Bulletin luxembourgeois des questions sociales

2004 Volume 15

aloss
association luxembourgeoise
des organismes de sécurité sociale

aloss
association luxembourgeoise
des organismes de sécurité sociale

BP 1308
L-1013 Luxembourg

ISBN 2-495-23043-1

TABLE DES MATIÈRES

ANNEXES : Dispositions légales et réglementaires

Allocution de Monsieur Carlo Wagner, Ministre de la Santé et de la Sécurité sociale à l'occasion de l'ouverture du séminaire du 22 avril 2004 organisé par l'aloss sur la " Gestion électronique des documents "

Mesdames, Messieurs,

La sécurité sociale est vorace de documents. Toute ouverture d'un droit aux prestations suppose une demande de la part de l'ayant droit. Toute demande doit être accompagnée par les documents appropriés : déclarations, attestations, factures et j'en passe. L'instruction des demandes comporte encore d'avantage de documents : avis du contrôle médical, attestations d'institutions de sécurité sociale étrangères.

La gestion des différents risques encourus par les quelques 570.000 personnes protégées par notre sécurité sociale entraîne la multiplication des dossiers, complique le traitement et le suivi des affaires, comporte des problèmes d'archivage. Face aux problèmes que comporte la gestion des documents papier, les différentes institutions ont tendance à s'appuyer sur une gestion électronique des documents.

La gestion électronique comporte de multiples avantages. Elle permet de faire abstraction de la circulation des documents et donc de la perte de pièces importantes. Elle facilite l'accès aux documents, qui peut être partagé entre les différents collaborateurs. Elle permet d'améliorer les flux de traitement des affaires et d'en assurer un meilleur suivi. L'assuré peut être renseigné plus rapidement sur l'état de son dossier. L'outil de gestion électronique des documents permet d'augmenter les performances de l'administration, d'améliorer les services au profit de l'assuré.

Toutefois, la gestion électronique des documents permet-elle de faire abstraction de la conservation des originaux papier ? L'archivage électronique peut-il remplacer l'archivage des documents papier ? Dans la mesure où l'assuré peut faire valoir ses droits aux prestations devant les juridictions, la question de la force probante des documents numérisés revêt une importance capitale. Telle est la question essentielle sur laquelle le séminaire d'aujourd'hui essaiera de trouver une réponse.

Je tiens à féliciter l'association luxembourgeoise des organismes de sécurité sociale (aloss), qui regroupe 18 institutions et administrations de la sécurité sociale, de consacrer son séminaire biennal à ce sujet, qui présente un intérêt commun.

Certaines institutions et administrations se sont d'ores et déjà orientées dans la direction de la gestion électronique des documents comme la Caisse nationale des prestations familiales, l'Association d'assurance contre les accidents, le Centre commun de la sécurité sociale, le Ministère et l'Inspection générale de la sécurité sociale. D'autres envisagent de le faire dans un avenir plus ou moins rapproché.

Les discussions et conclusions d'aujourd'hui devraient permettre de maintenir une certaine cohérence et d'éviter que des initiatives trop divergentes, voire contraires ne soient prises par les différentes institutions.

Pour la réalisation de ce séminaire l'aloss s'est associée le concours de l'Université du Luxembourg, du Centre de Recherche Public Gabriel Lippmann et du Laboratoire de Droit Economique, qu'il me tient à cœur de remercier pour leur participation.

Mesdames, Messieurs, il me reste à vous souhaiter un travail fructueux, afin que votre séminaire puisse être couronné du succès qu'il mérite.

L'introduction de la gestion électronique des documents dans l'administration: une décision stratégique complexe

Jean-Claude ASSELBORN

Professeur à l'Université du Luxembourg
Chef de projets au Centre de Recherche Public - Gabriel Lippmann

Les responsables des administrations sont de plus en plus souvent confrontés à la question de savoir si le moment est venu d'introduire un système de gestion électronique de documents (GED) dans le déroulement quotidien de l'administration. Bien qu'elle concerne à première vue le niveau opérationnel, la décision de le faire relève de la stratégie, car un tel choix déterminera l'évolution future de l'administration dans la société de l'information et touchera de près la culture administrative. De plus elle est délicate, car elle engage l'administration pour de nombreuses années et risque même d'être irréversible.

Pour aider les responsables administratifs à bien situer la complexité du problème dans sa globalité, le présent article introductif essaie d'en éclairer les différentes facettes, sans pour autant proposer des solutions toutes faites ou entrer dans des détails techniques. Le but est plutôt d'explorer toutes sortes d'implications que la décision risque d'avoir et d'amener les dirigeants administratifs à ne pas prendre une décision sur base des seuls arguments des prestataires de service dans le domaine de la gestion électronique de documents, souvent poussés davantage par leur désir de vendre un produit que par leur souci de résoudre un problème de l'administration.

Nous décrivons tout d'abord le cadre administratif général dans lequel se situe la décision de l'introduction d'un système GED et qui amène les responsables administratifs à en étudier l'opportunité.

Ensuite nous évoquons la vision d'une administration moderne, régulièrement suggérée par les promoteurs de systèmes GED pour convaincre les responsables administratifs, en décrivant les principaux avantages potentiels que l'introduction de la GED pourrait fournir à l'administration.

Nous soumettons ensuite cette vision idéalisée à une analyse critique en considérant aussi des alternatives possibles et en essayant de décrire les risques potentiels et les écueils éventuels auxquels l'introduction de la GED pourra être confrontée.

Différentes facettes sont analysées: les risques technologiques, l'impact sur la structure organisationnelle, le volet économique, les considérations ergonomiques et sociales, et enfin les questions juridiques.

1. Le cadre général de l'introduction de la GED dans l'administration

Les administrations font régulièrement l'objet de pressions politiques en vue de les amener à rationaliser leur travail en rendant leurs procédures plus transparentes et en mettant en oeuvre les outils techniques les plus modernes du moment. C'est ainsi qu'au début des années 1970, on a mis en place des organismes centralisés de gestion de l'information structurée des administrations, dans le but de bénéficier d'un effet d'économie d'échelle et de profiter au mieux des experts informatiques rares à l'époque. Le Centre Informatique de l'Etat ainsi que le Centre Informatique commun aux organismes de Sécurité Sociale ont progressivement pris en charge tous les processus répétitifs de masse et la gestion de bases de données volumineuses gérant des données communes à plusieurs entités administratives.

