1

Définitions et enjeux

Objectifs

L'évolution des technologies, les besoins de productivité ou encore l'augmentation des exigences réglementaires en matière de gestion de l'information, amènent de plus en plus d'organismes à décider de rationaliser leur production documentaire, de réorganiser leurs processus métier et à opter pour la diminution de l'utilisation du support papier. C'est notamment pour ces raisons que fleurissent bon nombre de projets de dématérialisation et/ou d'archivage électronique.

Mais avant même de se poser la question de lancer ou de programmer un projet de dématérialisation et/ou d'archivage électronique, il est impératif de se demander quelles notions recouvrent ces termes et à quels besoins un tel projet peut répondre.

1.1 DÉMATÉRIALISATION ET ARCHIVAGE ÉLECTRONIQUE

1.1.1 Qu'entend-on par dématérialisation ?

La dématérialisation correspond à deux sources de production documentaire donc à deux processus distincts :

- les documents sont créés à partir d'un document matériel (papier, microforme...) en utilisant un procédé de numérisation. Il s'agit d'une numérisation simple, le document scanné est une copie ;
- les documents sont créés directement sous forme électronique par l'emploi, par exemple, d'un outil de traitement de texte. Le document produit dans ce cas est

le document d'origine, et pourra être considéré comme un original sous réserve de respect de dispositions légales et techniques. L'arrêt de la Cour de cassation du 4 décembre 2008 (pourvoi n° 07-17622) précise un certain nombre de points permettant de donner force probante aux documents électroniques (voir les commentaires de Maître Isabelle Renard)[1].

À ces deux notions s'ajoute également celle de dématérialisation des échanges dont l'e-mail en est la parfaite illustration.

Exemple de la dématérialisation des factures

Afin d'illustrer ces différents aspects, prenons l'exemple de la dématérialisation des factures. De façon quasi naturelle la dématérialisation des factures fait d'abord penser au traitement des factures entrantes au format papier que l'on numérise afin de les intégrer au *workflow* comptable de l'entreprise, tout en les conservant au format papier pour être conforme en matière d'archivage aux exigences du code général des impôts et aux instructions fiscales. En fait il s'agit d'un processus traditionnel de GED (gestion électronique de documents, voir ci-après). Par ailleurs, remarquons que dans la majorité des cas la facture originale existe aujourd'hui sous forme numérique et qu'elle est imprimée uniquement pour son envoi. L'efficacité d'une telle dématérialisation est donc très limitée si l'on se réfère à l'ensemble du processus de facturation.

Ainsi une autre manière de traiter la dématérialisation des factures consiste à prendre en compte le processus de bout en bout. La facture une fois créée au format électronique est transmise en l'état et reprise telle quelle par le destinataire avec une intégration sans rupture à son système d'information. L'archivage a lieu uniquement au format électronique.

Cet exemple montre combien il est important de considérer un processus dans son intégralité en vue de sa dématérialisation afin d'obtenir un maximum d'efficacité. Il est même fortement conseillé de passer un peu de temps pour analyser s'il n'y aurait pas lieu de modifier le processus d'origine afin de profiter au mieux de sa transformation en électronique.

Pour cela il est même possible de s'appuyer sur des outils existants de longue date comme « l'analyse de la valeur », introduite en Europe en 1960, qui constitue une méthode rationnelle destinée à optimiser un produit, un procédé ou un processus au regard de la fonction que l'on en attend.

1.1.2 L'approche GED

Aux documents natifs électroniques sont liées deux problématiques : leur conservation dans le temps (obsolescence technologique et durée de vie des supports) et la possibilité de les consulter chaque fois que nécessaire (disponibilité et gestion des droits d'accès). Conserver sur son disque dur un contrat original signé électroniquement

1. Voir annexe B : premier arrêt de la Cour de cassation sur la preuve électronique

implique une limite importante à sa consultation. En effet le contrat original, inaccessible en dehors de son détenteur, ne garantit pas sa sécurité (le disque dur peut être endommagé), sauf à prévoir des sauvegardes régulières sur un autre support et n'offre aucune garantie dans le temps quant à la vérification de la signature électronique. De plus l'espace de stockage offert par ce type de support ne permet pas de gérer une volumétrie importante.

C'est pourquoi, de plus en plus d'organismes utilisent un logiciel de gestion électronique de documents (GED) afin de rendre ces documents disponibles aux collaborateurs concernés. On trouve le terme de GEIDE pour gestion électronique d'informations et de documents existants. Lancée dans les années 1980, la GED constitue un dispositif purement technique, destiné effectivement à favoriser l'accès aux documents à l'intérieur de l'organisme.

La GED peut être définie comme « un ensemble d'outils et de techniques permettant de dématérialiser, gérer, classer, indexer, rechercher, consulter, stocker et transmettre de façon dynamique l'information produite ou reçue par un organisme dans le cadre de ses activités ». En revanche, un outil de GED ne peut pas être assimilé à un système d'archivage électronique.

1.1.3 Qu'entend-on par archivage électronique ?

L'archivage peut être défini comme « l'ensemble des règles, méthodes, processus et solutions permettant, de manière raisonnée et sécurisée, la conservation, la consultation, la restitution, la gestion dans le temps et, à l'échéance de la durée de conservation, la destruction des documents ».

L'archivage électronique, quant à lui, nécessite en plus la mise en œuvre de processus automatisés de capture des documents et de données, la gestion de métadonnées et la conservation des informations sur un support adapté, évolutif et pérenne.

Un système d'archivage électronique (SAE) peut être défini comme un système permettant (voir chapitre 4 pour plus de détails) :

- la capture sécurisée de documents et données à valeur de preuve ou de documentation pour l'organisme ;
- leur rattachement à un plan de classement structuré et hiérarchisé ;
- la gestion de la confidentialité et des droits d'accès ;
- le maintien de l'intégrité des documents ;
- la conservation du contexte de capture, de création des documents et des données ainsi que de toutes modifications intervenues ;
- la conservation des documents dans le respect des durées prescrites.

1.1.4 Retour à la GED

La GED gère des documents qui peuvent évoluer ou être modifiés par opposition à un SAE qui ne gère que des documents figés, fixés et non modifiables et auxquels sont attachées des durées de conservation.

L'essor de la GED s'explique principalement par le fait que rechercher un document est dix fois plus coûteux que de le produire. Pour autant, s'équiper d'un outil de GED ne répond pas à toutes les questions en matière de gestion de l'information et n'est pas toujours la réponse adéquate. Penser la dématérialisation simplement en termes de réceptacle de stockage de l'information ne résout aucun problème et peut même, dans certains cas, devenir source de coûts et d'erreurs.

De la même manière, penser que la GED est la réponse au besoin de conservation au titre de l'archivage est une erreur que bon nombre d'organismes font encore aujourd'hui (de même que croire que sauvegarde et archivage sont la même chose).

