligations des parties au contrat ». Sont particulièrement visées les clauses ayant pour objet de limiter les moyens de preuve dont dispose le consommateur ou encore les clauses qui attribueraient la charge de la preuve à ce dernier alors qu'en principe celle-ci devrait peser sur le professionnel. En l'absence de telles conventions, c'est au juge que reviendra le cas échéant, le soin de régler les conflits de preuve conformément à l'*article 1316-2 du Code civil*[7].

L'*article L. 134-2 du Code de la consommation*[8] impose au professionnel de conserver pendant 10 ans, l'écrit constatant un contrat en ligne portant sur un montant supérieur à 120 € et de le tenir à disposition du consommateur lorsque celui-ci en fait la demande. Le délai de conservation court à compter de la conclusion du contrat « lorsque la livraison du bien ou l'exécution de la prestation est immédiate ». Si tel n'est pas le cas, « le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci».

7 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=EF68ACCC8621FB9C6DC130301BCF1367.tpdjo09v_3?idArticle=LEGIARTI000006437822&cidTexte=LEGITEXT000006070721&dateTexte=20100913
8 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=8664EB78A8622625650C57B137E352AA.tpdjo02v_1?idArticle=LEGIARTI000006292189&cidTexte=LEGITEXT000006069565&dateTexte=20100503

Remarque

On peut néanmoins s'interroger sur les éléments que le professionnel est tenu d'archiver en pratique (conditions générales de vente, commande, signature électronique, etc.) ou encore sur les modalités permettant au consommateur d'exercer son droit d'accès.

La loi pose le principe du recours aux factures électroniques signées dès le moment où le destinataire accepte ces factures. Celles-ci doivent être émises et transmises par voie électronique « dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique ». La durée de conservation des factures électronique dépendra de la matière et des délais de prescription qui s'y rattachent.

Le C.G.I. prévoit en outre que les factures, la signature électronique à laquelle elles sont liées ainsi que le certificat électronique attaché aux données de vérification de la signature électronique doivent être conservés dans leur contenu originel par l'émetteur et le destinataire. En matière commerciale, la durée de conservation des factures électronique sera de 10 ans, c'est-à-dire la durée à partir de laquelle se prescrivent.

Attention

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

Le Code de commerce prévoit que les documents comptables et les pièces justificatives doivent être conservés pendant 10 ans et ce sur tout support. Ils doivent obligatoirement être tenus par le commerçant et être « identifiés, numérotés et datés dès leur établissement par des moyens offrant toute garantie en matière de preuve ». En application de l'article L. 143-3 du Code du travail, l'employeur est tenu de conserver un double des bulletins de paie qu'il remet aux salariés lors du paiement de leur rémunération pendant une durée de 5 ans. Cette conservation peut s'effectuer sur papier ou sur support informatique dès lors que des garanties de contrôle équivalentes sont maintenues.

E. Politique d'archivage

1. Intérêt

On comprend donc l'importance pour une entreprise de mettre en place une méthodologie, une stratégie propre à l'archivage des documents. Cet archivage peut être effectué en interne (politique d'archivage interne) ou par un tiers : le tiers archiveur. Dans tous les cas, l'entreprise devra dresser un état des besoins prenant en compte les dimensions juridique, organisationnelle et technique. Cette phase visera à identifier le régime juridique des différents documents archivés par l'entreprise et de leur finalité juridique ou de gestion (courriers électroniques, actes juridiques, conditions générales, photos, plans, états de comptes bancaires, numérisation de documents papier ...).

Une fois ces exigences clairement précisées, une politique d'archivage permettra de définir les rôles et obligations de chaque acteur intervenant dans le domaine d'archivage. Elle définit les procédures à respecter en termes de procédures et outils permettant de garantir la traçabilité des actions effectuées sur les documents archivés.

Conseils, trucs et astuces

La réalisation d'audit est également conseillée.

La politique d'archivage mise en œuvre doit répondre aux exigences de conservation des documents mais encore de préservation de leur valeur probante des lors que l'électronique devient la règle.

La valeur probante des documents électroniques dépend des techniques utilisées au stade du stockage.

Techniquement, la politique d'archivage devra décrire en quoi les processus mis en œuvre permettent de répondre aux exigences :

- d'intelligibilité,
- durabilité,
- d'identification et
- d'intégrité.

2. Pas d'obligation

Attention

La mise en place d'une politique d'archivage n'est cependant pas une obligation juridique.

Mais, en détaillant les conditions de sécurité de l'archivage, ce document assurera au mieux sa fiabilité et permettra d'en rapporter la preuve devant les juges et les experts.

En outre, la Politique d'archivage doit être adaptée à la structure de l'entreprise. De ce fait, elle devra être rédigée en fonction des autres documents de l'entreprise qu'il s'agisse de la politique de sécurité de l'entreprise (surtout les grandes entreprises), la politique de gestion de preuve (pour assurer la preuve de la validité de l'écrit dans le temps), les contrats de travail, les contrats avec les prestataires, ou les chartes d'utilisation des outils informatiques ; elle doit donc être cohérente avec la politique générale de l'entreprise.

3. Spécifications

Une politique d'archivage ne peut être standard... Elle risquerait de ne pas apporter le degré de sécurité suffisant pour l'entreprise qui y est sujette.

La sécurisation juridique des informations numériques passe par la gestion de leur cycle de vie, et pas par l'utilisation de techniques éparses sans cohérence globale.

Les projets d'archivage électronique sont complexes car ils nécessitent une phase de réflexion préalable transverse à plusieurs dimensions de l'entreprise :

La dimension juridique	La dimension technique et organisationnelle
Identification des contraintes juridiques liées à l'information considérée (durée de conservation, enjeu probatoire, mise en évidence des contraintes éventuelles de compliance).	Qui devra apporter des réponses techniques aux spécifications issues de l'analyse juridique préalable, tout en intégrant les préconisations issues des normes d'archivage.

Remarque

Nous souhaitons insister sur l'importance de la documentation, plus couramment appelée « *Politique d'archivage* » .

Attention

La capacité de l'entreprise à produire sa politique d'archivage, en cas de litige sur un document restitué par son système, sera un gage a priori de la qualité du document, avant ou même en dehors de toute expertise.

4. La fonction réglementaire de la politique d'archivage

Abstraction faite des contraintes juridiques métiers, propres aux secteurs d'activité de chaque organisation, la politique d'archivage est également un outil de conformité légale.

Exemple

Ainsi, la durée peut-être déterminée par une obligation légale, par exemple obligation de conservation des données techniques de conservation (art L 34-1 du code des postes et des communications électroniques), obligation de conservation des contrats électroniques (art. 27 de la loi n°2004-575 du 21 juin 2004) ou par une prescription extinctive (cf chapitres sur archives publiques et privées).

L'obligation de conservation se double de l'obligation de destruction et de sécurité s'agissant de données à caractère personnel (Loi 78-17 du 6 janvier 1978, dite loi Informatique et Liberté).

Conseils, trucs et astuces

La CNIL (Commission Nationale Informatique et Liberté) recommande que la politique d'archivage soit formalisée et puisse être communiquée aux personnes concernées le cas échéant.

5. Les outils

Le recours aux normes n'est pas obligatoire. Toutefois, les partenaires contractuels ont la liberté d'y faire référence dans leurs conventions. Ces différentes normes peuvent servir de référentiel pour l'élaboration d'une politique d'archivage (voir chapitre Modèles et Normes).

F. Pérennité du document numérique

1. Introduction

Important

La caractéristique essentielle du document numérique par rapport au document papier tient en sa structure.

Le document papier se donne à voir dans sa simplicité voire dans la transparence de sa texture.

Le document numérique au contraire cache beaucoup plus de choses qu'il n'en montre.

2. Distinction

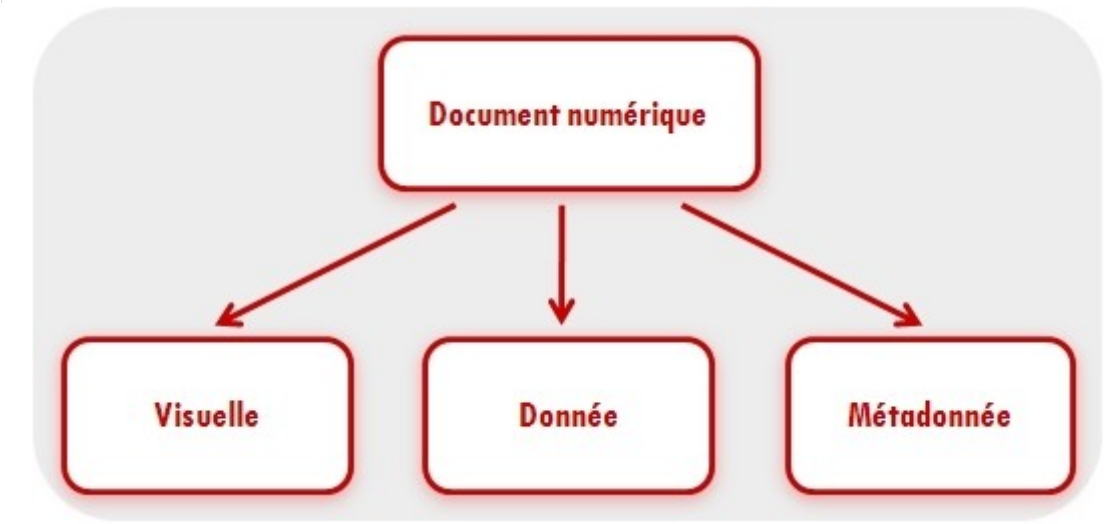
L'objet numérique dont la conservation est demandée est le document numérique. Toutefois, les textes qui exigent sa conservation intègre (archivage) ne prennent pas en compte la spécificité de cet objet. Celle-ci réside dans sa structure. La structure d'un document papier se réduit techniquement...à la qualité des fibres du papier et de l'encre utilisés.

Remarque

Celle d'un document numérique est un ensemble beaucoup plus complexe.