Au début des années 1980, les ordinateurs personnels ont fait leur apparition et avec eux une approche nouvelle de l'informatique, la bureautique, proposant la vision futuriste du "bureau sans papier". A l'époque, l'Etat luxembourgeois fit réaliser une étude d'opportunité sur la "bureautique au service de l'Etat", et le résultat n'en fut nullement un "bureau sans papier", mais l'introduction d'abord timide, ensuite de façon de plus en plus massive d'ordinateurs personnels dans les administrations. Tous ces ordinateurs, épaulés par des photocopieurs de plus en plus sophistiqués, contribuèrent à multiplier les documents papier, plutôt que de les réduire, et l'interconnexion progressive des ordinateurs personnels sous forme de réseaux locaux envahissant peu à peu tous les services ne changea rien à l'affaire. Par ailleurs, cette informatique parallèle fut parfois considérée comme une concurrence (déloyale?) à la "grande" informatique, ce qui plaça les organismes d'informatique centralisée dans une situation délicate, où ils étaient confrontés au dilemme de faire à la fois de la centralisation et de la décentralisation. En général, il s'en tinrent à la mission de centralisation qui leur était donnée par la loi, se contentant de jouer le rôle de centrale d'achat pour systèmes personnels, mais ne s'intéressant pas trop aux applications qui étaient envisagées par les administrations, ce qui plaça celles-ci dans la situation nouvelle d'organiser elles-mêmes leur bureautique. N'ayant pas la possibilité d'engager des informaticiens, fonction non prévue dans la carrière

administrative (en dehors des organismes d'informatique centralisée), les administrations durent recourir à la bonne volonté d'employés motivés par les nouvelles technologies et s'improvisant à l'occasion comme informaticiens amateurs. Le résultat n'en fut pas toujours convainquant, bien que des projets isolés fort intéressants fussent réalisés.

Les années 1990 virent l'apparition de l'internet, des téléphones portables et une révolution dans la façon générale de considérer l'informatique. Le courrier électronique devenait un vecteur qui remplaçait dans une large mesure le courrier en papier et les petits messages SMS transmis par les téléphones portables devinrent rapidement l'apanage de tous les jeunes branchés. Les administrations étaient soumises à de nouvelles pressions. La "réforme administrative" revint à l'ordre du jour et pour la première fois des solutions coopératives furent étudiées dans un cadre administratif. Une cible évidente de ces tentatives fut la gestion coopérative du courrier administratif, qui se prête très bien à la mise en place de procédures intégrées, depuis l'arrivée du courrier dans l'administration, jusqu'à son archivage dans des dossiers thématiques. C'est dans ce contexte que les discussions sur la GED devinrent de plus en plus fréquentes et un certain nombre d'administrations se sont lancées dans des expériences pilotes, dont certaines ont échoué. D'autres par contre ont présenté des résultats encourageants.

Avec l'arrivée d'un nouveau millénaire, les pressions de politique européenne engagèrent l'Etat dans une voie de *e-Europe, e-Luxembourg*[1)]*, e-Government* et les rapports comparatifs entre les réalisations des différents pays suggéraient que le Luxembourg avait des retards à combler, ce qui augmenta la pression politique sur les administrations à aller dans cette direction et à offrir des services "en-ligne".

Voilà la situation dans laquelle nous nous trouvons en ce moment, et les administrations, qui n'ont même pas encore réalisé la mise en oeuvre de la GED dans leur procédures quotidiennes, sont confrontées au nouveau défi de l'administration toute électronique. Par ailleurs, le ralentissement économique, qui a sensiblement réduit les ressources de l'Etat, ainsi que les pressions dues aux critères de convergence de Maastricht, font que les administrations ne peuvent guère augmenter le nombre de leurs collaborateurs et sont obligées de réaliser un volume de travail toujours croissant avec un effectif de plus en plus réduit, tout en offrant un service amélioré aux usagers.

C'est l'ensemble de ces pressions qui amène les responsables administratifs à aborder de façon plus consciencieuse la question de l'introduction de méthodes de gestion électronique de documents dans leurs services.

---

1) Voir http://www.eluxembourg.lu/eLuxembourg/index.html

2. Etudier les solutions GED possibles

La gestion électronique des documents a fait son apparition en même temps que la possibilité de numériser des images et de les stocker sur des supports optiques à très grande capacité et à coût très intéressant. En considérant un document papier comme une sorte d'image, il est possible de le stocker sous une forme entièrement électronique, tout en gardant la possibilité de le reproduire à tout instant comme copie conforme au document original. Dans sa forme électronique le document peut bénéficier de tous les avantages d'un traitement automatique, notamment les possibilités d'accès à des bases de données et la transmission automatisée d'un intervenant vers l'autre. Avec le temps les logiciels GED se sont étoffés et aujourd'hui les fournisseurs de tels systèmes sont fiers de mettre en vitrine toute une série d'avantages, comme le gain de place, la recherche par critères, la vitesse d'accès, la simultanéité d'accès en toute sécurité, la conservation cohérente et le traitement de dossier assisté par ordinateur. Par la suite nous aborderons chacun de ces points de façon plus détaillée.

2.1. Le gain de place

La plupart des administrations doivent conserver des dossiers avec des documents papier, qui remplissent des kilomètres de rayonnages. Cette conservation leur est imposée par des dispositions réglementaires, qui fixent, de façon pas toujours très claire, des durées obligatoires de conservation. En l'absence de règles précises, les administrations appliquent souvent un principe de prudence, qui les amène à ne pas jeter les documents anciens, ce qui a comme conséquence une montagne de vieux papier à gérer. Par sa nature même, ce problème ne se résout pas avec le temps, mais empire d'année en année.

Voilà pourquoi les responsables administratifs sont très sensibles à l'argument du gain de place, mis en avant par les fournisseurs de systèmes GED. Au lieu de kilomètres de rayonnages il suffirait à l'avenir de disposer de quelques armoires de disques optiques. En constatant de plus que l'espace, même de cave, est cher dans un environnement urbain, la réduction de l'espace nécessaire constitue certainement un avantage de poids.