Un outil de GED n'a pas, *a priori*, vocation à gérer les documents dans le temps donc à assurer et garantir leur conservation sur le moyen et long terme par l'application de règles de gestion (durées de conservation et destruction). Ces besoins sont du domaine de l'archivage et pour les documents électroniques relèvent de l'archivage électronique.

Mais il est fréquent que les documents qui ont vocation à être archivés soient conservés dans un outil de GED pendant une partie de leur cycle de vie. D'où la nécessité de prendre les bonnes dispositions afin d'éviter le danger, en cas de litige, de ne pas pouvoir disposer des éléments probants suffisants comme la garantie d'intégrité du document pendant sa conservation au sein du système de GED (qui autorise les modifications) avant d'être versé dans un système d'archivage. Sur ce point la loi est très claire et impose une garantie d'intégrité dès l'instant que le document est figé.

Cependant dans la pratique un document peut être figé et non modifiable dès sa création ou sa finalisation mais être un document constitutif d'un dossier amené à évoluer dans le temps et être alimenté au fur et à mesure.

Exemple

Le dossier client de l'opérateur Orange est constitué de plusieurs documents qui vont être créés tout au long de la relation client, à savoir :

- Le contrat d'abonnement à un mobile :
  - figé et non modifiable dès sa signature ;
  - archivé pour 10 ans à compter de sa résiliation.
- De nouveaux documents qui alimentent le dossier client pendant toute la durée d'exécution du contrat, par exemple :
  - les courriers ;
  - les avenants ;
  - les pièces justificatives.

Lorsque les dossiers étaient exclusivement constitués de documents papiers, une chemise était ouverte et les documents rangés au gré de leur création ou de leur réception.

La dématérialisation du dossier client et l'utilisation d'un outil de GED ont permis de traiter l'information à l'identique, tout en assurant pendant toute la période d'exécution du contrat puis lors de sa conservation au titre de l'archivage :

- la mise à disposition des documents tout en sécurisant les originaux ;
- la disponibilité de l'intégralité des documents ;
- la gestion de l'obsolescence des supports et des formats ;
- la traçabilité de tous les événements sur les documents et le système ;
- l'impossibilité de supprimer, de modifier ou de remplacer un document figé et non modifiable (voir chapitre 10 pour plus de détails sur la mise en œuvre de la solution).

Néanmoins cette logique de gestion nécessite que les outils soient en capacité de garantir la sécurité de la conservation et l'intégrité des documents durant une période plus ou moins longue. Rappelons qu'au regard de la loi du 13 mars 2000[1], quatre exigences sont clairement exprimées en matière de valeur probante d'un document électronique, à savoir son intégrité, son identification, son intelligibilité et sa pérennité.

C'est pourquoi il est nécessaire de coupler à l'outil de GED un SAE afin de garantir ces exigences et en particulier :

- la conservation de l'intégralité du dossier après transfert de la GED vers le SAE pendant toute la durée requise ;
- sa destruction à l'échéance de la durée de la conservation (ou dans quelques cas une conservation définitive).

Cet exemple démontre que la dématérialisation doit être envisagée comme un projet global de la gestion de l'information afin d'aborder la problématique de la conservation des documents tout au long de leur cycle de vie en prenant en compte leur utilité, leurs phases de vie et la sécurité nécessaire.

Plutôt que de choisir entre GED et SAE, la question à se poser concerne la fonctionnalité recherchée. Ainsi la GED est plus particulièrement destinée à faciliter l'accès aux documents pour un nombre relativement important d'individus et avec des temps de réponse relativement rapides. Un SAE quant à lui, doit avant tout répondre à des préoccupations de sécurité dans la mesure où il relève dans la majorité des cas d'une problématique de valeur probante.

De fait un SAE n'est, *a priori*, pas particulièrement adapté à répondre rapidement à beaucoup d'utilisateurs et à remplacer un système de GED. En effet d'un point de vue purement logique sécuritaire, plus il y a d'utilisateurs plus la confidentialité est difficile à assurer. Par ailleurs la sécurité impose également un certain nombre de traitements comme celui de vérification d'intégrité du document, voire de chiffrement. Chacun

1. Loi n° 2000-230 du 13 mars 2000 « *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* ».

de ces traitements prend du temps, ce qui peut venir en opposition à l'objectif initial de temps de réponse rapide.

Si l'on pousse au bout le raisonnement il n'est donc absolument pas aberrant d'envisager la conservation en double d'un même document, à la fois dans un système de GED et dans un SAE. La GED répond ainsi à une problématique opérationnelle au quotidien et le SAE aux contraintes sécuritaires indispensables lorsqu'il s'agit de valeur probante.

Cependant il est clair que ce qui précède va d'une certaine façon à l'encontre des politiques de réduction des coûts de stockage. Ainsi est-il également possible d'envisager une solution autour d'un document « virtuel » qui apparaîtrait dans la GED alors qu'il est réellement archivé. Il s'agit de la solution adoptée dans les espaces SharePoint quand un document concerne plusieurs dossiers : on ne le stocke qu'une fois et on fait un document virtuel dans les autres dossiers.

1.2 QUELS SONT LES ENJEUX ET OBJECTIFS DE LA DÉMATÉRIALISATION ET DE L'ARCHIVAGE ÉLECTRONIQUE ?

Décider de dématérialiser tout ou partie un processus métier nécessite d'en connaître les avantages que pourra en tirer l'organisme, les gains qu'il pourra réaliser et d'avoir la certitude que ce changement répondra aux besoins.

1.2.1 Les enjeux

Les enjeux et intérêts sont de plusieurs ordres et n'ont pas la même valeur selon les organismes, leur taille ou leur implantation géographique.

La dématérialisation est évidemment une solution technique qui peut couvrir les besoins suivants :

- permettre la consultation d'un même dossier par plusieurs personnes en même temps ;
- résoudre les problèmes de consultation multi-site, c'est-à-dire éviter les copies papiers ou l'envoi de pièces jointes dans les e-mails ;
- désengorger les messageries et les serveurs :
  - problème de la volumétrie liée à l'enregistrement par tous les destinataires des pièces jointes (certains outils de GED permettent d'envoyer un lien sur le document plutôt que le document lui-même) ;
  - sauvegarde effectuée plusieurs fois par les systèmes.
- accéder *via* une interface unique qui fédère différents applicatifs et bases de données. Cette source unique constitue alors la garantie que l'information disponible est fiable : le document a été validé et l'utilisateur a lui même la

garantie d'accéder à la bonne version du document (contrairement aux dossiers papiers pour lesquels on ne sait pas toujours où ils sont classés, qui les détient, ou qui se trouvent sur un site éloigné, une base de données est plus facilement accessible) ;

- travailler au quotidien à partir du document ou dossier électronique peut parfois suffire, même si le document original est sur support papier ;
- externaliser la conservation du papier (gain en espace de stockage dans les bureaux) et sécuriser les originaux papiers *via* une conservation physique dans des locaux adaptés ;
- permettre la consultation des informations aussi souvent que nécessaire tout en garantissant l'intégrité et la sécurité des originaux : moins de manipulations de l'original, donc moins de risques de perte ou de détérioration ;
- gagner du temps lors des recherches, on sait où se trouve le document. On évite d'aller dans les locaux de stockage qui ne sont pas forcément toujours près des bureaux (sous-sol, cave...) ;
- par la gestion de droits d'accès et d'habilitations, il est possible d'accéder au dossier dans la mesure où celui-ci est partagé, même si celui qui le gère est absent ;
- permettre la validation des documents plus rapides et plus fiables ;
- mieux gérer le *versionning* car le plus souvent les outils gèrent de façon automatique les versions (dans le cas de l'archivage électronique, il n'y a pas de version du document d'archive car chaque document est unique) ;
- gagner en achat de consommables : moins de papiers car moins de photocopies et moins d'encre et d'électricité pour les photocopieurs ou les imprimantes.