Elle comporte TROIS grands aspects :

Sa présentation visuelle	Les données qu'il contient	Les métadonnées
La présentation visuelle du document résulte de la manière dont il donne à voir les données qu'il comporte.	Les données sont constituées par les informations, formant un message intelligible saisi en mémoire d'ordinateur : les mots, les chiffres, les images.	Les données sont générées par le système, via l'utilisateur. Les métadonnées sont les informations générées par le système, parallèlement au contenu du document, et sans que l'utilisateur en ait conscience. • **Remarque :** **Elles sont généralement invisibles pour l'utilisateur. Elles tracent notamment les modalités de l'élaboration du document.**



3. Représentation

A côté des métadonnées qui le structurent, l'apparence physique du document peut varier en fonction du système d'information dans lequel il est lu.

Exemple

Ainsi un message électronique écrit en HTML n'a pas la même apparence en mode texte brut. Pour autant, il s'agit bien du même contenu.

Mais formellement, les changements matériels intervenus dans sa structure, donc dans sa présentation peuvent en changer le sens ou sa portée.

4. Pérennité du document numérique

Un document électronique ne peut être bien conservé à long terme s'il n'a été organisé, ni pourvu, dès sa création de la plupart des métadonnées nécessaires à sa conservation. Ces métadonnées concernent évidemment l'identification du document et ses différentes versions, sa description et son contexte de création, son classement au sein d'une arborescence pérenne, la gestion de son cycle de vie, la gestion à long terme de son accessibilité. C'est également la mise en relation et en perspective des documents et données avec d'autres documents qui donne ou ajoute du sens.

5. Les métadonnées utiles à la pérennisation

Il existe de nombreux standards de métadonnées.

Conseils, trucs et astuces

Le plus usuel et le plus simple est le Dublin Core normalisé sous la référence ISO 15836 (voir chapitre Références et modèles).

Il propose quinze éléments pour gérer des documents et des données dans un but de pérennisation.

La plupart des outils informatiques permettent aujourd'hui de gérer correctement les métadonnées.

Les plus importants sont :

L'identifiant	Les métadonnées de description	Les métadonnées de pérennisation
Il doit être unique dans l'organisation. Il doit être le plus simple possible.	• les auteurs • un titre • un type qui associé au classement peut déterminer son cycle de vie (durée d'utilité et durée de conservation) • une date de référence • les relations (appartenance à un dossier, un projet, une affaire ...) • un état : sa vie en compte quatre (document de travail, document validé, document périmé) • **les durées d'utilité :** la durée d'utilisation (DUA) contient les deux premiers âges du cycle de vie (actif ou vivant, semi-actif ou intermédiaire). L'âge actif est celui durant lequel le document sert quotidiennement pour le suivi des affaires. L'âge semi-actif est celui durant lequel le document est plus rarement utilisé. Lorsqu'il n'a plus d'utilité et n'a plus qu'une utilité de mémoire, le document peut-être conservé pour une besoin historique ou de manière définitive. (voir chapitre sur les durées) • **la durée de conservation** : Elle est déterminée en fonction du type du document, de ses usages et des risques qu'accepte de prendre l'établissement ou l'organisme. • **un historique** : Il s'agit de la gestion des versions. Chaque action doit être horodatée et on doit conserver l'identité de l'auteur.	Ce sont essentiellement des données techniques. Elles donnent de l'information sur les formats de données, sur les systèmes qui ont servi à les produire et sur leurs versions. Elles sont indispensables pour assurer la lisibilité des données et permettre la migration d'un format à un autre mieux maîtrisé. Ce sont aussi ces métadonnées qui vont régir l'accès de chaque individu aux données. On doit se conformer à la loi de 1978 et à l'ordonnance de 2005 pour tout accès.

6. Usage des métadonnées

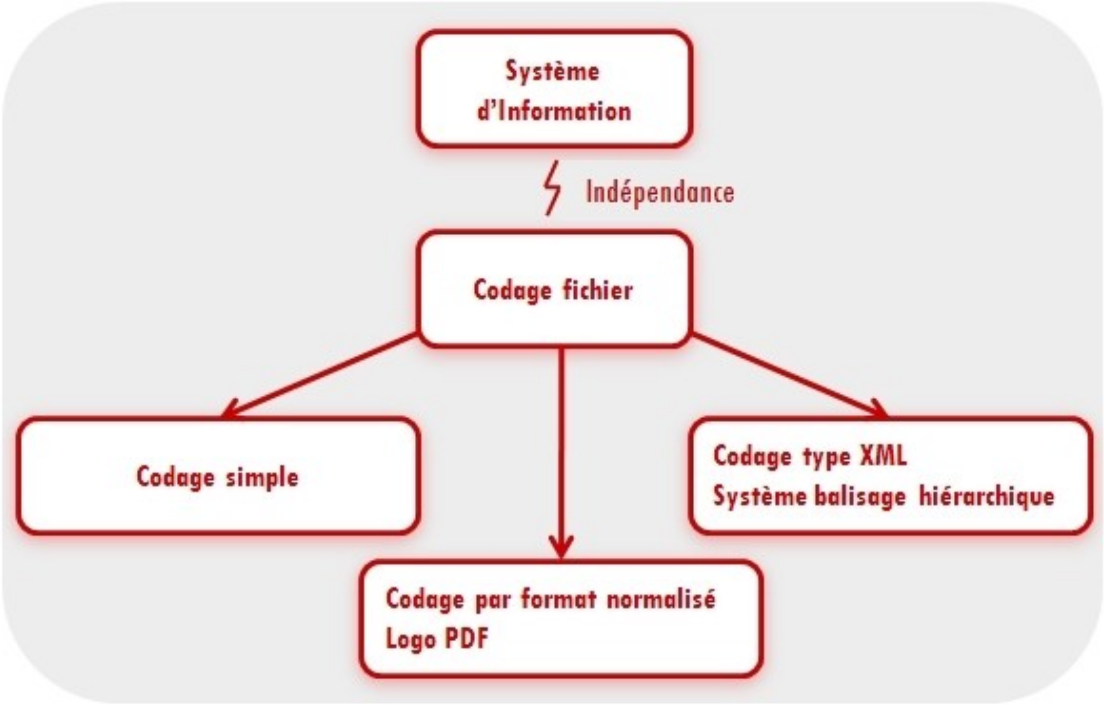
Elles servent à identifier le bon document dans le cadre d'une recherche ou d'une transmission.

Elles servent aussi à automatiser les transferts vers des systèmes d'archivage à long terme.

7. Conservation

Compte tenu de l'évolution particulièrement rapide des technologies, la conservation sur le long terme représente un véritable défi dont la réponse est autant technologique qu'organisationnelle.

- Ceci nécessite d'une part un codage des données indépendant des systèmes :
  - soit par des formats de codage très simples, ouverts et de ce fait relativement pérennes ;
  - soit par des formats normalisés adaptés à la conservation, comme le PDF;
  - soit par une structuration des données de type XML qui permet de s'affranchir d'un format propriétaire tout en facilitant la navigation au sein du document et son exploitation.



- D'autre part s'ajoute à cela la nécessité d'effectuer des migrations périodiques vers de nouveaux supports.

La conservation dans le temps ne touche pas que les supports, les contenus risquent également de perdre de leur exploitabilité s'ils ne sont pas entretenus car plus le temps passe et plus l'information peut devenir difficile d'accès.

Par ailleurs la conservation de la signature numérique pose un véritable problème dans la mesure où elle interdit toute migration de format de codage (au risque de perdre son intégrité) pourtant indispensable afin d'assurer la lisibilité sur le long terme. Cependant ceci est vrai si l'on veut conserver la possibilité de vérifier la signature dans le temps. En revanche, il est tout à fait possible de vérifier la signature une fois pour toute avant l'archivage des documents et de conserver la trace de ces contrôles en ayant par exemple recours à un tiers du type autorité de gestion de preuve qui par ailleurs permettra également de régler le problème de la faiblesse de tout procédé cryptographique qui ne peut résister indéfiniment aux avancées et évolutions techniques qui font qu'un jour ou l'autre il sera percé.

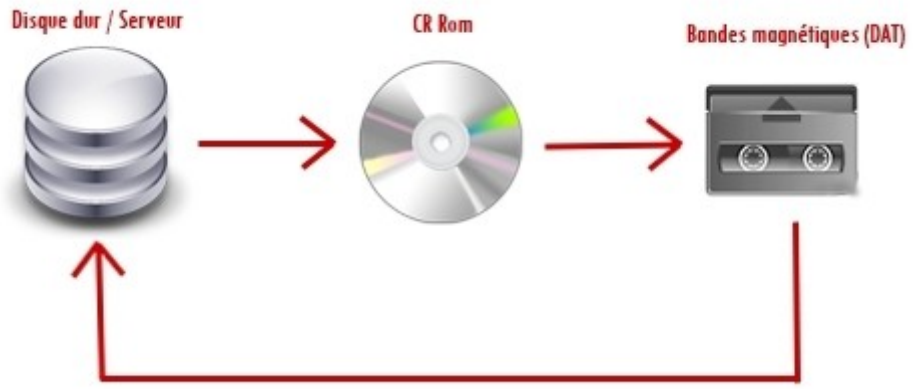
Important

L'archivage électronique se doit par définition de garantir la pérennité mais plus

encore, dans la mesure où il correspond à l'organisation raisonnée d'une conservation sécurisée de l'information créée aujourd'hui afin de pouvoir la réutiliser demain ou après demain.

Remarque

De plus en plus ce besoin d'archivage est ressenti comme une nécessité pour les entreprises et devient une obligation.



G. Conservation électronique des documents

1. Introduction

Remarque

Le forum des droits sur l'internet a publié des recommandations.