Se pose toutefois le problème de savoir ce qu'on fera des documents papier originaux. Peut-on simplement les détruire? Nous aurons à y revenir sous le point des questions juridiques. Mais dès maintenant on peut noter que si l'on se contente d'appliquer un principe de prudence, en ne détruisant pas les originaux, mais en les conservant de façon chronologique dans des boîtes archivées en des endroits où le prix de l'espace de stockage est réduit, p.ex. un hangar en dehors de la ville, on fait un gain financier qui peut compenser le coût du système de GED. On y revient chercher un original uniquement lorsqu'on a à le produire explicitement pour obtenir gain de cause. Or cette éventualité est extrêmement rare. Par ailleurs, la disponibilité permanente de

l'image du document au sein de l'administration permet tous les traitements quotidiens du document. Au lieu de reposer de façon inactive dans les archives, le document peut à tout moment être exploité de façon intelligente.

2.2. La recherche par critères

Le document numérisé constitue une image, qui ne peut pas être exploitée directement par des méthodes informatiques. Pour rendre cette image accessible, il est indispensable de la décrire à l'aide de renseignements complémentaires, comme la date d'entrée, l'expéditeur, le destinataire, l'agent concerné, l'objet du document, peut-être même un résumé du document. Ces renseignements doivent être identifiés pour chaque document et être mis dans une base de données (indexation), ce qui permet de retrouver ultérieurement le document.

A noter que ceci ne doit pas nécessairement constituer un travail supplémentaire pour l'administration, car même à l'époque des registres manuels de courrier, l'administration devait inscrire ces renseignements, sauf que par après ils n'étaient guère exploitables automatiquement. Les fournisseurs de systèmes GED ne manqueront pas d'offrir des systèmes de recueil automatique de ces renseignements, par des méthodes d'analyse automatique du document, de localisation et de reconnaissance de certaines plages bien définies, et de l'extraction automatique des données intervenant dans les descripteurs. Ces techniques sont tout à fait performantes lorsqu'il s'agit de documents standardisés, comme les formulaires administratifs. En structurant judicieusement ces documents, en les munissant éventuellement de codes à barre, permettant d'identifier correctement le type de document ou le code d'identification de l'usager, une grande partie du travail de recueil des descripteurs du document pourra être rendue quasi-automatique.

Une fois ces descripteurs saisis et stockés sur des disques magnétiques extrêmement rapides, des perspectives tout à fait nouvelles s'offrent à celui qui doit rechercher un document précis. Les documents papier sont toujours stockés dans un ordre déterminé, p.ex. l'ordre chronologique, et pour retrouver le document par un autre critère, p.ex. le destinataire du document, on doit, soit constituer une table de correspondance manuelle ou informatisée permettant d'établir un lien entre les deux critères, soit stocker le document en deux endroits différents en produisant une copie du document, qui elle augmente de nouveau le volume de papier à gérer.

Avec la mise en base de données systématique des descripteurs du document par les systèmes de GED, on peut accéder au même document par des critères de recherche variés, et même combiner plusieurs de ces critères pour faire une recherche évoluée, p.ex. on peut chercher une réclamation qui nous est parvenue l'année dernière au cours du mois d'avril ou de mai de la part d'un usager déterminé. Le système fera la recherche et affichera en une fraction de seconde les descriptifs de tous les documents

qui répondent à ce critère combiné. L'agent administratif n'a qu'à parcourir la liste des réponses et sélectionner le document qui convient, un peu comme il le fait lors d'une recherche avec un navigateur web. Une fois le document sélectionné, le système GED va le récupérer dans l'archive optique et le reproduit à l'écran de l'usager.

De plus, les descripteurs initiaux du document peuvent être enrichis au cours du traitement en y ajoutant des indicateurs sur l'état de traitement, les agents ayant travaillé dessus ou les décisions administratives prises en relation avec le document. Ainsi chaque document électronique peut conserver sa propre histoire et ces données de traitement peuvent elles aussi de nouveau intervenir dans des critères de recherche, p.ex. nous voudrions afficher tous les formulaires de type A33 dont le traitement n'était pas achevé trois semaines après l'entrée du document dans l'administration. On comprend que le changement de technologie permet aussi d'envisager une adaptation de l'organisation des procédures administratives.

2.3. La vitesse et la simultanéité d'accès

En gestion manuelle des documents, accéder à un dossier présuppose en général qu'il faut se lever, ouvrir une armoire, localiser un dossier et le récupérer. Il faut ensuite chercher le document dans le dossier et plus tard refaire toutes ces opérations en sens inverse. Si par malheur le document a déjà été rangé dans les archives historiques, on doit le cas échéant envoyer quelqu'un dans la cave pour récupérer le dossier ou le document, ce qui peut prendre de quelques minutes à quelques heures.

Avec un système GED, l'accès peut se faire en quelques secondes, et ceci pour n'importe lequel parmi les millions de documents archivés électroniquement. L'utilisateur n'a pas besoin d'interrompre le rythme de ses activités et peut accéder de façon quasi-instantanée aux documents, ce qui peut se révéler être un grand avantage s'il est sollicité par téléphone par un usager externe de l'administration. Le service-client s'en trouve amélioré et l'agent administratif n'a pas besoin de rappeler ultérieurement la personne concernée, lorsqu'il aura finalement eu accès au document en papier.

Si un document papier n'est classé qu'en un seul endroit, alors il n'est accessible que par une seule personne à la fois. Un autre utilisateur concerné doit, soit attendre que le document soit libéré, soit se procurer une photocopie du document. En archivage électronique, le même document peut être consulté en même temps par un nombre quelconque de personnes, chacun voyant à son écran une copie du document électronique, alors que l'original électronique reste en permanence disponible sur le disque optique. Ceci va certainement accélérer le traitement des affaires et à nouveau le service-client s'en trouvera amélioré.

De plus, cette diffusion simultanée du même document en permet une révision rapide par plusieurs intervenants, en donnant à chacun la possibilité d'annoter le document, de formuler des commentaires ou de rédiger des consignes relatives au document. Toutes ces annotations peuvent être stockées de façon séparée, sans engendrer la moindre modification du document original.