Au sens de l'archivage électronique, nous reprenons ici quelques-uns des enjeux cités dans un livre blanc publié par FedISA[1]. Il s'agit tout d'abord d'un enjeu stratégique afin de choisir quelles données conserver en dehors des aspects purement obligatoires, légaux et réglementaires. En effet, selon son domaine d'activité un organisme peut avoir un véritable intérêt à conserver ses différents procédés, savoir-faire ou autres afin de pouvoir les réutiliser ultérieurement ou tout simplement afin d'en garder une trace historique au sens du patrimoine intellectuel de l'entreprise. Afin d'illustrer ce propos signalons l'exemple d'une écurie de F1 qui archive l'ensemble de ses e-mails afin de ne pas courir le risque de perdre une information qui pourrait se révéler précieuse ultérieurement.

Au cours de la mise en place d'un SAE d'autres enjeux interviennent dont le premier est d'ordre purement organisationnel selon trois aspects. D'une part il faudra autant que faire se peut optimiser la structuration des données afin d'en faciliter la gestion et maîtriser la redondance de l'information. D'autre part, il faudra détruire les données inutiles ou périmées qui alourdissent le système. Enfin, il faudra faciliter l'accès à l'information tout en respectant des droits d'accès établis de façon stricte.

1. *L'archivage électronique à l'usage du dirigeant*, MA Chabin, E Caprioli, JM Rietsch.

L'enjeu est donc également la sécurité et oblige au respect d'une véritable cohérence entre les différentes démarches associées au sein de l'organisme. En effet pourquoi fermer la porte de son usine si l'on ne bloque pas les accès à l'information, certes immatérielle, avec la même logique ?

Arrive ensuite un enjeu plus technique destiné à répondre au paradoxe de l'archivage électronique qui consiste à conserver des documents pendant des durées assez longues alors que les solutions proposées sont très rapidement obsolètes. Comment dès lors protéger l'organisme contre cette obsolescence des technologies tout en lui offrant une garantie de disponibilité des données sur le moyen, long terme et en lui permettant une évolution naturelle des volumes de données à archiver.

Du point de vue juridique, l'enjeu consiste à pouvoir retrouver certains documents en cas de litige et faire en sorte qu'ils puissent effectivement être retenus comme éléments de preuve.

Enfin l'enjeu est éminemment financier et ceci à double titre : le premier au regard des investissements directement liés à la mise en place du système d'archivage et à son exploitation, le second face au risque encouru si l'organisme se trouve dans l'impossibilité de retrouver et donc de fournir l'information requise ou encore qu'elle ne puisse être retenue comme élément de preuve.

1.2.2 Comment gagner le défi de la mise en œuvre de la dématérialisation et de l'archivage électronique ?

Le défi de la dématérialisation et de l'archivage électronique repose sur la conception en amont du projet. Ce dernier se doit de prendre en compte les exigences et les besoins métier de l'organisme tout en gagnant le défi de la maîtrise des coûts et de la conservation exhaustive, raisonnée et efficace de l'information.

À l'heure actuelle, l'électronique est omniprésente dans la vie et l'organisation interne de tous les organismes quels qu'ils soient. Qu'il s'agisse d'un courrier client, d'un dépôt d'une demande de congé ou encore d'une facture. Le papier est souvent le support d'impression mais de plus en plus rarement l'original.

Pour autant, l'utilisation de l'électronique n'est pas toujours synonyme de dématérialisation. En effet, un courrier peut être créé *via* l'utilisation d'un outil bureautique puis être imprimé pour signature. L'original du document est dans ce cas le papier et non le document électronique. L'outil bureautique peut alors être comparé au stylo ou à la machine à écrire. Il ne s'agit que d'un instrument.

La dématérialisation doit être envisagée dans un processus global de création, de conservation et de restitution de l'information. Trois exemples viennent étayer nos propos.

Premier exemple, principe d'un courrier « recommandé » électronique

Un courrier est créé au moyen d'un traitement de texte, sa validation réalisée par un *workflow*, il est ensuite signé grâce à une signature électronique, puis envoyé par messagerie électronique avec accusé de réception électronique.

La trace de ce courrier pourra être assurée par l'enregistrement dans une base de données GED, du courrier, de l'e-mail d'accompagnement et de l'accusé de dépôt et de réception du destinataire.

Tous ces documents pourront être classés dans un dossier qui sera crypté et/ou scellé et un horodatage de toutes ces opérations fournira une garantie supplémentaire. Il s'agit là d'une dématérialisation globale de processus.

Deuxième exemple, e-mail sécurisé et bureau de poste restante électronique

Une autre façon de répondre à cette notion de courrier « recommandé » électronique ou encore d'e-mail sécurisé consiste à utiliser la logique de la poste restante. Plutôt que d'envoyer un e-mail directement au destinataire, on le transmet à l'équivalent d'un bureau de poste restante électronique qui avertit le destinataire qu'un « recommandé » lui a été envoyé. Il n'a alors qu'à cliquer sur un lien pour accéder à ce « recommandé », après s'être identifié. Outre la traçabilité de chaque opération – dépose du courrier, avertissement du destinataire, recherche du courrier –, l'ensemble des courriers ainsi envoyé peut ensuite être conservé.

Un tel dispositif peut soit être abrité en interne soit être totalement externe et fonctionner alors avec une logique de tiers de confiance pour renforcer la notion de preuve.

Au-delà de l'aspect purement fonctionnel, cet exemple montre bien que la dématérialisation peut transformer un processus qui dans le monde classique est terriblement lourd à gérer, en quelque chose de très efficace.

Troisième exemple, dématérialisation partielle du courrier sortant

Une assistante qui disposait de peu de place pour la conservation des documents papier du service avait décidé de numériser les documents avant de les ranger dans un local situé en sous-sol. Ce choix voulait répondre à ce manque de place et néanmoins un besoin de consultation quotidien.