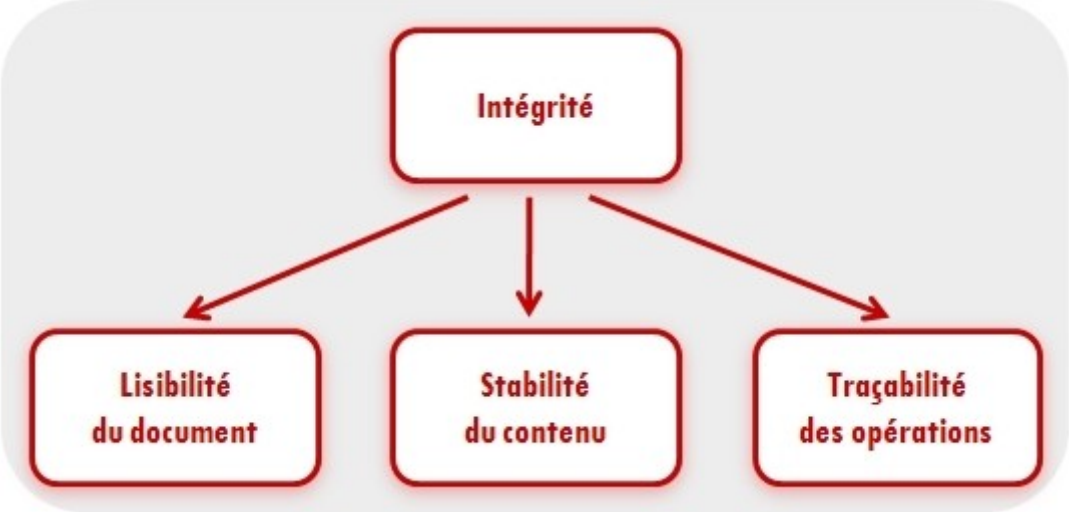
Les travaux se sont principalement concentrés sur la conservation électronique des documents dans le secteur privé (Raisons évoquées dans le chapitre Archives publiques et privées).

Ils ont pour but de favoriser le développement d'une pratique sûre de l'archivage électronique en entreprise en précisant les modalités de conservation d'un document électronique utilisable à des fins de preuve.

2. Les modalités d'une conservation électronique

La notion d'intégrité doit être assurée par le respect cumulée des TROIS critères suivants :

- la lisibilité du document ;
- la stabilité du contenu informationnel ;
- la traçabilité des opérations sur le document.



L'emploi de bonnes pratiques à travers les quatre étapes du processus de conservation qui sont le

- versement,
- l'enregistrement,
- la gestion et
- la restitution des documents.

Les migrations n'affectent pas le statut juridique d'origine du document si l'intégrité peut-être vérifiée. Dans les cas des documents signés au moyen d'un procédé cryptographique, des vérifications sont nécessaires et leurs résultats devront être conservés dans les métadonnées associées au document.

3. La mise en place d'un environnement de confiance

Le forum recommande l'emploi de contrats de services se référant aux bonnes pratiques édictées.

Il convient également que ce contrat soit accompagné de certaines clauses types.

Exemple

- Clause de sécurité,
- d'information et de conseil,
- de reprise et de continuité,
- de confidentialité,
- d'assurance professionnelle.

Le forum recommande la mise en place d'un document interne (charte ou politique d'archivage) accompagné d'un contrôle-qualité.

H. Sécurité du système d'archivage

1. Introduction

Important

Définition :

La sécurité du système d'archivage a pour objectif de protéger et valoriser l'information stockée. Cette dernière doit être sécurisée dès sa création ainsi qu'à travers les autres étapes du processus de conservation que sont le versement, l'enregistrement, la gestion et la restitution des documents.

Le terme sécurité est un ensemble qui se décompose en plusieurs critères. Les plus importants sont :

- la disponibilité,
- l'intégrité et
- l'authentification.

2. *Disponibilité*

Important

La disponibilité est un critère important de la sécurité car il a pour objectif de mettre à disposition à tout moment le document archivé pendant toute la période de conservation.

Elle se décline avant tout par la notion d'accessibilité qui permet de retrouver les données. Cette notion implique que la sécurité est en fait l'aboutissement d'une politique tant d'un point de vue organisation des données que de choix techniques.

Remarque

L'organisation offrira une structure efficace tant d'un point de vue classement que recherche.

Les choix techniques devront faire preuve de performances. Ils sont de ce fait liés aux techniques utilisées au niveau support et transmission de l'information. Les temps d'accès divergeront en fonction des supports choisis ainsi que les temps de transmission varieront en fonction du réseau.

Conseils, trucs et astuces

Ne pas recueillir d'information est en effet un problème d'indisponibilité, tandis qu'obtenir des informations fausses est un souci d'intégrité.

3. Intégrité

a) Introduction

Important

L'objet archivé n'a pu en aucune manière, être modifié, altéré ou dénaturé depuis qu'il a été créé. (article 4.f du Règlement CE n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information).

Remarque

L'intégrité représente un critère de sécurité de base.

Il est le plus difficile à mettre en œuvre sur l'ensemble du traitement de l'information. Il se subdivise en deux parties :

- celle liée aux données et
- celle liée aux traitements.

L'auteur, signataire de l'acte, doit être sûr que le document qu'il a signé (établissement), transmis et conservé est le même (contenu identique) que celui reçu et conservé, le cas échéant, par le ou les destinataire(s). L'intégrité liée aux données est mise en cause informatiquement parlant si un élément binaire (bit) a été modifié. Pour autant, comme déjà vu, cette intégrité technique est différente de l'intégrité juridique qui, elle, associe un sens au document (destination). Pour éviter toute ambigüité, le forum des droits sur l'internet (cf chapitre conservation des documents numériques) a préconisé quelques recommandations.

Exemple

L'apposition d'une signature électronique a pour effet de sceller numériquement le contenu associé. Cette caractéristique permet de déceler toute altération du document même minime. Il est donc possible, par contrôle de la signature, de démontrer l'intégrité du document présenté. Toutefois, si elle permet de les déceler, la signature électronique n'interdit pas d'éventuelles modifications du document.

En général, les atteintes à l'intégrité sont d'origine malveillante. Les cas d'accidents ou d'erreurs sont beaucoup plus rares. En effet la perte d'intégrité peut présenter des dangers vitaux. Les cas pratiques sont très nombreux et inquiétants. L'enjeu est également juridique dans la mesure où l'entreprise se doit de garantir l'intégrité de ses traitements et des flux d'informations qu'elle émet, au risque d'être condamnée comme indiqué ci-après.

b) Traçabilité

Important

La traçabilité est un des moyens de garantir l'intégrité. La traçabilité est une procédure visant à suivre automatiquement un objet (garder la trace des évènements vécus par cet objet) depuis sa naissance jusqu'à sa conservation finale ou sa destruction.

Le simple fait de constituer un journal et de tracer les différentes opérations effectuées par exemple sur un système d'archivage électronique offre une véritable garantie.

Il deviendra en effet extrêmement difficile voire impossible pour un tiers de mettre en doute le système en insinuant par exemple qu'il a été possible de modifier les journaux d'événements ainsi générés. Sur ce point la traçabilité vient donc en parfait complément de l'intégrité comme vu au sujet des recommandations du Forum des Droits sur Internet au sujet de l'intégrité du contenu de l'information.

La traçabilité revêt ainsi

- le contrôle (réalité des actions effectuées sur un objet) et
- la preuve (la trace des actions opérées).

c) Aspects juridiques

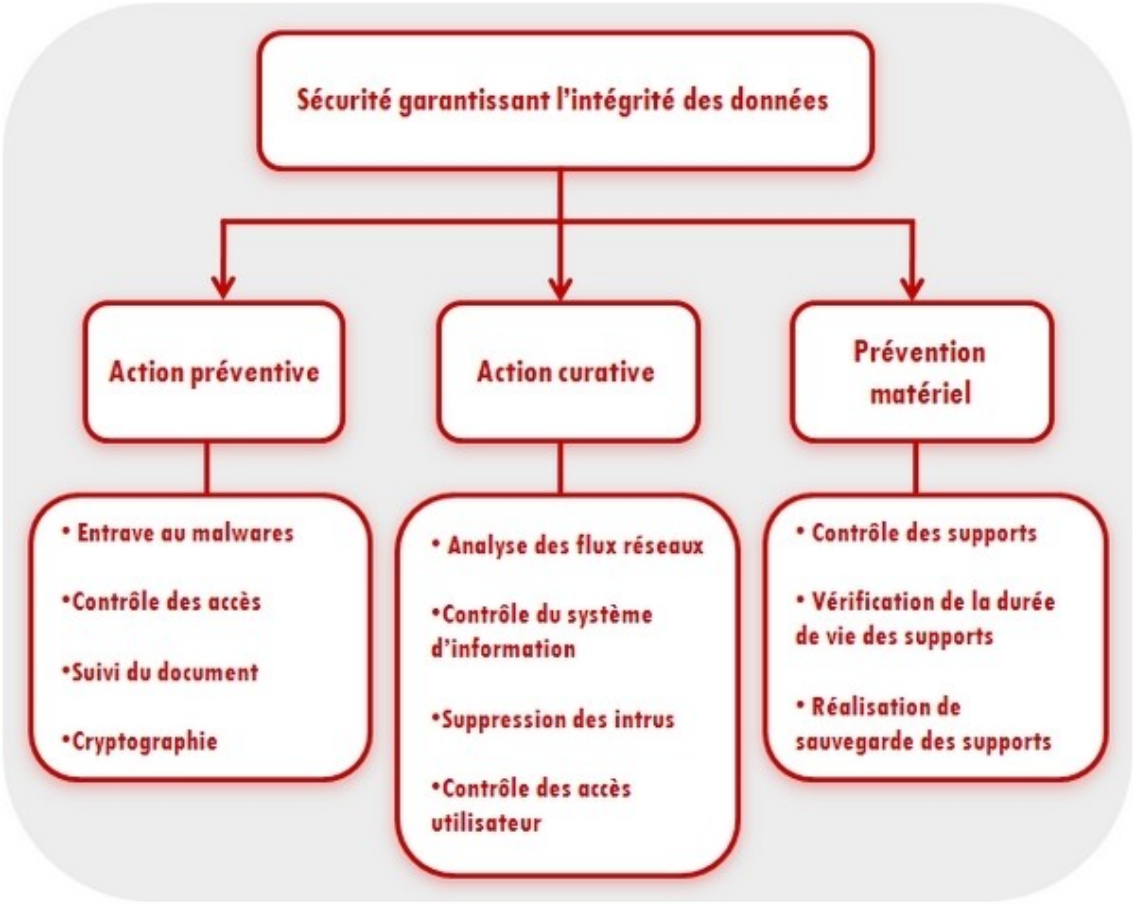
Le législateur par l'article 323-2 du code pénal cherche à punir les auteurs de virus par une peine de cinq ans d'emprisonnement et de 75.000 euros d'amende. La loi de juin 2004 relative à la confiance dans l'économie numérique (article 323-3-1 du code pénal)stipule que « le fait sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

d) Actions à mettre en œuvre pour garantir l'intégrité

Plusieurs types d'actions peuvent être mises en place dans le cadre d'un plan de sécurité.