2.4. La sécurité d'accès

L'accès à des documents administratifs en papier reste problématique, car en principe tous ceux qui peuvent accéder au local de stockage de par leurs fonctions, pourront consulter les documents et pourront théoriquement accéder à des dossiers autres que ceux qu'ils devaient ramener. Parmi eux, il peut y avoir des personnes à charges subalternes, comme les garçons de salle ou le personnel de nettoyage ou des agents d'entretien et de maintenance. Il peut aussi s'agir de personnel auxiliaire ou temporaire (p.ex. stagiaires), non lié par les mêmes serments que les fonctionnaires réguliers et non formé aux règles déontologiques applicables dans le service. Ceci peut être particulièrement critique lorsqu'il s'agit de documents de nature confidentielle et sensible, p.ex. des documents contenant des données à caractère médical, comme on en gère dans les caisses de maladie ou les organismes d'assurance accident. La divulgation de telles données peut tomber sous les dispositions de la législation sur la protection des personnes à l'égard du traitement des données à caractère personnel[1)] et l'administration est obligée de prendre toutes les mesures pour que ces données ne soient pas divulguées à des tiers non autorisés. Sa responsabilité est donc engagée.

Les systèmes GED protègent l'accès aux documents électroniques, en permettant de définir des droits d'accès tels que chacun ne puisse accéder qu'aux seuls documents auxquels il est autorisé à accéder de par ses fonctions, ou par son plan de travail. Ces droits peuvent être très sélectifs, en réservant l'accès à certains documents au seul chef responsable, alors que d'autres documents du même dossier pourront être accédés par ses collaborateurs, mais non pas par d'autres personnes. L'utilisation d'un système GED permet donc d'augmenter la confidentialité des documents.

---

1) Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [Mém. A 2002, n° 91, pp. 1835-1854]. Voir en particulier l'article 7 (Traitement de catégories particulières de données par les services de la santé), l'article 21 (Subordination), l'article 22 (Sécurité des traitements), l'article 23 (Mesures de sécurité particulières), l'article 25 (Sanctions relatives à la subordination et à la sécurité des traitements).

Un espion curieux n'a plus un accès physique aux documents, mais doit forcément passer par un système d'authentification de son identité et de contrôle de droit d'accès avant d'être en mesure de demander un document précis et de l'afficher à l'écran. Aussi tous les accès au document sont-ils retraçables et on peut de cette façon savoir exactement qui a accédé à quoi.

De plus, le serveur de documents se trouve généralement installé dans un local sécurisé à accès restreint, ce qui empêche que des personnes non autorisées puissent accéder physiquement aux installations de stockage. Les fournisseurs de systèmes GED peuvent même offrir des solutions de chiffrement de données sur les disques optiques, en vue d'empêcher que leur contenu ne tombe entre des mains non autorisées lors d'intrusions via des réseaux télématiques ou de vol de supports optiques. Seules les personnes autorisées possèdent la clé de déchiffrement des documents encryptés sur les disques optiques et personne d'autre, même pas le technicien de maintenance du système, n'arrivera à les reproduire sous leur forme originale.

2.5. La conservation cohérente

L'administration ne devrait pas perdre des documents, mais il arrive régulièrement que des documents ne soient plus retrouvés. Et il suffit de peu de choses pour que cela arrive. Un document consulté et reclassé après traitement dans le dossier voisin ne sera plus jamais retrouvé. Il se trouve toujours physiquement dans l'administration, mais on n'a aucune indication sur sa localisation actuelle.

En GED, le document électronique ne change jamais de place: il est gravé de façon ineffaçable sur un disque optique et toute consultation produit simplement une copie momentanée en mémoire de l'original gravé sur le disque. Ainsi, quoi qu'il arrive, le document pourra toujours être retrouvé, et même si d'un point de vue logique il fait partie d'un ou même de plusieurs dossiers, de façon physique il est unique et sera toujours récupéré au même endroit. Ceci augmente la fiabilité de l'administration et évite des pertes de temps dues à des recherches infructueuses.

En GED, on fait donc une distinction entre le document physiquement stocké sur un support informatique non réinscriptible et son affectation logique à des dossiers différents. En réalité ces dossiers ne sont que virtuels et sont des sortes de tables de matières électroniques, stockées sur des disques magnétiques rapides. Chaque document se trouvant dans un tel dossier, n'y figure que par une référence à l'endroit de stockage physique ou à un identifiant permettant de le localiser physiquement.

Ceci donne une grande souplesse à l'organisation de l'information administrative, car on peut définir des dossiers virtuels parfaitement adaptés aux finalités des traitements administratifs prévus. Pour un utilisateur qui consulte un tel dossier électronique, tout se passe comme si ce dossier existait physiquement, alors qu'en réalité chaque document du dossier est

recopié à partir de son endroit de stockage au moment même où l'on veut le consulter. Rien n'empêche donc de rendre le même document accessible à travers de multiples dossiers virtuels. Ainsi, on peut envisager que chaque agent administratif travaille avec des dossiers qui ne contiennent que les documents qui sont réellement nécessaires à son travail.

2.6. Le traitement des dossiers assisté par ordinateur

Lorsqu'un document papier entre dans une administration ayant mis en place un système GED, il est d'abord numérisé, contrôlé et enregistré sur un support électronique permanent. Ensuite il est analysé et on en extrait les descripteurs significatifs. Parmi ces descripteurs on peut prévoir un code, identifiant le genre de procédure administrative que ce document doit parcourir, p.ex. une demande de remboursement financier. Ce code permet ensuite de router le document à travers l'administration, en planifiant toute la chaîne des intervenants et en le faisant passer automatiquement de l'un vers l'autre (système de routage de flux de travaux), ou bien, de façon moins rigide, en mettant les documents à traiter dans une corbeille électronique commune, où ils peuvent être récupérés pour traitement par un agent disponible et qualifié, qui pourra, après traitement, le redéposer dans une corbeille appropriée pour la suite du traitement. Ces corbeilles pourront aussi être remplies automatiquement par l'ordinateur, qui peut sélectionner certains documents à traiter en fonction de contraintes de calendrier, p.ex. lorsqu'un certain délai est échu ou lorsqu'un certain intervenant, qui était absent pour une raison ou une autre, est de nouveau présent.