Le courrier était créé au moyen d'un traitement de texte puis imprimé pour signature. Il était ensuite conservé soit en raison de sa valeur juridique en tant que telle soit comme un élément de preuve. Deux solutions étaient possibles :

1. Faire une photocopie de l'original papier signé.
2. Numériser l'original signé avant envoi.

La première solution basée sur la photocopie de tous les courriers posait, à relativement court terme, trois problèmes : la volumétrie bien évidemment, le classement des papiers et la consultation.

La deuxième solution de numériser le document avant envoi permettait de répondre au problème de la volumétrie et du classement papier.

En revanche, les limites étaient :

- en cas d'absence de l'assistante, personne ne pouvait accéder aux documents conservés sur son disque dur ;

- aucune traçabilité des mouvements sur les documents n'était faite ;
- aucune garantie de non-destruction, de non-modification n'était assurée ;
- aucune gestion dans le temps des documents (durées de conservation) n'était activée ;
- la recherche était possible à partir du plan de classement mais il n'y avait pas de métadonnées.

Dans ces trois exemples, la dématérialisation suppose un réceptacle de stockage adapté à la conservation et au suivi (traçabilité) tout en permettant la consultation. D'où le lien étroit entre dématérialisation et archivage électronique, avec ou sans valeur probante. Ils montrent qu'avant de décider de dématérialiser toute activité, il convient d'identifier ce que l'on a réellement besoin de faire, quelles sont les fonctionnalités attendues, pourquoi et dans quel contexte.

1.3 TERMINOLOGIE

Afin de faciliter au maximum la compréhension de la suite de l'ouvrage, nous donnons ci-après des définitions qui nous paraissent essentielles et auxquelles le lecteur pourra se référer avantageusement.

1.3.1 Numérique/électronique

Ces deux termes sont très proches mais néanmoins différents. Ainsi l'*électronique* correspond à une partie de la physique et de la technique tandis que l'adjectif associé caractérise ce qui fonctionne suivant le principe de l'électronique, ce qui utilise les dispositifs électroniques. Quant au *numérique* il se dit de la représentation d'informations ou de grandeurs physiques au moyen de caractères tels que des chiffres, ou au moyen de signaux à valeurs discrètes, en l'occurrence 0 et 1 pour l'informatique. Numérique se dit aussi de systèmes, dispositifs ou procédés dont le fonctionnement fait appel à un tel mode de représentation, par opposition à analogique[1].

Retenons simplement qu'électronique est plutôt orienté matériel tandis que numérique correspond plus à une façon de représenter l'information. Quoi qu'il en soit nous utiliserons quasi indifféremment ces deux termes dans cet ouvrage mais tenions à apporter ces précisions.

Ainsi lorsque l'on évoque l'archivage électronique il serait plus précis de dire : archivage de données numériques sur support électronique.

1.3.2 Données, document, fichier, information, dossier

Pour simplifier, nous retiendrons que les « données » représentent l'élément de base de l'« information » qui elle-même constitue un renseignement. Les données peuvent être structurées (données relationnelles, données objet), semi-structurées (HTML, XML, graphes) ou non structurées (texte, images, son).

1. Petit Larousse 2009

Un « document » est également constitué d'un ensemble de données et à ce titre peut être vu comme un support possible de l'information, mais également comme un élément d'information, sachant qu'avec d'autres, il concourt à la formation d'un tout.

Le terme « fichier » a davantage une connotation technique, et peut être vu comme un ensemble de caractères informatiques (un ensemble de bits et d'octets), comparable à « dossier » pris comme un ensemble de documents ou encore à « document », plus proche du contenu au sens informationnel du terme. Il est d'ailleurs très difficile de définir précisément ce qu'est un document. En effet dans un univers papier on l'assimile à la fois au support et au texte inscrit (ou de façon plus large à l'information) tandis que dans un univers dématérialisé il est déjà beaucoup plus compliqué de définir la notion même de support. En effet s'agit-il du disque magnétique sur lequel sont inscrits les octets, de l'écran sur lequel s'affiche le contenu ? Retenons simplement que ce qui nous intéresse ici relève du contenu informationnel du document, des données qu'il contient de toute nature : texte, son, images, vidéo...[1]

1.3.3 Intégrité, complétude

Ce terme revêt une importance toute particulière dans la mesure où la garantie d'intégrité constitue une des conditions de recevabilité d'un document en tant qu'élément de preuve. Or sa signification ou encore sa perception peut être différente suivant que l'on se place d'un point de vue technique ou juridique. Globalement la garantie d'intégrité consiste à préserver l'objet dans son état d'origine, sans altération aucune, il s'agit d'une forme de stabilité du document mais également d'un ensemble, d'une liste d'objets et on parlera alors plutôt de « complétude » pour bien marquer la différence.

Aspect technique

Afin de garantir l'intégrité d'un fichier du point de vue technique, on a régulièrement recours à des algorithmes de calcul d'empreinte qui permettent de détecter la moindre modification même d'un seul bit (*binary digit*). Ces algorithmes génèrent, pour chaque document, un nombre fixe de bits que les Anglo-Saxons appellent « *digest* » ou « *hash* » et les Français « résumé » ou « condensât ». On parle parfois à tort de signature de document, ce qui peut être à l'origine de contresens fâcheux dans la mesure où la signature électronique permet d'abord d'identifier son auteur et en complément de vérifier l'intégrité du document grâce au calcul d'empreinte.

1. Roger T. Pédauque, travail collectif de réflexion en cours au sein du réseau thématique pluridisciplinaire 33 du département STIC (Sciences et technologies de l'information et de la communication) du CNRS Version 3, 8 -07-2003.

Au sujet des empreintes et des algorithmes correspondants

L'empreinte d'un document électronique peut être comparée à l'empreinte digitale ou génétique d'un individu. C'est en quelque sorte l'ADN du document. Ses propriétés sont les suivantes :

– si l'on change un seul bit du document, par exemple une simple virgule, son empreinte change ;

– la probabilité que deux documents aient la même empreinte est quasiment nulle ;

– il n'est pas possible de reconstituer le document à partir de sa seule empreinte.

La collision : un hasard improbable

Sous l'angle purement statistique, un algorithme générant une empreinte de n bits permet d'identifier 2^n empreintes différentes. Ainsi d'un point de vue purement théorique, avec une longueur de 2 bits il sera possible d'avoir 2^2 soit 4 empreintes différentes (00-01-10-11). Or le nombre de fichiers dont on peut vouloir contrôler l'intégrité est *a priori* infini. Une même empreinte peut ainsi correspondre à plusieurs fichiers. L'empreinte ne serait donc pas unique, il s'agit de collisions.

Le théorème, ou paradoxe, des anniversaires montre qu'il faut $2^{n/2}$ essais pour trouver une collision avec une probabilité de plus de 50 pour cent. Le nombre n/2 représente le nombre de bits de sécurité tandis que $2^{n/2}$ représente la force d'une fonction de hachage ou de calcul d'empreinte. La collision est supposée être le fait du hasard, et non le fruit d'une action malveillante qui pourrait abaisser le niveau de la probabilité.