- La **première est une action préventive** qui met en œuvre des dispositifs d'entrave aux logiciels malveillants, logiciels espions, logiciels de traçage (antivirus, anti-spams, firewall, anti–spywares ...(cf technique)) de contrôle d'accessibilité par des logiciels externes (firewall, licences, programmes espions ...), de mise en place d'identification, de suivi des documents (métadonnées, signature électronique, authentification, ...), de mise en place de chiffrement autorisée et efficace des données (cryptographie).
- La **deuxième est une action curative** qui par une analyse régulière de l'activité sur le réseau, un contrôle régulier du système d'information et de son intégrité (partie ou totalité des données), une suppression systématique des intrus (virus, spam, programmes espions... qui auraient franchi la barrière préventive, le contrôle et le suivi des accès pour veiller à l'identification et à l'authentification des personnes ayant accès à votre site informatique.
- Le **troisième est la garantie** apportée par les supports de stockage (disques magnétiques, bandes, disques optiques ...) . Ceux-ci ont une durée de vie parfois plus courte que les durées de conservation légale des documents. En outre, il sera indispensable d'effectuer régulièrement des

sauvegardes complètes des supports pour répondre à la fois aux problèmes d'intégrité des supports mais aussi aux problèmes de panne.

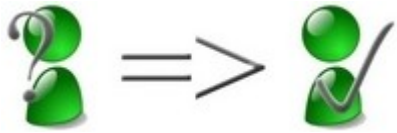


4. Identification/Authentification

a) Introduction

Important

Identifier quelqu'un consiste à établir l'identité de la personne tandis qu'authentifier revient à certifier l'exactitude de son identité.



L'article 4.e du Règlement CE n° 460/2004 du Parlement européen et du conseil du 10 mars 2004 définit l'authentification comme « la confirmation de l'identité prétendue d'entités ou d'utilisateurs ».

En matière de contrôle d'accès, il faut d'authentifier la personne après l'avoir identifié. En général, on identifie la personne grâce à un système d'identifiant (login et mot de passe).

Pour autant, rien ne garantit de façon certaine qu'il s'agit bien de la bonne personne. Une personne disposant des identifiants peut très bien usurper l'identité numérique.

Exemple

Il existe aujourd'hui d'autres procédés plus fiables d'authentification (chiffrement, carte à puce, solutions biométriques ...)

Il est donc nécessaire de réaliser un bon contrôle d'accès tant aux informations qu'aux programmes de traitement. L'enjeu consiste à faire en sorte que les informations ne soient accessibles qu'aux personnes connues d'une part (notion de confidentialité) et autorisées d'autre part (notion d'habilitation avec sa consonance légale).

b) Actions à mettre en œuvre pour l'identification/authentification

Là aussi, la politique d'archivage a dû définir les utilisateurs, les données et leurs droits d'accès. En outre, il faudra impérativement :

- définir les accès et les contrôles à instaurer.
- définir des indices de sécurité pour les informations sensibles et des niveaux d'habilitation pour les utilisateurs correspondants.
- contrôler les accès.
- effectuer une classification en termes de confidentialité et sensibilité, des informations gérées et transportées par les réseaux informatiques et télécoms de l'entreprise.
- classifier l'information.
- assurer que dans les conditions normalement prévues, seuls les utilisateurs autorisés (ou habilités) ont accès aux informations concernées (notion de confidentialité).
- Mettre en œuvre la préservation de la confidentialité par un système de chiffrement. Ce système rend les données illisibles par toute personne ne possédant pas la clé pour les déchiffrer.

c) Aspects juridiques

Attention

Les enjeux sont essentiellement de deux ordres, légal et commercial avec les conséquences financières correspondantes.

Informations à caractère personnel : L'un des premiers enjeux d'atteinte à la confidentialité touche à l'accès aux bases de données regroupant en particulier des informations à caractère personnel. Dans ce contexte, l'article 34 de la Loi Informatique, Fichiers et Libertés modifiée par la loi du 6 août 2004 (loi n°2004-801) dispose que « le responsable du traitement est tenu de prendre toutes préoccupations utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

A défaut d'avoir pris « toutes préoccupations utiles », l'employeur s'expose aux peines prévues à l'article 226-22 du code pénal. Même si ce délit est non intentionnel, l'employeur pourrait être tenu pour responsable (même à son insu) de l'imprudence ou de la négligence de ses salariés, ayant permis la divulgation d'une donnée à caractère personnel.

Attention

L'usurpation d'identité est un délit grave qui doit être combattu par la traçabilité du système d'information.

Cela devient un délit pénal dès l'instant ou « le fait de prendre le nom d'un tiers dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales » (article 434-23 du Code Pénal).

Exemple

Si le nom patronymique d'un individu est reproduit sans son autorisation dans un nom de domaine, l'usurpation d'identité pourrait être éventuellement sanctionnée civilement (article 1382 du code civil).

I. Techniques du système d'archivage

1. Introduction

La technologie doit mettre en œuvre des dispositifs permettant de décliner la sécurité à travers ses diverses composantes (disponibilité, authentification et intégrité) , la durabilité et la solidité des liens entre documents initiaux et archivés (pérennité et conservation), la force probante du système d'archivage à travers le chiffrement, la cryptographie et la signature électronique.

2. Les dispositifs de protection

Conseils, trucs et astuces

Chaque ordinateur est susceptible d'être victime d'une attaque d'un pirate informatique. Ainsi, il est nécessaire de se protéger contre les intrusions réseaux en installant un dispositif de protection.

	**Antivirus**	Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et de l'éradiquer. Ces programmes s'appuient sur la signature virale propre à chaque virus pour le détecter. Certains s'appuient sur un contrôle d'intégrité c'est-à-dire sur une modification éventuelle du fichier. L'éradication ou désinfection prend plusieurs formes : • la suppression de la signature dans chaque fichier, • la suppression du fichier infecté • la mise en quarantaine du fichier infecté, c'est-à-dire un déplacement de ce dernier dans un emplacement où il ne pourra plus s'exécuter.
	**Le système pare-feu (firewall)**	C'est un système permettant de protéger un ordinateur ou un réseau des intrusions provenant d'un réseau tiers. Il filtre les données échangées. C'est un système logiciel constituant un intermédiaire entre le réseau local et l'externe. Il contient un ensemble de règles prédéfinies permettant l'autorisation ou le blocage des connexions, de rejeter ou d'accepter les échanges. Dans le cas où le pare-feu se limite à un ordinateur personnel, celui-ci contrôle l'accès au réseau des applications installées sur la machine. Il permet également de repérer et d'empêcher l'ouverture non sollicitée de la part d'applications non autorisées.
	**Serveur mandataire (proxy)**	C'est une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet. La plupart du temps, le serveur proxy est utilisé pour le web. Il s'agit d'un serveur mandaté par une application pour effectuer une requête à sa place. Leurs fonctionnalités principales sont leur capacité à garder en mémoire les pages les plu souvent visitées, à assurer un suivi des connexions et leur filtrage (liste noire) et à permettre une authentification.
	**Système de détection d'intrusions**	C'est un mécanisme écoutant le trafic réseau de manière furtive afin de repérer les activités suspectes ou anormales et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.
	**Les réseaux privés virtuels**	Les réseaux locaux d'entreprises sont de plus en plus souvent reliés à Internet pour communiquer avec des filiales, des clients ou même du personnel éloigné. Les données sensibles ainsi transmises sur internet sont vulnérables. La première solution consisterait à relier par des lignes spécialisées les différents interlocuteurs mais le coût est trop élevé pour de nombreuses organisations. La seconde solution consiste à utiliser internet comme support de transmission en utilisant un protocole d'encapsulation, c'est-à-dire en encapsulant les

		données à transmettre de façon chiffrée. On parle ainsi de réseau virtuel pour désigner le réseau artificiellement créé.
 	**Biométrie et carte à puce**	Les lecteurs biométriques se basent sur des éléments physiques de la personne pour l'identifier. Le plus connu est celui de la prise d'empreintes digitales.

3. Les dispositifs de preuve

a) Le chiffrement

Important

Le chiffrement est le procédé par lequel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement.

L'identité de l'émetteur d'une information numérisée s'effectue au moyen de certificats électroniques délivrés par une des autorités de certification habilitées par le MINEFI, qui garantit le lien entre la personne inscrivant une signature électronique et la société qui a fait l'acquisition du certificat.

Le chiffrement est de type :

- **symétrique** quand il utilise la même clé pour chiffrer et déchiffrer.
- **asymétrique** quand il utilise des clés différentes : une paire composée d'une clé publique, servant au chiffrement, et d'une clé privée, servant à déchiffrer. Le point fondamental est l'impossibilité calculatoire de déduire la clé privée de la clé publique.

Les méthodes les plus connues sont le DES, le TripleDES et l'AES pour la cryptographie symétrique, et le RSA pour la cryptographie asymétrique, aussi appelée cryptographie à clé publique.

Important

Le Data Encryption Standard (DES) est un algorithme de chiffrement par bloc utilisant des clés de 56 bits.

Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable.

Important

Le Triple DES (aussi appelé 3DES) est un algorithme enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes.

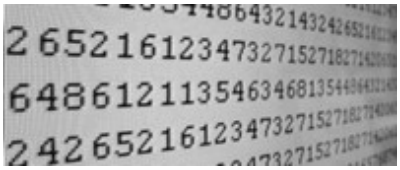
Le standard de chiffrement avancé (Advanced Encryption Standard ou AES) est un algorithme de chiffrement symétrique qui prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite selon le numéro de ligne.