Ainsi les documents circulent de façon complètement automatisée et il n'y aura plus de délais dus au transport physique des documents d'un bureau vers l'autre. De plus, comme il n'y a plus de piles de documents papier en attente de traitement, les bureaux seront nettement plus dégagés et l'environnement de travail s'en trouvera amélioré.

L'assistance informatique ne doit pas nécessairement se limiter au transport rapide des documents. On peut envisager des logiciels d'assistance bien plus puissants, qui préparent déjà le travail de l'agent administratif concerné, en réalisant toutes les tâches de routine, comme la mise à disposition de données complémentaires, nécessaires à l'appréciation de l'affaire en cours et récupérées automatiquement dans toutes sortes de fichiers ou de bases de données, ou bien des calculs auxiliaires, l'assistance à l'application de règles de gestion ou la production d'une lettre type. L'ordinateur fait en quelque sorte un pré-traitement du dossier; ainsi, il peut p. ex. vérifier que toutes les pièces nécessaires sont présentes dans le dossier.

L'agent administratif, pour sa part, pourra se concentrer sur ses compétences typiquement humaines: l'appréciation de faits et l'interprétation de règles dans des cas limites, l'identification d'incohérences cachées ou le redressement d'erreurs. Toutes ces compétences sont le fruit

de sa longue expérience professionnelle et de ses capacités cognitives. L'ordinateur ne peut pas réaliser ces tâches-là. Par contre l'ordinateur peut faire du bon travail préparatoire et aussi réaliser certains post-traitements, comme p.ex. l'exécution de certaines décisions. Il en résulte que ces systèmes de traitement de dossiers assisté par ordinateur combinent judicieusement les compétences humaines et les possibilités de traitement automatisé. La productivité des agents en sera améliorée, les tâches répétitives et fastidieuses sont éliminées.

De plus, ces systèmes de traitement de dossier assisté par ordinateur sont parfaitement au courant de l'état de traitement de chaque dossier, ce qui permet un suivi automatique du travail réalisé par une entité administrative. Des anomalies, p.ex. des délais trop longs, pourront être détectées et signalées aux responsables par le système de gestion des travaux. Ceci permet de réagir plus rapidement aux goulots d'étranglement momentanés et aux demandes sur l'état d'avancement des dossiers de la part des usagers. A la limite, on constate qu'il devient techniquement possible que les usagers eux-mêmes, après identification correcte, puissent accéder à ces informations sur l'avancement du traitement de leur affaire.

Le lecteur attentif aura constaté que nous nous sommes éloignés de la GED simple, qui se contente généralement d'archiver sous une forme électronique des grandes quantités de documents; nous sommes progressivement passés à un système intégré, qui fait à la fois de la gestion de documents, mais aussi de la gestion d'informations au sens large. Il en résulte que pour atteindre ce niveau-là, le système de gestion électronique de documents devra offrir des passerelles avec le système d'information automatisé déjà en place. Les fournisseurs de systèmes GED ne manqueront pas d'offrir leurs services pour réaliser ces passerelles. Ceci peut néanmoins présenter des difficultés et nous aurons à y revenir lors de l'analyse des risques.

2.7. Vers une gestion de documents électroniques

Jusqu'à présent, nous avons toujours supposé que les documents existaient initialement sous forme originale en papier, que cet original n'était conservé que pour des raisons de valeur probante lors d'un litige devant les tribunaux, et que les traitements réels se faisaient sur l'image numérisée de ces documents.

Mais les objectifs des visions *e-Government* vont bien au-delà de cette approche traditionnelle et visent clairement l'interaction directe et complètement électronique de l'usager avec son administration. A ce moment, l'usager pourrait remplir ses formulaires directement sous une forme électronique et toute l'étape de numérisation et d'analyse des documents deviendrait superflue. Si ceci soulève de nouveaux problèmes (comme p.ex. l'authentification certaine de l'interlocuteur, la confidentialité des transmissions, la garantie de non-répudiation de la part de l'usager, le

datage certain, l'intégrité du document lors de sa transmission), on constate néanmoins qu'il y a une certaine continuité dans l'approche. Ainsi la GED se décline sous de nombreuses formes et la suppression complète du papier n'en constitue que l'aboutissement le plus évolué.

On peut ainsi concevoir un passage progressif vers des solutions GED de plus en plus sophistiquées:

- on pourrait commencer par un système où la procédure administrative continuerait à se faire de façon traditionnelle sur le document papier, mais où, après traitement, les documents seraient archivés sous une forme électronique, en vue de les retrouver ultérieurement;
- on pourrait ensuite introduire des systèmes de distribution automatique des documents électroniques à travers le système administratif;
- par après, on développerait progressivement des applications de traitement d'affaires assisté par ordinateur, en intégrant de plus en plus la gestion des documents et la gestion informatique classique;
- finalement, on passerait à des solutions *e-Government* complètement électroniques, où le citoyen interagirait directement via internet avec le système administratif assisté par ordinateur.

Mais les contraintes politiques et stratégiques pourraient aussi obliger les responsables administratifs à envisager de passer directement à une solution évoluée, offrant à l'usager de l'administration la possibilité d'utiliser des démarches traditionnelles, ou bien de profiter de la souplesse des nouveaux canaux de communication électronique.

Avant de se lancer dans un projet de GED, il est donc indispensable d'avoir préalablement éclairci la question de la stratégie, afin de savoir clairement ce qu'on entend par GED dans un contexte donné. Il est évident que, suivant le niveau de GED visé, la complexité du projet et les ressources nécessaires pourront varier dans une très large mesure. Il n'y a donc pas seulement un type de projet GED, mais chaque projet est différent et dépend de l'environnement socio-économique et de multiples contraintes à satisfaire. Voilà pourquoi il n'est pas possible de décrire une solution universelle, tout comme il n'existera pas un produit passe-partout qui résoudra tous les problèmes. D'un autre côté, quel que soit le niveau de GED visé, il faut être conscient qu'on devra probablement un jour évoluer vers un niveau plus élevé. On a donc tout intérêt à prendre en compte dès le départ l'évolution de la solution dans le temps, afin de ne pas avoir à refaire tout le travail le jour où l'on se proposera de passer au niveau supérieur.