À l'origine de ce théorème, Richard Von Mises, énonce qu'il suffit d'un groupe de 23 individus pour avoir une chance sur deux que deux personnes de ce groupe aient leur anniversaire le même jour, contrairement à ce que l'intuition laisse présumer. À partir de 50 personnes, il n'y a que 3 % de chances que tous les anniversaires diffèrent !

Un « hasch » de 128 bits ne représente plus une sécurité suffisante...

Dès le début des années 2000, il était clairement admis que les clés de 56 bits de l'algorithme de chiffrement DES (*Data Encryption Standard*) étaient faibles et aisément crackables. En prenant n/2 = 56, c'est-à-dire n = 112, le théorème des anniversaires nous indique que les empreintes de 112 bits sont faibles. Par extension, les empreintes de 128 bits (n/2 = 64) ne présentent pas une sécurité suffisante.

En 2005 nous écrivions qu'il était alors acquis que le minimum pour une empreinte était de 160 bits (n/2 = 80). Il fallait alors en effet 280 calculs (plus de 10^{24}, c'est-à-dire plus d'un million de milliards de milliards de calculs) pour obtenir une collision avec une probabilité supérieure à 50 pour cent. Les durées de tels calculs nous laissent tranquilles pour quelque temps... quoique.

Que penser pour l'avenir ?

La loi de Moore stipule que la puissance des ordinateurs gagne un facteur 8 tous les 3 ans. Comme évoqué précédemment, les ordinateurs des années 2000 étaient capables de calculer 256 valeurs en quelques jours. En appliquant le facteur 8 il est dès lors possible de faire la même chose avec 264 dans 3 ans, 272 dans 6 ans et 280 dans 9 ans, soit en 2010. Nous avons ainsi atteint la limite pour affaiblir suffisamment les empreintes de 160 bits avec n/2 = 80 bits et conseiller de ne plus les utiliser. La poursuite du même raisonnement conduit à attendre 27 ans, aux environs de 2030 pour 128 bits et des empreintes de 256 bits.

Deux algorithmes valent mieux qu'un

Attention toutefois au fait que cette analyse ne repose que sur une statistique. Une personne malveillante pourrait agir autrement pour obtenir un nouveau fichier ayant la

même empreinte que l'original et mettre en œuvre des procédés plus efficaces qu'une simple recherche purement probabiliste. Pour s'en prémunir, il est donc fortement recommandé d'utiliser une empreinte d'au moins 256 bits soit 32 octets. Pour accroître la sécurité, il est également possible d'utiliser deux algorithmes différents de hachage en parallèle. Un hackeur aura alors beaucoup plus de mal à trouver un texte intelligible produisant les mêmes empreintes que le texte d'origine avec les deux algorithmes à la fois.

À ce jour, aucune tentative n'a abouti à régénérer facilement un document pour que celui-ci ait une empreinte préétablie. Les travaux de Joux, Carribault et Lemuet ont mobilisé le supercalculateur du Tera Nova CEA et ses 256 Itanium2 pendant 80 000 heures-processeur (plus de 9 ans) pour parvenir le 12 août 2004 à une collision avec l'algorithme SHA-0 (160 bits). La démarche des chercheurs consistait à trouver deux fichiers ayant la même empreinte et non à faire passer pour authentique un fichier pirate.

Principaux algorithmes de calcul d'empreintes

MD4 (*Message Digest 4*)

L'algorithme de hachage MD4 a été conçu par le professeur Ronald Rivest du MIT. La taille de la signature est de 128 bits. L'algorithme a été abandonné au profit du MD5 après la découverte de faiblesses dans sa conception (Den Boer et Bosselaers). D'autres attaques plus efficaces ont suivi, notamment par Hans Dobbertin du service du chiffre allemand et l'équipe chinoise à l'origine de l'attaque sur MD5 (Wang et al.).

MD5 (*Message Digest 5*)

Développé par Rivest en 1991, MD5 produit une empreinte de 128 bits à partir d'un texte de taille arbitraire. MD5 manipule le texte d'entrée par blocs de 512 bits.

SHA (*Secure Hash Algorithm*)

SHA est la fonction de hachage utilisée par SHS (*Secure Hash Standard*), la norme du gouvernement américain pour le hachage, élaborée par la NIST (National Institue of Standards and Technology) et la NSA (National Security Agency). SHA-1 est une amélioration de SHA publiée en 1994.

RIPE-MD

Développée dans le cadre du projet RIPE *(RACE Integrity Primitives Evaluation*) de la Communauté européenne, RIPE-MD fournit une empreinte de 128 bits. RIPE-MD-160 est une version renforcée de RIPE-MD qui fournit une empreinte de 160 bits.

Une collision complète a été trouvée en août 2004, en même temps que la collision sur le MD5. Une autre attaque sur une version simplifiée avait été publiée en 1997 par Hans Dobbertin.

WHIRLPOOL

Whirlpool est une fonction de hachage http://fr.wikipedia.org/wiki/Cryptographie conçue par Vincent Rijmen et Paulo Barreto pour le projet de la communauté européenne NESSIE (*New European Schemes for Signatures, Integrity and Encryption*). La fonction utilise une architecture de type Miyaguchi-Preneel connue pour sa résistance à la cryptanalyse et produit des empreintes de 512 bits.

En interne, l'algorithme travaille sur 512 bits grâce à une fonction similaire à celle de l'algorithme de chiffrement symétrique AES *(Advanced Encryption Standard*) auquel Vincent Rijmen a également participé.

Aspect juridique

Il est tout à fait possible de modifier un format de document sans porter atteinte à son intégrité juridique, alors que son intégrité technique sera perdue. L'intégrité technique représente un des éléments permettant de satisfaire l'intégrité juridique pour laquelle l'information prime sur la manière avec laquelle elle est formatée et conservée. Du point de vue juridique, l'intégrité concerne en réalité l'information, le contenu informationnel quel que soit le format du support tant logique que physique. Il est ainsi tout à fait possible de modifier l'intégrité technique des fichiers (suite à un processus de migration de format par exemple) sans altérer l'intégrité du contenu informationnel.

Dans pareil cas il est toutefois nécessaire de tracer (voir plus bas) et de documenter tout processus de migration de format, de support ou d'outil afin de garantir que ce processus de migration a bien respecté un certain nombre de contraintes. Il s'agit aussi de pouvoir alimenter les métadonnées liées à cette migration (nouveau format, nouveau support, explication sur les raisons de la migration, par qui a-t-elle été réalisée, pour quelles raisons…).

Ainsi, dans ses recommandations sur la « conservation électronique des documents », le Forum de Droits sur Internet[1] propose en définitive, pour garantir l'intégrité d'un écrit, que trois critères soient cumulativement réunis par le processus de conservation, à savoir :

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

La lisibilité désigne la possibilité d'avoir accès, au moment de la restitution du document, à l'ensemble des informations qu'il comporte. Cette démarche peut être grandement facilitée grâce aux métadonnées associées au document. Attention au fait que ce terme possède en réalité une double signification. La première consiste à être capable de relire, tandis que la deuxième revient à pouvoir interpréter ce que l'on vient de relire. En ce sens, cette seconde signification est plus proche de la notion d'intelligibilité.