Important

RSA (Rivest Shamir Adleman) est un algorithme asymétrique de cryptographie à clé publique, très utilisé dans le commerce électronique et plus généralement pour échanger des données confidentielles sur Internet.

Il a été décrit en 1977 par Ron Rivest, Adi Shamir et Len Adleman, d'où le sigle RSA. En 2008, c'est le système à clef publique le plus utilisé (carte bancaire française, de nombreux sites web commerciaux...).

b) La cryptographie



En France, une législation considérait, jusqu'en 1996, ces outils comme des «armes de guerre», en raison de leur intérêt stratégique. La loi de 1996 a assoupli la législation en distinguant le scellement qui consiste à garantir l'intégrité de chaque message par un sceau chiffré (il est libre), les opérations de confidentialité qui consistent à chiffrer le contenu du message en le rendant illisible (elles sont soumises à déclaration et demande d'autorisation).

La loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) a depuis totalement libéralisé l'utilisation des moyens de cryptologie. L'utilisation civile de ces procédés n'est pas sans inquiéter les gouvernements car en favorisant les communications secrètes entre individus malintentionnés, il y a un risque potentiel pour la sécurité intérieure mais garder le contrôle de ces techniques se heurte aux principes de la protection de la vie privée et de la liberté d'expression. Il faut composer entre les exigences de la sécurité et celles des intérêts privés (commerce notamment).

Remarque

La question est donc comment satisfaire les intérêts privés tout en assurant la sécurité nationale et l'intégrité du territoire ?

La diffusion publique des moyens de cryptographie (DES) a fragilisé les données confidentielles nationales d'où l'émergence de nouveaux procédés. Il faut en conséquence contrôler l'utilisation des moyens de chiffrement dans le cadre d'affaires pénales pour assurer la sécurité des transactions financières. La sécurité serait assurée par un système efficace de chiffrement, une authentification par des techniques de signature électronique requérant également l'utilisation d'un algorithme cryptographique. Mais les acteurs souffrent des incertitudes liées à la dématérialisation des échanges (s'assurer de l'identité de son interlocuteur peu fiable). Les échanges de données cryptées n'assurent pas que le destinataire des messages soit effectivement l'utilisateur légitime de la clé privée.

c) Signature

Attention

C'est un moyen de preuve. C'est un terme générique qui signifie plusieurs degrés de sécurité.

Le 13/12/1999, la directive européenne définit la signature électronique et précise le régime de preuve applicable aux échanges en ligne. La loi du 13/03/2000 transpose la directive, refond le droit de la preuve en droit français. Le décret d'application du 30/03/2001 précise les conditions de fiabilité de la signature.

Important

La signature correspond au processus technique qui permet au destinataire d'un message signé de donner l'assurance que ce message provient bien d'une personne déterminée, garantit l'authentification et l'intégrité pendant la transmission électronique du message (comme un sceau apposé sur le document).

La loi permet d'apporter en tant que preuve un écrit électronique et de considérer que cet écrit a même force probante que le papier.

Remarque

Les supports et les modalités de transmission deviennent indifférents.

Cet apport de la loi n'exclut pas tout conflit de preuve. Le juge déterminera alors par tous moyens le titre le plus vraisemblable. Le décret de 2001 présume que la signature est fiable si elle est sécurisée et vérifiée par un certificat électronique.

La signature sécurisée est basée sur la cryptographie asymétrique : clé publique et clé privée, signature annexée ou incluse dans le message. Il importe que la preuve soit conservée dans des conditions de nature à en garantir son intégrité.

Toute signature non sécurisée sera présumée non fiable et contestable en justice. Elle reste un moyen de preuve lorsque la preuve est libre et que la sincérité du détenteur de l'écrit ne peut être contestée. Cela signifie que la fiabilité de la signature passe par l'intervention d'un tiers à l'acte.

Sans rentrer dans le détail de la technologie utilisée, la loi lie la preuve des actes sous seing privé à la fiabilité du procédé de signature électronique utilisé. En ce sens, la "solidité" et la durabilité du lien entre la signature électronique et le message constitue un aspect fondamental. Pour bénéficier de la présomption de fiabilité ou pour la validité de certains actes juridiques, les parties devront avoir recours à la signature électronique sécurisée.

L'art. 1316-4 du code civil donne une définition fonctionnelle de la signature en général.

Important

La signature électronique (ou manuscrite) remplit deux fonctions juridiques de base : l'identification de l'auteur de l'acte et l'expression du consentement du signataire au contenu de l'acte.

Le procédé de signature électronique doit donc identifier le signataire, garantir le lien entre l'acte et la personne dont il émane et assurer l'intégrité de l'écrit signé.

Remarque

A l'heure actuelle, seules les signatures électroniques basées sur la cryptologie à clé publique (à savoir les signatures numériques) répondent aux exigences légales et plus particulièrement à la garantie de la solidité du lien entre la signature et le message.

L'identification du signataire s'effectue par le biais d'un certificat électronique d'identification, émis par un tiers. On en déduit la notion de tiers qui participe à la confiance. La demande de certificat, l'enregistrement du titulaire et sa délivrance permettent son identification. La vérification de l'identité en face-à-face (rencontre physique contre, notamment, la présentation d'une pièce d'identité) est une condition essentielle pour assurer la sécurité qui va découler ultérieurement des actes signés. C'est le Prestataire de Services de Certification électronique (P.S.C.E.) ou " autorité de certification " qui délivre un certificat électronique.

Ce certificat servira au destinataire à vérifier que c'est la personne qui dit avoir signé le document électronique et que le message (acte) est intègre (non modifié depuis le moment de sa signature). Ces fonctions juridiques sont permises par les clés de cryptographie asymétriques (2 clés).

4. Les dispositifs de sûreté de fonctionnement

a) Présentation

Il caractérise le niveau de confiance du système.

Important

Une défaillance correspond à un dysfonctionnement du service, c'est à dire un état de fonctionnement anormal ou plus exactement non conforme aux spécifications.

Il existe plusieurs moyens de limiter les défaillances d'un service par

- la prévention des fautes (éviter les fautes en les anticipant),
- la tolérance aux fautes (fournir un service conforme aux spécifications malgré les fautes),
- l'élimination des fautes (réduire par actions correctives),
- la prévision des fautes par anticipation.

Comme chacun le sait, les risques de pannes d'un système sont nombreux.

Exemple

Les origines peuvent être physiques (catastrophe naturelle, panne matérielle ou réseau, coupure électrique), humaines (erreur de conception, sabotage, piratage) ou opérationnelles (bogue, dysfonctionnement).

b) Problématique

Conseils, trucs et astuces

Il est impossible d'empêcher totalement les pannes.

Une solution consiste à mettre en place des mécanismes de duplication pour prendre le relais de préférence sans interruption de service (tolérance aux pannes).

Il est nécessaire de prévoir des mécanismes de sauvegarde idéalement sur des sites distants afin de garantir la pérennité des données contre les erreurs de manipulation ou des sinistres (sauvegarde).

La mise en place d'un équilibrage de charge consiste à distribuer une tâche à un ensemble de machines. Ce type de mécanisme s'appuie sur un élément chargé de distribuer le travail entre différentes machines. (répartiteur de charge)

Conseils, trucs et astuces

L'idéal consiste en la mise en place de plusieurs ordinateurs formant un réseau de nœuds où chacun est capable de fonctionner indépendamment des autres (cluster).

c) Solutions

i Technologie RAID

Conseils, trucs et astuces

Cette technologie permet de constituer une unité de stockage à partir de plusieurs disques durs.

L'unité ainsi créée (grappe) a une grande tolérance aux pannes et une grande capacité d'écriture. La répartition sur plusieurs disques permet d'en augmenter la sécurité et de fiabiliser les services. Plusieurs types de configuration peuvent être mis en place avec les disques selon les besoins de l'organisation.

ii Protection électrique

Un onduleur est un dispositif permettant de protéger des matériels électroniques contre les aléas électriques. Il s'agit d'un boîtier placé en interface entre le réseau électrique et les matériels à brancher. Il permet de basculer sur une batterie de secours en cas de problème.

5. Format des données

La conservation des données (cf chapitre pérennisation) nécessite des formats de données lisibles dans le temps.

Conseils, trucs et astuces

Il faudra en conséquence utiliser un codage des données indépendant des systèmes dont le format sera très simple et ouvert; normalisé et adapté à la conservation.

De surcroît, la structuration des données (métadonnées) sera de type XML à ce jour de type texte, portable, lisible. (voir norme NF Z42-013)

Conservation active :

- Plutôt que de chercher le support idéal qui n'existe pas encore, il faut prévoir dès l'origine les migrations indispensables permettant de garantir la conservation des données dans le temps.
- Il faudra adapter les moyens d'archivage électronique aux évolutions technologiques à travers le changement de support mais aussi le type de chiffrement car le risque de casser des clés de 128 bits dans les cinq à dix ans est non négligeable. En effet, si le risque demeure limité aujourd'hui, il

ne faut pas l'écarter. Cela impliquera qu'il faille "resigner" périodiquement le document électronique pour être sûr de son intégrité ou l'assurer par d'autres moyens.

- Il faudra veiller à garder l'ensemble des éléments nécessaires à la vérification dans le temps et surtout prévoir a minima d'horodater régulièrement les documents concernés afin de contourner l'obsolescence des procédés cryptographiques.

J. Référentiel et modèles

1. Introduction

Depuis plusieurs années, le développement de la dématérialisation fait que le besoin de normes destinées à permettre de définir, de concevoir, de développer, d'exploiter des systèmes d'archivage se ressent de plus en plus. En effet, la grande majorité des solutions installées étant conçues pour des raisons légales et réglementaires, il est essentiel de pouvoir en vérifier leur conformité aux lois et leur capacité à répondre aux exigences réglementaires. La loi ne détaille pas la façon pratique d'archiver des documents numériques. En conséquence, les normes jouent un rôle essentiel car elles sont représentatives de l'« état de l'art ».