3. Envisager des solutions alternatives

En suivant l'argumentaire des prestataires de services et systèmes de GED, nous avons pu constater que la GED offre effectivement des solutions convaincantes à un grand nombre de problèmes qui pourraient se présenter

dans l'administration. Certains pourraient même être amenés à croire que sans GED il n'y a pas de salut ou qu'ils risqueraient d'être considérés comme des gestionnaires poussiéreux et arriérés, menant des combats d'arrière-garde contre le progrès technologique, s'ils n'empruntaient pas la voie tracée par les promoteurs de systèmes GED.

Tel n'est pourtant pas le cas. Même si la GED offre des solutions à toute une panoplie de problèmes, il s'agit d'abord de savoir si ce sont aussi les problèmes de l'administration concernée, et si oui, d'explorer quelles autres solutions pourraient être envisagées pour venir à bout de ces problèmes. Des solutions alternatives peuvent parfois apporter une réponse plus fondamentale au problème, une fois qu'il a été correctement identifié. Le responsable administratif se posera donc d'abord la question de savoir quelles sont les causes profondes du problème, avant de se contenter d'une solution qui traite les symptômes visibles du problème, sans réellement en attaquer les causes.

3.1. Le problème du manque de place de stockage

L'administration qui voit ses archives s'étendre à des kilomètres de dossiers peut facilement être séduite par la perspective de réduction de cet espace à quelques armoires de systèmes électroniques. Mais n'a-t-elle pas simplement fait un changement superficiel, en remplaçant une forme de support par une autre?

La véritable question à se poser, c'est "*quelles sont les causes de l'extension démesurée des archives?*". Et en essayant d'étudier cette question on trouvera peut-être que les archives s'étendent toujours davantage parce qu'on ne jette jamais rien, ou parce qu'on conserve trop longtemps des documents périmés. Ainsi p.ex. une étude réalisée au service du personnel d'une grande banque de la place financière a montré que 75% des documents conservés dans les dossiers du personnel ne servaient à rien et n'étaient jamais consultés après classement dans le dossier. Pourquoi alors archiver ces documents? L'analyse a montré que les responsables administratifs ne jettent jamais des documents papier, parce qu'ils ont peur qu'on puisse leur en faire le reproche un jour. Ceci a comme conséquence que les dossiers jouent en quelque sorte le rôle de poubelles où l'on conserve tout ce qu'il faudrait en réalité jeter.

On pourra invoquer des délais de conservation légaux. S'il est vrai que de tels délais peuvent exister, on doit néanmoins constater que les règles correspondantes sont souvent floues et ne précisent nullement ce qu'il faut conserver et ce qu'on pourrait jeter. L'administration doit garder la trace de ses actions, mais est-ce que toute notice provisoire doit réellement être tracée? Ne suffit-il pas que l'administration garde simplement la trace de ses décisions, sans conserver éternellement l'ensemble des éléments qui ont mené à la décision?

Il est d'ailleurs curieux de constater que les administrations ont parfois des plans de classement très développés, qui précisent où chaque document doit être rangé. Mais il n'existe pratiquement jamais de procédure organisée pour nettoyer les dossiers, en enlevant systématiquement les documents périmés et n'intervenant plus dans d'éventuels litiges ultérieurs.

Ricardo Semler cite le cas d'une entreprise brésilienne[1)], qui était sur le point de faire une importante commande d'armoires d'archivage supplémentaires. Au lieu de lancer la commande, l'entreprise a décidé de fermer tous les bureaux pendant une demi-journée et de consacrer cette matinée à passer en revue les dossiers, en jetant tout ce qui ne servait plus et en se posant la question "*Qu'est-ce qui peut arriver de plus grave, lorsqu'on jette ce document?*". Le résultat fut impressionnant. Les gens étaient étonnés par toutes les choses inutiles qu'ils conservaient dans leurs armoires et à la fin de l'opération il ne restait plus qu'un quart des documents initiaux. Au lieu d'acheter des armoires, on avait des armoires en trop.

Si cette entreprise s'était au contraire décidée à acquérir un système GED pour résoudre le problème de place, elle aurait continué à gérer tous ces documents inutiles, mais sous une forme électronique. Et comme les documents numérisés sont gravés de façon ineffaçable sur le disque optique, il n'est même pas possible de les détruire sélectivement. Au lieu d'armoires supplémentaires, ce sont des disques optiques supplémentaires qu'il faut acheter, tout en trouvant une solution pour gérer les disques anciens.

Le responsable administratif, confronté au problème de la place d'archivage, étudiera donc d'abord les moyens lui permettant de réduire le volume de papier, en simplifiant ses procédures, en réduisant le nombre de formulaires et en ne demandant pas des informations qui figurent depuis longtemps dans son système informatique. Il cherchera ensuite des moyens pour conserver les documents juste le temps qu'il faudra pour répondre aux contraintes légales. Ensuite seulement il réfléchira à la meilleure solution technique pour gérer les documents restants.

Il y a toutefois des situations où la numérisation des documents s'offre de façon tout à fait naturelle: c'est la cas lorsque les documents à gérer sont par nature déjà des images ou des schémas, p.ex. des croquis d'accidents ou des photos.

3.2. Le problème de l'accès convivial aux documents

A cause de l'indexation des documents, les systèmes GED permettent un accès souple et par des chemins variés aux documents. L'indexation peut même être en grande partie automatisée lorsque les documents sont

---

1) R. Semler "Das SEMCO System", Heyne 1993, pp. 176-180.

numérisés, du moins lorsqu'il s'agit de documents standards, comme des formulaires.

Le décideur administratif devra donc vérifier si ceci est bien son cas. En effet, dès que les documents à gérer sont de forme libre, la description du document doit se faire de façon manuelle. Dans ce cas la numérisation du document n'est plus indispensable et rien ne s'oppose à la mise en oeuvre d'une solution où les documents continuent de circuler sous forme papier, alors que la gestion des documents et de leurs descriptifs se fait de façon électronique.