La stabilité du contenu informationnel désigne la nécessité de pouvoir garantir que les informations véhiculées par le document restent les mêmes depuis l'origine et qu'aucune n'est omise ou rajoutée au cours du processus de conservation. Le contenu informationnel s'entend de l'ensemble des informations, quelle que soit leur nature ou leur origine, issues du document et, le cas échéant, de sa mise en forme.

La traçabilité désigne la faculté de présenter et de vérifier l'ensemble des traitements, opérés sur le document lors du processus de conservation.

1. http://www.foruminternet.org/telechargement/documents/reco-archivage-20051201.pdf.

À retenir de l'intégrité

Ce qui précède démontre bien qu'en matière d'intégrité, il faut absolument faire la différence entre l'intégrité « technique » et l'intégrité « juridique ». Or seule l'intégrité « technique » a tendance à être véritablement appréhendée grâce aux algorithmes de calcul des empreintes numériques sur lesquels elle s'appuie. Certes ces contrôles d'empreintes sont importants voire nécessaires mais largement insuffisants dans le cadre d'un processus complet de conservation d'autant plus que les algorithmes utilisés sont soumis à l'obsolescence cryptographique.

1.3.4 Métadonnées

De par la présence du préfixe grec meta, indiquant l'auto référence, une métadonnée est elle-même une donnée servant à définir ou à décrire une autre donnée quel que soit son support (papier ou électronique).

Dans le cadre de nos préoccupations, retenons qu'il existe pour simplifier deux grands ensembles de métadonnées, l'un correspondant à un complément d'information et l'autre à des informations de gestion alimentées au fur et à mesure de l'avancement du document dans son cycle de vie. Les données complémentaires peuvent par exemple informer sur le créateur du document, de la date de création, de son format d'origine, etc. À ce titre elles représentent véritablement « l'identité numérique du document » car il est essentiel que l'on puisse véritablement s'y fier, leur faire confiance.

Enfin des métadonnées de qualité vont grandement faciliter la consultation et permettre d'améliorer la pertinence des résultats trouvés par un utilisateur au cours de ses recherches.

1.3.5 Stockage, conservation, archivage

Ces trois termes sont parfaitement complémentaires. Ainsi le stockage représente plutôt une fonction de base technique à laquelle la conservation ajoute une notion de préservation dans le temps. L'archivage complète la conservation avec des fonctions de gestion et de préservation du contexte.

La conservation représente donc une fonction destinée à préserver, et surtout à maintenir intact l'objet conservé quitte à utiliser différents types de stockage pour ce même objet. L'archivage consiste à prendre en compte, en plus de la conservation, les fonctions inhérentes à l'archivage, comme le fait de verser, de recueillir des nouvelles informations, de classer et surtout de permettre l'interrogation et de retrouver dans le temps les objets concernés. Le stockage revêt plus un rôle technique tandis que l'archivage représente un ensemble de fonctions dont la conservation fait partie, qui s'appuie naturellement sur du stockage.

1.3.6 Rétention

Ce mot est à utiliser avec précaution dans un contexte d'archivage. En effet, il provient d'une mauvaise traduction de son équivalent anglais « *retention* » dont la signification est à prendre ici dans son sens de conservation. La bonne interprétation à retenir est ainsi durée de conservation (ou DUA pour durée d'utilisation administrative). En effet, en français, rétention comporte la notion de garder une information qui devrait être diffusée ou encore l'idée d'être retenue contre son gré, nous sommes ainsi loin de la signification recherchée.

1.3.7 Gel

Au cours de la vie d'une archive, il se peut qu'un litige ou un contentieux se déclare. Dans pareil cas l'ensemble des documents correspondants doit être protégé contre toute destruction, même en fin de durée de prescription. Il s'agit de la fonction de « gel » qui doit absolument exister dans tout SAE. À l'issue du litige cette même fonction libère les documents qui reprennent leur vie normale d'archives.

1.4 POUR ÉVITER LES CONFUSIONS

1.4.1 Archivage, sauvegarde

Ces deux termes sont plutôt à comparer d'après leurs finalités et objectifs respectifs, lesquels sont totalement différents. En effet si la sauvegarde, tout comme l'archivage, revient à conserver de l'information, la finalité de la sauvegarde est uniquement de permettre une copie des données d'origine afin d'éviter de les perdre en cas de dysfonctionnement du dispositif sur lequel elles sont enregistrées et de pouvoir les restaurer dans pareil cas. De ce fait, la durée de conservation des sauvegardes est relativement limitée mais surtout les données doivent être sauvegardées très régulièrement voire en quasi-permanence dans la mesure où sont concernées des informations qui évoluent constamment. Après être ainsi passés par une logique de réplication asynchrone puis de CDP (*Continuous Data Protection*) nous en sommes aujourd'hui à un stade de réplication synchrone de plus en plus systématique des architectures.

La sauvegarde consiste ainsi à dupliquer l'information sur du court terme, il s'agit d'une opération préventive qui ne nécessite aucune recherche particulière.

À l'inverse l'archivage doit permettre une conservation qui peut être beaucoup plus longue, voire *ad vitam æternam*. L'archivage doit également permettre une interrogation aisée, même si elle est contrôlée, des objets conservés. L'archivage implique par conséquent l'existence de métadonnées métier. Contrairement à la sauvegarde, les données archivées sont figées, c'est-à-dire dans un état définitif donc non modifiables. L'archivage vise ainsi à sécuriser dans le temps (court, moyen ou long terme) et à permettre un accès aussi aisé que possible mais contrôlé aux données.

Le tableau ci-dessous résume l'ensemble des différences entre ces deux processus que sont la sauvegarde et l'archivage.

Tableau 1.1 — Sauvegarde et archivage

Un système de sauvegarde	Un système d'archivage
• concerne les données modifiables, en cours d'évolution ; • permet la restauration de données perdues dans le cadre d'un plan de reprise d'activité ; • est généralement organisé off-line et sur un autre site ; • doit permettre une restauration rapide et donc un accès suffisamment performant mais à fréquence très imprévisible.	• s'adresse aux données figées, validées ; • concerne la conservation de données afin de respecter ses obligations légales, réglementaires auxquelles s'ajoutent éventuellement les besoins historiques, patrimoniaux ; • permet la consultation en ligne et peut également prévoir une notion off-line, voire near-line ; • offre un accès avec une fréquence relativement régulière mais en général décroissante avec le temps.

Retenons en guise de synthèse que si l'information sauvegardée n'est pas archivée, l'information archivée doit faire l'objet de sauvegardes afin d'être sécurisée.