La référence ISO 15836 –Dublin Core

2. La norme NF Z42-013 de juillet 1999 révisée en décembre 2001

Important

Il s'agit d'une norme relative à la conception et à l'exploitation des systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes. (*voir site Wikipédia*[9])

Elle propose différentes options techniques en fonction des besoins. Pour chaque option, elle impose des conditions en termes de durabilité et de fidélité technique des systèmes.

Cette norme permet de stocker des documents sur des disques WORM (Write Once Read Many) non réinscriptibles, c'est à dire que l'on met en œuvre des supports offrant pour l'écriture une transformation irréversible. La norme préconise des formats d'encodage standards, de façon à ce que les utilisateurs puissent recourir à plusieurs sources d'outils de restitution (ex : format tiff, sgml avec ses variantes xml et html, pdf). Les procédures opérationnelles du système d'archivage doivent être établies par écrit et documentées et le système d'archivage doit assurer la traçabilité des enregistrements et être audité périodiquement. La mise en place d'une solution d'archivage implique une forte imbrication des dimensions juridique, technique et organisationnelle qui doivent être menées de concert en fonction les besoins d'archivage des documents de l'organisation en cause (entreprises privées ou publiques, administrations, ...).En conséquence, ce qui compte, c'est la certitude que l'écrit émane bien de celui auquel il pourrait être opposé et que ni son origine, ni son contenu n'ont été modifiés ou falsifiés. Si pour l'établissement de l'acte, le texte ne renvoie pas à un décret en Conseil d'Etat pour apprécier les modalités de respect de ces conditions, il convient de se reporter au nouvel article 1316-4 du code civil relatif à la signature électronique.

3. La norme ISO 14721 OAIS sur l'archivage électronique à long terme

9 - http://fr.wikipedia.org/wiki/NF_Z_42-013

Important

Cette Recommandation définit une base commune de termes et de concepts s'appliquant à un Système ouvert d'archivage d'information (OAIS - Open Archival Information System).

Elle permet une véritable comparaison et une mise en évidence des différences entre les archives aussi bien actuelles que futures. Elle fournit une base pour le développement des futurs standards dans le domaine de l'archivage.

Important

Un OAIS est une organisation autour d'un système d'archivage de données structurées, pouvant accueillir accessoirement des documents papier, des microformes, des échantillons, des objets multimédia ou informatique.

On peut s'inspirer de ce modèle d'archivage historique pour concevoir l'archivage courant et intermédiaire des données structurées à conserver dans le système d'archivage électronique d'une entreprise ou d'un organisme. Après avoir introduit l'objet du document et son domaine d'application, le modèle présente l'organisation à mettre en place entre un contributeur, un utilisateur et le management d'un OAIS, et décrit leurs rôles, leurs responsabilités et leurs interactions. Il définit ensuite l'unité d'archive élémentaire et décrit comment elle doit être pérennisée grâce à plusieurs catégories de métadonnées. Le modèle OAIS est découpé en six entités fonctionnelles principales :

- entrées,
- stockage,
- gestion des données,
- administration,
- planification de la pérennisation,
- et accès.

Le modèle d'information décrit ensuite les catégories d'informations échangées et gérées dans un OAIS.

Une autre dimension de la pérennisation est abordée, celle de la migration inéluctable et récurrente de données numériques à conserver indéfiniment.

Le programme ADELE d'administration électronique emploie la norme OAIS d'archivage électronique utilisant des métadonnées.

4. La norme ISO : NF ISO 15489-1 d'avril 2002 sur le RECORD MANAGEMENT

Elle met en exergue les notions de disponibilité, d'accessibilité, de durabilité (pérennité), d'intégrité et de confidentialité des données ainsi que l'identification, l'authentification et la traçabilité.

Important

L'ISO 15489-1 est un guide pour l'organisation et la gestion des documents d'archives des organismes, publics ou privés, pour le compte de clients internes ou externes.

Le « Records Management » comporte la mise en place de politiques et de normes, la répartition des responsabilités et des compétences, l'élaboration, la validation et la diffusion de procédures, la conception, mise en œuvre et maintenance de systèmes pour l'organisation et la gestion des documents d'archives.

5. MOREQ (MOdels REQuirements for the management of electronic records) NF ISO 15489-2

Important

Ces spécifications décrivent les exigences pour l'organisation de l'archivage électronique ou « Model Requirements for the Management of Electronic Records » (MoReq).

Il insiste principalement sur les exigences fonctionnelles pour l'archivage électronique à des fins de preuve à l'aide d'un système d'archivage électronique (SAE). Les spécifications sont rédigées pour être également applicables au secteur public et aux entreprises du secteur privé qui souhaitent mettre en place un SAE, ou qui souhaitent évaluer la capacité de leur système existant au regard de l'archivage électronique. Bien qu'il s'agisse essentiellement de spécifications fonctionnelles, il est évident que des éléments non-fonctionnels jouent un rôle central dans le succès d'un SAE, de même que pour tout système d'information. Toutefois, ces éléments non fonctionnels varient considérablement d'un environnement à l'autre. C'est pourquoi ces éléments ne sont décrits que sommairement.

Ainsi, les spécifications se prononcent sur les exigences de gestion des documents archivés, mais elles n'incluent pas toutes les fonctionnalités associées au suivi des adresses de localisation, au code-barre, etc. De même, les étapes pratiques de mise en place d'un SAE ne rentrent pas dans le champ du modèle.

K. Applications

1. Dématérialisation

Dématérialisation des courriers	Dématérialisation de la facture	Dématérialisation des offres publiques
• Analyse des circuits d'information	• Les mentions à porter sur les factures. • Les factures transmises par	• Mise en ligne des documents de consultations des

Dématérialisation des courriers	Dématérialisation de la facture	Dématérialisation des offres publiques
interne. • Les étapes du processus : ouverture des courriers, suppression des éléments polluants, numérisation des documents, gestion des index, gestion des envois et workflow, archivage et sécurisation.	voie électronique. • Les obligations relatives à la conservation et au stockage des factures. • Le contrôle de l'administration des procédés de transmission par voie électronique. • Autofacturation (émission de la facture par le client). • Sous-traitance de la facturation (tierce personne mandatée pour l'établissement des factures). • Facturation périodique.	entreprises (DCE) : règlement de la consultation, lettre de consultation, cahier des charges, renseignements complémentaires. • Téléchargement des documents. • Mise en place de l'acte de candidature et de l'offre. • Réception de la "double enveloppe". • Analyse des candidatures. • Examen des réponses.

2. Les notaires et les huissiers entrent pleinement dans le numérique

Deux décrets du 10 août 2005 précisent les conditions d'établissement, de conservation et de copie des actes authentiques sur support électronique prévus à l'article 1317 alinéa 2 du Code civil.

Les décrets n° 2005-972 et 2005-973 modifient respectivement le décret du 29 février 1956 relatif au statut des huissiers de justice et le décret du 26 novembre 1971 relatif aux actes établis par les notaires Ces décrets rendent effective la possibilité d'établir des actes authentiques sur support électronique y compris à distance (D.N. art. 20) en complément du traditionnel support papier.

Les systèmes techniques permettant l'établissement des actes authentiques électroniques sont soumis à l'agrément des instances professionnelles supérieures de chaque profession (art. 26 D.H. et art 16 D.N.), ce qui permettra de garantir l'interopérabilité des systèmes au sein des professions.

Les actes authentiques électroniques dressés par les officiers publics sont signés au moyen d'une signature électronique sécurisée (décret n° 2001-272) mais certains actes conservent les vestiges de « l'acte papier » puisque « pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite » (D.N. 17 al. 3).

Ainsi que l'avait recommandé le Forum des droits sur l'internet, la conservation des actes électroniques est assurée par un minutier central placé sous le contrôle de chaque profession concernée (D.H. art. 29-4 et D.N. art. 28). Cette conservation se fait dans des conditions garantissant l'intégrité et la lisibilité de l'acte mais aussi sa traçabilité. L'accès à l'acte est réservé à la personne qui le détient ou l'enregistre dans le minutier central (D.H. art. 29-4 al. 4 et D.N. art. 28-3 al. 3).

Des copies authentiques ou des expéditions des actes peuvent être délivrées quel que soit le support initial de l'acte ou le support final de la copie (D.H. art. 29-6 et D.N. art. 33), confirmant ainsi l'équivalence des supports.

Remarque

Cependant certaines procédures nécessitent encore une « re-matérialisation » de

l'acte (D.H. 29-6 al.3) de façon sécurisée sa comptabilité informatique en pouvant garantir au fisc que celle-ci n'a pas objet d'une publication, l'usage d'un dépôt notarié garantit le secret du contenu du dépôt.

3. La facture électronique

La facture est un élément central des transactions mais sa reconnaissance sous forme électronique reste cantonnée à la matière fiscale.

Le décret n°2003 -659 du 18 juillet 2003 est intervenu pour définir les modalités d'émission et de conservation des factures transmises par voie électronique et sécurisées au moyen d'une signature électronique. Un arrêté du 18 juillet 2003 a fixé les conditions d'émission et de conservation des factures dématérialisées.

Les factures électroniques doivent être conservées dans leur format original c'est à dire sur support informatique pendant une durée au moins égale au délai de droit de reprise tel qu'énoncé à l'alinéa 1er de l'article L. 169 du livre des procédures fiscales (LPF), sur tout support au choix de l'entreprise pendant les trois années suivantes. En cas de contrôle, si l'administration constate un défaut de conservation total ou partiel, celui -ci sera sanctionné par la remise en cause des déductions fiscales de TVA.

La facture émise et celle reçue doivent être identiques et restituables par l'entreprise à qui l'administration en fait la demande, dans un format habituellement admis dans les usages commerciaux.

Des exigences sont imposées par les textes pour la signature fiscale. La signature doit être propre au signataire, permettre d'identifier le signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, garantir le lien pour détecter toute modification. Les textes fiscaux préconisent l'utilisation d'un système de chiffrement des données reposant sur les technologies de cryptographie asymétrique. L'utilisation d'un certificat électronique délivré par un prestataire de services de certification électronique (PSCE) est exigée.

Les factures, la signature électronique à laquelle elles sont liées ainsi que le certificat électronique attaché aux données de vérification de la signature électronique doivent être conservés dans leur contenu originel pour constituer une facture d'origine. La valeur probante d'une facture est liée essentiellement à l'utilisation d'un dispositif technique assurant au système une fiabilité permettant d'assimiler la facture transmise par voie électronique à un original.