On constate en effet que dès qu'on s'élève au dessus du niveau opérationnel de l'administration, les documents deviennent de moins en moins structurés et les agents traitants de plus en plus réticents à les consulter sur écran. A ce moment une solution GED pure risque de provoquer des problèmes d'acceptabilité.

Au cours des études du programme RACE[1)], on a proposé des solutions de gestion électronique des affaires souvent complexes, qui sont gérées quotidiennement par les administrations gouvernementales. La solution n'imposait pas la numérisation des documents, mais se concentrait sur la gestion de toutes les informations importantes intervenant dans la gestion d'une affaire: son historique, les intervenants, la description succincte des documents échangés, la description des événements qui sont apparus en relation avec l'affaire (entretiens téléphoniques, notices, réunions), les décisions prises. Ces expériences ont montré qu'il est tout à fait possible de mettre en oeuvre une gestion électronique des informations relatives à des affaires, sans pour autant passer à une numérisation systématique des documents. En effet, lorsque le document est peu structuré, la forme papier garde ses avantages. Sinon, la première chose que feront les agents traitants, c'est d'imprimer une copie papier du document, sur laquelle ils travailleront et qu'ils archiveront par après.

Le décideur devra donc bien se rendre compte du type de documents qui sont gérés par son administration et ensuite estimer si la numérisation des documents pourra réellement résoudre son problème. Les solutions GED sont plutôt adaptées à des situations très procédurales, où les messages échangés sont très structurés et standardisés. Le décideur se rendra compte à ce moment que les situations qui se prêtent bien à une numérisation des documents sont exactement les mêmes que celles qui se prêtent à un échange de messages internet à l'aide de formulaires électroniques, où le papier est complètement supprimé. Une alternative sera alors d'envisager de passer directement à une solution *e-Government*, plutôt que d'investir de

---

1) RACE = Réforme administrative par la Coopération électronique; ce programme de recherche, mené par l'auteur de l'article au Centre de Recherche Public - Gabriel Lippmann, s'est déroulé dans un certain nombre de ministères et d'administrations entre 1998 et 2002.

grandes sommes dans la gestion du papier, qui peut alors être considéré comme un support d'information dépassé, dont le rôle diminuera de toute façon dans les années à venir.

3.3. Le problème de la réactivité

Les solutions GED permettent d'afficher dans les délais les plus courts des documents qui se trouvent dans le système d'archivage électronique. Ceci permet notamment de réagir très rapidement à des demandes ponctuelles des usagers.

Le décideur se posera toutefois la question de savoir si cette situation est fréquente dans l'application GED qu'il envisage. Il se demandera ensuite s'il est vraiment nécessaire de disposer à ce moment de la version numérisée d'un document papier, ou s'il suffit déjà de pouvoir renseigner l'usager sur l'état d'avancement de son affaire. A ce moment, un bon système de gestion d'affaires, sans numérisation systématique des documents, pourrait aussi convenir.

De nouveau, il essaiera d'identifier la cause du problème, plutôt que de traiter un symptôme du problème. Pourquoi l'usager contacte-t-il l'administration? Il se peut qu'il n'ait pas reçu d'accusé de réception à sa demande et il voudrait s'assurer que son document est bien arrivé à destination. Dans ce cas, le responsable administratif aurait intérêt à améliorer systématiquement la communication avec l'usager plutôt que de chercher des moyens pour retrouver rapidement un document donné.

Le problème de l'usager, c'est qu'il voudrait être renseigné sur le déroulement de la procédure administrative. Le décideur se posera dès lors la question de savoir s'il ne devrait pas plutôt mettre en place un système permettant à l'usager de suivre à distance l'évolution de son dossier administratif. Bien sûr, un système GED pourra convenir comme solution, mais il y a peut-être d'autres solutions plus pertinentes.

3.4. Le problème de la sécurité

Les systèmes GED permettent de conserver les documents de façon confidentielle, en réservant l'accès aux seules personnes autorisées.

Le décideur déterminera si des problèmes de sécurité se posent réellement dans son administration. En effet, si les données ne sont pas sensibles, si le cadre administratif est bien formé et conscient de ses obligations déontologiques, le problème de la sécurité d'accès ne se posera peut-être pas. Depuis toujours, des institutions ont su gérer des documents papier classifiés secrets, en mettant en oeuvre des procédures organisationnelles très rigoureuses, plutôt que des solutions technologiques.

La faiblesse des solutions technologiques, c'est qu'elles ne protègent pas vraiment contre les abus commis par des agents autorisés d'accéder à des dossiers dans l'exercice de leurs fonctions. Or, l'expérience montre que la plupart des fuites de renseignements confidentiels proviennent de personnes qui y ont accès de façon légitime.

Le décideur devra donc établir si une solution GED seule va résoudre son éventuel problème de confidentialité et de sécurité d'accès.

3.5. Le problème de la gestion cohérente des dossiers

Les systèmes GED permettent de gérer des dossiers de façon souple et cohérente, en créant des dossiers virtuels qui font référence à des images de documents.

On notera toutefois que cet effet ne provient pas tant de la numérisation des documents que de la mise en oeuvre d'un système de gestion de dossiers. L'important n'est pas la copie numérisée d'un document papier, mais l'essence du message transporté par le document en papier. Or, l'objet d'un document peut souvent être résumé par une phrase bien choisie ou un code de classification, sans pour autant devoir chaque fois visualiser la forme du document correspondant. Une fois l'extraction de la signification administrative du document réalisée, l'original papier perd beaucoup de son intérêt.

Le décideur se posera donc la question de savoir s'il dispose d'un bon système de gestion de dossiers et analysera aussi des solutions qui ne nécessitent pas forcément la numérisation des documents. Il est vrai que les systèmes GED évolués offrent en général cette possibilité.

***

Dans ce qui précède nous avons passé en revue des approches alternatives à l'abandon du papier et à la gestion de documents numérisés complètement électroniques. Nous avons pu constater que rares sont les situations où l'abandon du papier constitue la seule approche rationnelle possible. Le décideur pèsera donc le pour et le contre de chaque approche et arrivera peut-être à la conclusion que tous comptes faits, une approche GED avec numérisation totale des documents papier n'est pas nécessaire dans son cas de figure. Il préféra peut-être investir dans un système de gestion d'affaires, sans abandonner le support papier, car les avantages espérés peuvent très bien provenir d'une gestion coopérative d'affaires en cours, plutôt que de l'affichage des documents qui les ont déclenchées.