1.4.2 Gestion des archives, archivage électronique et *records management*

Parler de « *records management* » en France constitue déjà une difficulté dans la mesure où la doctrine archivistique française, qu'on retrouve dans la législation française, considère l'archive comme un tout depuis sa production ou sa réception par une personne physique ou morale, jusqu'à sa destruction ou sa conservation pour une durée illimitée. La loi française du 3 janvier 1979 modifiée par la loi n° 2008-696 du 15 juillet 2008 définit les archives comme « l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité.

La conservation de ces documents est organisée [...] tant pour les besoins de la gestion et de la justification des droits [...] ». Une même profession, celle des archivistes, intervient sur tous les différents âges de la vie des archives.

À l'inverse, les pays anglo-saxons disposent de termes différents pour caractériser les différentes étapes du cycle de vie de l'archive d'abord « *record* » puis « *archive* » pour le définitif. La norme ISO 15489 définit ainsi les « records » comme les « documents créés, reçus et préservés à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité ». Cette norme concerne les processus à mettre en œuvre afin, qu'au sein d'un organisme, un document conserve sa valeur de preuve, son intégrité et son intelligibilité grâce à sa capture dans un système d'enregistrement adapté. Un tel système garantit pour le document, le fait qu'il ne soit plus modifiable, son rattachement à un plan de classement basé sur les fonctions et activités de l'organisme, la détermination de sa durée de conservation, son sort final ainsi que les droits d'accès afférents. Nous y reviendrons très largement dans la suite de notre ouvrage.

Si l'on se réfère aux trois étapes retenues pour le cycle de vie de l'archive, à savoir : courante, intermédiaire et patrimoniale ou définitive, le *records management* ne concerne que les deux premières étapes. Généralement on parle d'archivage électronique à partir du moment où un versement (transfert) intervient, depuis une application métier, une application de *records management*, un serveur de messagerie... vers une plate-forme d'archivage externe. Une démarche de records management va plus loin puisqu'elle prend en compte le document dès sa création (voir schéma en fin de chapitre).

En pratique le terme « archives » renvoie au quotidien plus généralement à quelque chose d'ancien tandis que les « archives courantes » sont plus communément désignées par les mots « documents » ou encore « dossiers ».

Quoi qu'il en soit, l'essentiel est que ces documents soient figés, c'est-à-dire que leur contenu ne soit plus modifiable et qu'ils soient conservés pendant une certaine durée pour des raisons légales, réglementaires ou fonctionnelles avec des garanties d'intelligibilité, d'intégrité et de confidentialité.

1.4.3 GED ou GEIDE, SAE

La GED (gestion électronique de documents) ou GEIDE (gestion électronique d'informations et de documents existants), pour reprendre la définition donnée par l'APROGED (association des professionnels de la GEIDE) représente un ensemble d'outils et de techniques qui permettent de dématérialiser, classer, gérer et stocker des documents à partir d'applications informatiques dans le cadre normal des activités de l'entreprise. Datant des années 1980, la GED comporte des éléments essentiellement techniques sans connotation ni préoccupation juridique.

Il s'agit là d'une différence importante avec un SAE (système d'archivage électronique) dont le rôle est de conserver des documents électroniques avec une vocation légale et réglementaire importante dès l'origine. La majorité de l'activité GED est basée sur la notion de numérisation de documents existants et non sur la capture et la conservation de documents nativement numériques. Pour une meilleure compréhension de l'ensemble de la problématique relative à l'archivage électronique nous reproduisons ci-dessous un tableau comparatif des deux approches, tiré du document décrivant les spécifications MoReq2 (*Model Requirements for the Management of Electronic Records*)[1].

1. http://dlm-network.org/moreq2. Voir également la traduction française diffusée par les Archives de France.

Tableau 1.2 — GED et archivage

Un système de GED	Un système d'archivage électronique
• permet la modification des documents et la production de plusieurs versions ; • peut permettre la destruction des documents par leurs auteurs ; • peut comporter la gestion de durées de conservation ; • peut comprendre une structure organisée de stockage, sous le contrôle des utilisateurs ; • est *a priori* dédié à la gestion quotidienne des documents pour la conduite des affaires.	• interdit la modification des documents ; • interdit la destruction de documents en dehors d'un contrôle strict ; • comprend obligatoirement un contrôle rigoureux des durées de conservation ; • comprend obligatoirement l'utilisation d'une structure rigoureuse de classement (le plan de classement), gérée et contrôlée par l'administrateur ; • peut faciliter les tâches quotidiennes mais est aussi destiné à la constitution d'un fonds sécurisé des documents probants de l'entreprise.

1.4.4 Coffre-fort électronique

Définition

Il faut tout d'abord distinguer :

- le coffre outil qui correspond à un logiciel ;
- le coffre service avec une logique de SAE typique des tiers archiveurs.

Aujourd'hui, un SAE peut également être un coffre au sens grand public ; voir remarque ci-après.

En terme de fonctionnalités un coffre-fort électronique/numérique doit être vu comme un coffre-fort classique. Son fonctionnement est donc assez simple, voire rudimentaire et consiste à pouvoir y déposer un objet numérique et être capable de le retirer à tout moment avec une véritable garantie de sécurité en particulier en matière d'intégrité et de traçabilité.

Un coffre outil ne gère pas directement la confidentialité alors qu'un coffre service se doit de le faire en y associant également la notion de disponibilité.

Au-delà du simple coffre, l'offre peut s'étendre à la notion de salle des coffres où l'on dispose alors d'un ensemble sécurisé à l'intérieur duquel chacun dispose de son propre espace, de son propre coffre. Bien évidemment il n'y a aucune possibilité de communication entre les différents coffres d'un même espace afin de respecter l'aspect confidentialité.

> **Remarque** : Il existe également une autre approche du coffre, plutôt orientée particulier qu'entreprise, avec une notion sous-jacente de coffre-fort électronique du citoyen. Dans ce cas la notion de coffre doit être vue comme quelque chose de très simple à utiliser, de très intuitif et d'un autre côté souvent limité en terme de volumétrie. Nous ne nous intéressons pas ici à ce deuxième aspect.

Fonctions d'un coffre-fort électronique outil

Les principales fonctions d'un coffre-fort électronique se décomposent de la façon suivante :

- les fonctions ayant trait à la gestion d'un objet numérique, à savoir : déposer, lire et éliminer ;
- les fonctions liées au contrôle de l'intégrité de chaque objet numérique qui est conservé au sein du coffre-fort électronique mais aussi à l'intégrité de l'ensemble des objets ;
- la fonction de journalisation des actions dans le coffre-fort électronique relatives à la manipulation et au contrôle de l'intégrité des objets numériques qui y sont stockés ;
- les fonctions ayant trait à l'administration globale du coffre-fort électronique, comme l'initialisation du coffre-fort, la détection des anomalies, la gestion et le contrôle des accès.