4. Les huissiers de justice s'affranchissent du papier

La nécessité de garantir l'intégrité et la pérennité des actes authentiques et de tous les documents électroniques établis ou conservés par les huissiers de justice a incité la *Chambre Nationale des Huissiers de justice*[10] à confier à la société Expérian la mise en place d'une solution de conservation électronique centralisée. Cette solution repose sur la plate-forme de dématérialisation de documents et intègre le coffre-fort électronique.

Cette plate-forme donne aux huissiers accès à des services complémentaires, le minutier central qui rassemble l'ensemble des premiers originaux de l'étude dématérialisées et archivés par la profession, un service d'archivage sécurisé de documents électroniques, un envoi de courriers électroniques certifiés, un véritable coffre-fort permettant d'archiver les documents pour lesquels les entreprises ou particuliers ont souhaité qu'un procès verbal de dépôt soit établi par huissier.

10 - http://www.huissier-justice.fr/

5. L'acte authentique devant notaire devient électronique

Rachida Dati a officiellement lancé le 28 octobre 2008 depuis le conseil du notariat la version électronique des actes authentiques mode privilégié de l'intervention du notaire. Concrètement, les parties se rendront toujours à l'étude pour signer un acte authentique mais et c'est l'évolution majeure, elles le feront désormais de manière électronique en apposant leur signature sur une tablette numérique.

En savoir plus: Dossier complet sur le lancement de la version électronique des actes authentiques

- Discours de Madame Rachida Dati (cf.), Garde des Sceaux, Ministre de la Justice - Congrès des notaires, à Lille, le 18 mai 2009.
- *Le site des notaires*[11]
- La libre circulation des actes authentiques en Europe

En pratique, pour lancer chaque procédure de signature d'un acte authentique électronique, chaque notaire détient une clé REAL, une sorte de clé USB personnelle dont l'accès est sécurisé par un code PIN qu'il doit insérer dans le port USB de son ordinateur. Elle contient l'ensemble des éléments d'identification du notaire ainsi que son signature numérique.

L. Marché

Le marché de la dématérialisation rassemble :

- les éditeurs de solutions logicielles
- les distributeurs de matériels et de solutions logicielles,
- les éditeurs de plateformes de dématérialisation,
- les prestataires de services en dématérialisation
- les tiers de confiance (autorités de certification, opérateurs techniques de certification, éditeurs de solutions de confiance, coffre-fort électronique),
- les sociétés de conseil et d'assistance à maîtrise d'ouvrage,
- les intégrateurs et sociétés de services informatiques (SSII),
- les fabricants de scanners.

L'essor du commerce en ligne est bénéfique pour les éditeurs de solutions de sécurité sur Internet.

Les principaux domaines d'application entourant la dématérialisation sont la facturation électronique, le bulletin de paie et le contrat électronique (nouvelle loi n °2009-526 du 12 mai 2009), le courrier électronique en recommandé et les lettre recommandées « hybrides », les actes des professions réglementées (huissiers et notaires), la comptabilité publique des collectivités territoriales, le contrôle de légalité, les marchés publics et les procédures administratives.

Les échanges électroniques dans la sphère publique sont encadrés par l'ordonnance n°2005-1516 du 8 décembre 2005.

Les données à caractère personnel sont protégées par les dispositions de la loi n °78-17 du 6 janvier 1978 modifiée par la loi n°2004-801 du 6 août 2004.

11 - http://www.notaires.fr

Savoir-faire

III

A. Exercice

Question

[*Solution n°1 p 107*]

Expliquer en quoi la signature peut elle être un moyen de preuve ?

B. Exercice : Cas pratique dirigé

[*Solution n°1 p 109*]

Lors d'une séance de chat sur internet, Pierre et Jean-Paul s'interrogent mutuellement sur la question de la conservation des données numériques.

Question 1

Jean-Paul explique à Pierre que pour qu'un écrit numérique ait une force probante, il faut que l'on soit capable de connaître son origine et qu'il ait été établi et conservé dans des conditions de nature à en garantir l'intégrité. (1 réponse juste)

- ○ Jean-Paul a tort.
- ○ Jean-Paul a raison.

Question 2

Jean-Paul précise par ailleurs que la mise en place d'une politique d'archivage n'est pas une obligation juridique (1 réponse juste)

- ○ Jean-Paul a encore raison.
- ○ Cette fois Jean-Paul a tort.

Question 3

Pierre demande à Jean-Paul les critères à respecter afin de s'assurer de l'intégrité des documents.

- ○ Jean-Paul doit répondre la lisibilité du document et la traçabilité des opérations effectuées sur ce dernier.
- ○ Jean-Paul doit répondre la lisibilité du document, la traçabilité des opérations effectuées sur ce dernier et la description opérations de migration.
- ○ Jean-Paul est censé répondre autre chose.

Question 4

Pierre affirme à Jean-Paul qu'il est important que la politique d'archivage définisse les utilisateurs, les données et leurs droits d'accès. La confidentialité est en effet une notion primordiale qui doit être préservée et ce, même si l'absence de mise en œuvre des « préoccupations utiles » prévue par la loi n'expose pas à des sanctions pénales. (1 réponse juste)

- ○ Pierre a raison.
- ○ Pierre a tort.

Question 5

Jean-Paul est en train de travailler sur un projet concernant un archivage public. Dans le document qu'on lui a remis, le Sigle DUA revient souvent, il demande ce que cela veut dire. Pierre lui répond « Date Unique Administrative » Est-ce juste ? (1 réponse juste)

- ○ Oui
- ○ Non

C. Quiz

Réalisez l'exercice proposé en répondant aux questions qui vous sont posées.
Bonne chance !

Enoncé 1

[*Solution n°2 p 111*]

Une fois un certificat délivré, il est toujours valide.

- ○ Vrai
- ○ Faux

Enoncé 2

[*Solution n°3 p 111*]

Dans l'archivage public, il convient de distinguer :

- ○ Les archives courantes, les archives légales, les archives en retraitement.
- ○ Les archives à durée administrative limitée, les archives définitives.

Enoncé 3

[*Solution n°4 p 112*]

Déterminez les dispositifs matériels et logiciels pour assurer la sécurité du système d'archivage :

- ○ Un logiciel antivirus, un système de détection d'intrusions, le système pare feu.
- ○ Un pilote de périphérique, le gestionnaire de tâches.

Enoncé 4

[*Solution n°5 p 112*]

L'archivage électronique présente les avantages suivants :

- ○ La sécurité, la confidentialité, la diminution du risque de perte.
- ○ La pérennité des supports, l'accès permanent aux données.

Enoncé 5

[*Solution n°6 p 112*]

L'archivage est :

○	Un acte matériel
○	Un acte juridique
○	Une opération de sauvegarde
○	Un rangement de documents papier
○	Un stockage de documents appelés à ne pas être modifiés

Enoncé 6

[*Solution n°7 p 112*]

L'écrit numérique :

○	Peut être utilisé comme élément de preuve, est dissocié de son support, peut connaître plusieurs supports physiques.
○	Doit être associé à un support papier, doit être conservé 15 ans.

Enoncé 7

[*Solution n°8 p 112*]

La caractéristique essentielle du document numérique par rapport au document papier tient :

○	Les métadonnées, le stockage, sa présentation visuelle.
○	Sa structure, la qualité du papier.

Enoncé 8

[*Solution n°9 p 113*]

La dématérialisation :

○	Est un procédé de conservation des documents.
○	Est un moyen de limiter les pertes de données.
○	Est une technique de transformation de documents numériques.
○	Est un procédé de transformation de documents papiers en document numérique.
○	Est une méthode de lecture optique de document papier.

Enoncé 9

[*Solution n°10 p 113*]

La pérennité d'un document numérique dépend :

○	Du mode de stockage, des métadonnées associées, du type de fichier de stockage.
○	Du système d'exploitation, de l'arborescence.

Exnoncé 10

[*Solution n°11 p 113*]

La signature électronique :

○	Est un moyen de preuve, est un terme générique signifiant plusieurs degrés de sécurité, est nécessaire dans tout mécanisme de sauvegarde.
○	Doit être sécurisée en se basant sur la cryptographie pour être fiable et non contestable, permet d'identifier exclusivement le signataire.

Enoncé 11

[*Solution n°12 p 113*]

Les différences entre archives publiques et archives privées se situent :

○	Dans la durée légale de conservation des documents, sur les types des documents archivés.
○	Sur le caractère de neutralité des collectivités publiques, sur l'organisation des différents suivis des archives, sur la nature des documents.

Enoncé 12

[*Solution n°13 p 113*]

Les métadonnées les plus importantes :

○	Des éléments de description (auteur, titre ...), l'identifiant de document, le type de fichier.
○	La durée d'utilité selon le document, la durée de conservation.

Enoncé 13

[*Solution n°14 p 114*]

Les modalités nécessaires et suffisantes pour assurer la sécurité du document numérique sont :

○	La lisibilité du document (quel que soit le support).
○	La stabilité du contenu informationnel (intégrité).
○	La traçabilité des opérations sur le document (historique).
○	Les bonnes pratiques du processus de conservation (versement, enregistrement, gestion et restitution).
○	Les migrations vers d'autres supports de stockage (pour éviter tout problème technique).

Enoncé 14

[*Solution n°15 p 114*]

On appelle intégrité d'un document :

○	Le moyen de le crypter.
○	La possibilité de l'identifier.
○	Le fait de ne pas le modifier.
○	La possibilité de le lire.

Enoncé 15

[*Solution n°16 p 114*]

On archive pour :

○	Justifier des droits et obligations des organisations en cas de contestation, établir une preuve, conserver la mémoire, éviter la perte de documents
○	Disposer de sources et ressources dans un but de statistiques

Enoncé 16

[*Solution n°17 p 114*]

Pour mettre en œuvre l'identification/authentification :

○	Il faut définir les accès et contrôles à assurer, il faut contrôler les accès utilisateur, il faut mettre en place une action préventive contre les logiciels d'accessibilité externe, il faut que seuls les utilisateurs autorisées aient accès aux informations concernées.
○	Il faut définir des indices de sécurité pour les informations sensibles.