1.4.5 Service d'archivage électronique

Définition

Un service d'archivage peut utiliser un coffre outil comme base technique. Ainsi, vis-à-vis de l'offre coffre-fort, un service d'archivage peut être vu comme un complément destiné à apporter entre autres les fonctions de versement, de classement, d'interrogation permettant au final à un utilisateur de retrouver les objets conservés. Cette notion englobe donc à la fois les aspects techniques et organisationnels.

Un service d'archivage électronique nécessite obligatoirement à la fois des logiciels et des plates-formes matérielles ainsi qu'un ensemble de procédures d'où l'utilisation du nom de SAE pour système d'archivage électronique.

Fonctions de base de l'archivage électronique

À titre indicatif, nous donnons dans le tableau 1.3 une liste des grandes fonctions de l'archivage électronique.

Au sujet de la suppression

En ce qui concerne la suppression, il est recommandé de n'appliquer l'automatisation qu'aux archives n'ayant pas de valeur légale ou qui pourraient être réutilisées. Les archives, notamment pour la sphère privée, restent la propriété du service versant/producteur, donc les détruire sans leur autorisation pose un véritable problème déontologique ! Lors de l'arrivée à échéance de conservation, le service archives ou le prestataire d'archivage demandent en général au service versant ou propriétaire de valider les destructions. Cette action se traduit par un document appelé communément « Ordre de destruction ».

Tableau 1.3 — Fonction d'un service d'archivage

Fonctions	Définition et complément
CAPTURE – CONNEXION	Applications quelconques Tout type d'objet numérique Métadonnées Vérifications
CLASSEMENT	Plan de classement Métadonnées Hiérarchisation Indexation full texte
RÈGLES DE GESTION	Droits d'accès (consultation) Habilitations (droit de faire) Formats Durées de conservation Événements déclencheurs de l'archivage Niveaux de services
CONFORMITÉ, VALEUR PROBANTE	Contrôles des signatures électroniques Horodatage Imputabilité Intégrité Traçabilité Gel, suspension des durées de conservation
CONSERVATION	Support adapté Migrations transparentes Conversion de format de fichier
INTERROGATION – RESTITUTION	Interrogation *via* un identifiant unique, des métadonnées, etc. Restitution possible en fonction de droits voire empêcher de connaître l'existence de documents dont on n'a pas les droits de consultation Consultation (à l'écran, impression, etc.) Restitution unitaire ou de masse
SUPPRESSION	Suppression manuelle ou automatique avec ou sans demande de confirmation Sécurisation de la suppression Suppression complète immédiate (avec notamment élimination des copies de sauvegarde)

Ces ordres de destruction peuvent également être conservés pour les raisons suivantes :

- être certain que le service versant a bien validé la suppression ;
- permettre au service concerné de vérifier qu'aucun contrôle, audit, contentieux en cours pourrait avoir besoin de ces documents ;
- conserver la trace que ces documents ont bien existé, qu'ils ont vécu en respectant le cycle de vie de l'information, qu'ils ont bien été détruits quand ils devaient l'être, à savoir :

– ni avant l'échéance : les documents n'ont pas été détruits frauduleusement ou pour cacher quelque chose ;
– ni après l'échéance (par exemple dans le respect des directives CNIL sur les données à caractère personnel).

1.4.6 e-Discovery

Il s'agit d'une procédure spécifique de la loi américaine comportant deux caractéristiques principales. La première consiste, avant d'entamer un procès, à pouvoir produire par l'ensemble des parties en présence, la totalité des informations susceptibles d'être utilisées pour le litige et ce quels qu'en soient la forme et le format (papier, témoignages, électronique...). La seconde revient à produire les informations demandées, au cours du procès, suite à la requête d'une des parties et à l'assignation du juge correspondante.

Signalons enfin que, depuis 2007, certaines spécificités en matière électronique ont été ajoutées à la loi d'origine, avec obligation de gérer de façon conforme la conservation des données au format électronique ESI (*Electronic Stored Information*).

Pour clore ce chapitre nous donnons ci-dessous un schéma permettant de mieux comprendre les différences entre archivage électronique, GED, *records management* et e-Discovery.

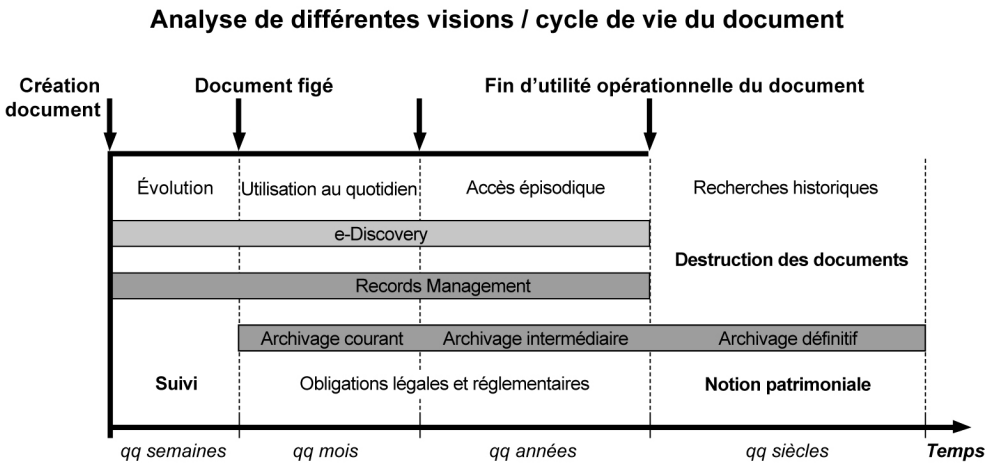

Figure 1.1 — Archivage, GED, RM et e-Discovery

En résumé

Un système de gestion de l'information et des documents doit être conçu en fonction de l'organisme et en regard de ses besoins. Il est primordial d'avoir identifié un certain nombre d'éléments (documents concernés, utilisateurs, processus métier, réglementation...). L'électronique doit répondre à des besoins de gestion, de gouvernance et de rationalisation de l'information.

Dématérialiser l'information n'est pas une fin en soi. Cette solution est une réponse à des besoins clairement identifiés et doit être possible tant en regard de la législation et de la réglementation, que des pratiques internes à l'organisme ou encore à sa capacité à s'intégrer au système d'information existant.

La dématérialisation n'est pas la réponse à tous les problèmes de gestion de l'information et des archives que l'on peut appliquer de façon standardisée.

Quant à l'archivage électronique il peut être vu comme une conséquence de la dématérialisation. Là encore il ne constitue pas une fin en soi. En effet, l'objectif principal de l'archivage n'est pas de conserver mais bien de retrouver et de pouvoir prouver. Tout comme la dématérialisation il doit s'intégrer au système d'information quitte à devoir le modifier, entre autres afin de prendre en compte certaines contraintes. À titre d'illustration de nos propos, citons l'obligation de garantir l'intégrité d'un document électronique dès l'instant où il est figé, validé et non pas seulement au moment où il est archivé.