Enoncé 17

[*Solution n°18 p 115*]

Quels sont dans la liste les éléments qui représentent une norme en terme de système d'archivage ?

○	DUBLIN CORE et MOREQ
○	ADELE, CIT
○	OASIS

Enoncé 18

[*Solution n°19 p 115*]

Quels sont les types de chiffrement symétriques dans cette liste ?

○	AES
○	RSA
○	DES
○	Cryptographie à clé publique
○	Triple DES

Enoncé 19

[*Solution n°20 p 115*]

Un document numérique a une valeur probatoire :

○	Si on est capable de connaître son origine et son auteur.
○	Si on lui associe un seul support de stockage.
○	Si on peut le lire, l'utiliser tout le long de sa vie.
○	Si on est capable de conserver son contenu.
○	S'il est disponible à tout instant.

Enoncé 20

[*Solution n°21 p 115*]

Une archive est :

○	Un document ancien
○	Un document papier, un document numérique, un document appelé à évoluer, un document qui peut prendre n'importe quelle forme

Solution des exercices rédactionnels

> Solution n°1 *(exercice p. 99)*

C'est un moyen de preuve. C'est un terme générique qui signifie plusieurs degrés de sécurité.

Voir *Techniques du système d'archivage : Signature* (cf. Signature p 78)

Correction des exercices auto-évalués

> Solution n°1 *(exercice p. 99)*

Question 1

- ○ Jean-Paul a tort.

  Commentaire :

  Non, Relisez l'article 1316-1 du Code Civil.

- ◉ Jean-Paul a raison.

  Commentaire :

  En effet, l'article 1316-1 du Code Civil définit les conditions à remplir pour qu'un écrit numérique ait une valeur probante. Cet article est fondamental car il pose les deux conditions juridiques de l'admission en preuve d'un écrit numérique : « 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. »

Question 2

- ◉ Jean-Paul a encore raison.

  Commentaire :

  En effet. Toutefois, détaillant les conditions de sécurité de l'archivage, ce document assurera au mieux sa fiabilité et permettra d'en rapporter la preuve devant les juges et les experts. C'est un outil de conformité légale.

- ○ Cette fois Jean-Paul a tort.

  Commentaire :

  Non, La politique d'archivage mise en œuvre permet de répondre aux exigences de conservation des documents mais encore de préservation de leur valeur probante des lors que l'électronique devient la règle. Elle est grandement conseillée mais sa mise en œuvre ne découle pas d'une disposition légale.

Question 3

○	Jean-Paul doit répondre la lisibilité du document et la traçabilité des opérations effectuées sur ce dernier. *Commentaire :* *Non, cela est insuffisant. La stabilité du contenu informationnel doit être également respectée.*
○	Jean-Paul doit répondre la lisibilité du document, la traçabilité des opérations effectuées sur ce dernier et la description opérations de migration. *Commentaire :* *Cela n'est pas la bonne réponse. La stabilité du contenu informationnel doit être également respectée. De plus, les migrations n'entrent pas comme critère pour la vérification de l'intégrité.*
◉	Jean-Paul est censé répondre autre chose. *Commentaire :* *Effectivement, la notion d'intégrité doit être assurée par le respect cumulée des TROIS critères suivants : la lisibilité du document ; la stabilité du contenu informationnel ; la traçabilité des opérations sur le document.*

Question 4

○	Pierre a raison. *Commentaire :* *Non. Veuillez relire l'énoncé.*
◉	Pierre a tort. *Commentaire :* *Effectivement. L 'article 34 de la Loi Informatique, Fichiers et Libertés modifiée par la loi du 6 août 2004 (loi n°2004-801) dispose que « le responsable du traitement est tenu de prendre toutes préoccupations utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». A défaut d'avoir pris « toutes préoccupations utiles », l'employeur s'expose aux peines prévues à l'article 226-22 du code pénal. Même si ce délit est non intentionnel, l'employeur pourrait être tenu pour responsable (même à son insu) de l'imprudence ou de la négligence de ses salariés, ayant permis la divulgation d'une donnée à caractère personnel.*

Question 5

○	Oui *<u>Commentaire :</u>* *Réfléchissez....Un indice, le A est juste le U correspond à Durée.*
◉	Non *<u>Commentaire :</u>* *Aux termes de l'article 2 du décret 79-1037 du 3 décembre 1979 modifié, précisé par la circulaire du 2 novembre 2001, il convient de distinguer :* *les **archives courantes** qui correspondent aux documents utilisés pour le traitement quotidien des affaires dont la conservation est assurée dans le service d'origine ;* *les **archives intermédiaires** qui correspondent aux documents qui, n'étant plus d'un usage courant, doivent néanmoins être conservés temporairement à proximité des services d'origine pour les besoins administratifs ou juridiques ;* *les **archives définitives** qui correspondent aux documents qui sont conservés indéfiniment, pour les besoins de la gestion et de la justification des droits des personnes pour la documentation historique de la recherche. Ces archives définitives ou historiques sont constituées après tri et élimination, à partir des archives intermédiaires.* *Les documents passent d'une des périodes précités à une autre, en fonction de leur **Durée d'Utilité administrative (DUA)**. Cette durée correspond au délai minimal durant lequel les documents doivent être conservées dans les locaux des établissements ou services producteurs, en tant qu'archive courante ou intermédiaire. Elle est déterminée en fonction des besoins du service producteur ou des délais de recours légaux. La DUA d'un document est déterminée au moyen d'un acte réglementaire ou par le biais de tableau de gestion adopté conjointement par le service producteur et l'administration des archives.*

> Solution n°2 *(exercice p. 101)*

○	Vrai
◉	Faux

> Solution n°3 *(exercice p. 101)*

○	Les archives courantes, les archives légales, les archives en retraitement.
◉	Les archives à durée administrative limitée, les archives définitives.

> Solution n°4 *(exercice p. 101)*

◉	Un logiciel antivirus, un système de détection d'intrusions, le système pare feu.
○	Un pilote de périphérique, le gestionnaire de tâches.

> Solution n°5 *(exercice p. 101)*

○	La sécurité, la confidentialité, la diminution du risque de perte.
◉	La pérennité des supports, l'accès permanent aux données.

> Solution n°6 *(exercice p. 102)*

○	Un acte matériel
◉	Un acte juridique
○	Une opération de sauvegarde
○	Un rangement de documents papier
○	Un stockage de documents appelés à ne pas être modifiés

> Solution n°7 *(exercice p. 102)*

◉	Peut être utilisé comme élément de preuve, est dissocié de son support, peut connaître plusieurs supports physiques.
○	Doit être associé à un support papier, doit être conservé 15 ans.

> Solution n°8 *(exercice p. 102)*

◉	Les métadonnées, le stockage, sa présentation visuelle.
○	Sa structure, la qualité du papier.

> Solution n°9 *(exercice p. 102)*

○	Est un procédé de conservation des documents.
◉	Est un moyen de limiter les pertes de données.
○	Est une technique de transformation de documents numériques.
○	Est un procédé de transformation de documents papiers en document numérique.
○	Est une méthode de lecture optique de document papier.

> Solution n°10 *(exercice p. 103)*

◉	Du mode de stockage, des métadonnées associées, du type de fichier de stockage.
○	Du système d'exploitation, de l'arborescence.

> Solution n°11 *(exercice p. 103)*

○	Est un moyen de preuve, est un terme générique signifiant plusieurs degrés de sécurité, est nécessaire dans tout mécanisme de sauvegarde.
◉	Doit être sécurisée en se basant sur la cryptographie pour être fiable et non contestable, permet d'identifier exclusivement le signataire.

> Solution n°12 *(exercice p. 103)*

◉	Dans la durée légale de conservation des documents, sur les types des documents archivés.
○	Sur le caractère de neutralité des collectivités publiques, sur l'organisation des différents suivis des archives, sur la nature des documents.

> Solution n°13 *(exercice p. 103)*

◉	Des éléments de description (auteur, titre ...), l'identifiant de document, le type de fichier.
○	La durée d'utilité selon le document, la durée de conservation.

> Solution n°14 *(exercice p. 104)*

◉	La lisibilité du document (quel que soit le support).
○	La stabilité du contenu informationnel (intégrité).
○	La traçabilité des opérations sur le document (historique).
○	Les bonnes pratiques du processus de conservation (versement, enregistrement, gestion et restitution).
○	Les migrations vers d'autres supports de stockage (pour éviter tout problème technique).

> Solution n°15 *(exercice p. 104)*

○	Le moyen de le crypter.
○	La possibilité de l'identifier.
◉	Le fait de ne pas le modifier.
○	La possibilité de le lire.

> Solution n°16 *(exercice p. 104)*

◉	Justifier des droits et obligations des organisations en cas de contestation, établir une preuve, conserver la mémoire, éviter la perte de documents
○	Disposer de sources et ressources dans un but de statistiques

> Solution n°17 *(exercice p. 104)*

◉	Il faut définir les accès et contrôles à assurer, il faut contrôler les accès utilisateur, il faut mettre en place une action préventive contre les logiciels d'accessibilité externe, il faut que seuls les utilisateurs autorisées aient accès aux informations concernées.
○	Il faut définir des indices de sécurité pour les informations sensibles.

> Solution n°18 *(exercice p. 105)*

◉	DUBLIN CORE et MOREQ
○	ADELE, CIT
○	OASIS

> Solution n°19 *(exercice p. 105)*

○	AES
○	RSA
○	DES
◉	Cryptographie à clé publique
○	Triple DES

> Solution n°20 *(exercice p. 105)*

◉	Si on est capable de connaître son origine et son auteur.
○	Si on lui associe un seul support de stockage.
○	Si on peut le lire, l'utiliser tout le long de sa vie.
○	Si on est capable de conserver son contenu.
○	S'il est disponible à tout instant.

> Solution n°21 *(exercice p. 106)*

○	Un document ancien
◉	Un document papier, un document numérique, un document appelé à évoluer, un document qui peut prendre n'importe quelle forme