4. Evaluer les risques

Mais il se peut tout aussi bien que le décideur soit arrivé à la conclusion que la mise en place d'un système GED plus ou moins évolué constitue la voie que son administration devrait suivre à l'avenir. Dès lors, il devra en mesurer l'impact et déterminer si les conséquences prévisibles sont assumables par son administration et s'il dispose des moyens pour maîtriser les risques associés inévitables. Bien sûr, la perception du degré de ces risques dépend fortement du contexte et de l'état de développement de l'administration concernée. Aussi ne sera-t-il pas possible dans cet article de fournir une mesure objective de l'intensité d'un risque donné. Nous essaierons plutôt de passer en revue les différentes catégories de risques, afin que le décideur n'oublie pas l'un ou l'autre aspect important.

Les facettes à analyser sont multiples et variées: les risques technologiques ne sont pas négligeables, mais le volet organisationnel est souvent plus délicat encore. Aux questions économiques s'ajoutent des problèmes d'acceptabilité par le personnel. Finalement, l'étude des question juridiques peut se révéler très délicate.

4.1. Les risques technologiques

La mise en oeuvre de la GED ressemble davantage à un projet de construction d'un bâtiment administratif qu'à l'acquisition d'une voiture de service par l'administration. En effet, les solutions GED résultent de la combinaison de nombreux composants, tous différents les uns des autres, et faisant intervenir des fournisseurs spécialisés, un peu comme dans la construction d'un bâtiment de nombreux corps de métiers interviennent et doivent être coordonnés.

Ainsi, il y a les produits de numérisation, "scanners" plus ou moins évolués, qui doivent être choisis en fonction de la nature et de la masse des documents à numériser. Il y a les produits d'analyse et de reconnaissance de données inscrites sur des documents, en vue d'automatiser la saisie des descripteurs; ces produits font intervenir des technologies différentes de celles utilisées par les produits de numérisation. Il y a les solutions de stockage sur des disques optiques ou d'autres types de mémoires de masse. Il faut aussi un système de gestion de bases de données pour gérer les données structurées associées aux documents. Il y a finalement les produits de routage de flux de travaux, qui gèrent les affaires en cours et se chargent d'organiser leur traitement assisté par ordinateur.

Cette complexité de projet engendre plusieurs problèmes:

- le problème de la coordination des activités des différents intervenants;
- le problème de l'interconnexion de composants en provenance de producteurs différents;

- le problème de l'évolution variable dans le temps des différents composants.

L'administration devient ainsi maître d'ouvrage d'un projet complexe dont elle ne maîtrise pas tous les détails techniques; elle a donc intérêt à s'adresser à un maître d'oeuvre compétent, qui fera figure d'intégrateur et fournira une solution clef en mains, en déchargeant le maître d'ouvrage des tâches de coordination et de négociation avec les sous-traitants fournissant les différents composants. Le choix d'un tel **intégrateur** constitue un élément critique de tout le projet.

L'intégrateur devra veiller à ce que les différents composants puissent travailler ensemble. A cette fin, il fournira les interfaces qui permettent les échanges de données entre deux composants. Dans ce contexte se pose le problème des standards d'échange; l'administration a intérêt à privilégier des solutions qui respectent des **standards** largement reconnus et d'éviter des solutions ad-hoc développées sur mesure par un prestataire donné.

Comme pour un bâtiment, la durée de vie du produit s'étend sur des dizaines d'années, voire sur des périodes plus longues encore. Mais contrairement à ce qui se passe pour un bâtiment, les technologies informatiques évoluent rapidement, et ce qui paraît correspondre à l'état de l'art aujourd'hui peut être considéré comme vétuste dans quelques années. Il est donc essentiel de garantir **l'évolutivité** de la solution en veillant à ce qu'elle soit modulaire et permette d'échanger sans problèmes un composant contre un autre mieux approprié. Ceci n'est possible que lorsque les interfaces respectent rigoureusement des standards appliqués par le plus grand nombre possible de fournisseurs.

Il en résulte que la **relation avec le maître d'oeuvre** risque de se prolonger au-delà de la mise en service initiale et qu'une relation de confiance s'étendant sur de nombreuses années devra s'établir entre l'administration et son maître d'oeuvre intégrateur. Dès le début, l'administration devra faire un pari sur la perennité probable du maître d'oeuvre et sur la possibilité de faire évoluer les produits utilisés.

On comprend donc aussi qu'un projet GED n'est jamais vraiment clôturé et risque de lier des ressources permanentes dans l'administration.

Toutes les solutions technologiques posent le problème de leur **disponibilité permanente**. Plus une solution est intégrée et détermine le travail d'un nombre important de personnes, plus l'administration qui la met en oeuvre en devient dépendante. En cas de non disponibilité de l'infrastructure technique pour cause de panne, d'accident, de grève ou de sabotage, le fonctionnement de l'administration sera bloqué. Les solutions papier traditionnelles ne présentent pas ce même degré de dépendance.

Le décideur doit donc être conscient qu'il faudra prévoir (et financer) des mesures nécessaires pour assurer la disponibilité sans interruption de la solution choisie, en prévoyant des mesures de protection contre les pannes (contrats de maintenance, équipements de secours, solutions externes de rechange), contre les accidents (protection incendie, copies de sauvegarde, plan catastrophe), contre le blocage abusif (sécurité d'accès des locaux et des installations annexes, découplage entre réseau interne et réseau externe, mesures contre l'intrusion informatique).

Nous avons décrit plus haut comment les solutions GED pouvaient largement tirer profit d'une interaction intelligente avec les applications informatiques existantes. L'accès à des données gérées au niveau centralisé par un centre de calcul mis en place dans les années 1970 risque de ne pas se faire sans problèmes, tout d'abord parce que les technologies centralisées mises en oeuvre à l'époque ne sont pas forcément appropriées à une communication avec des systèmes externes, ensuite parce qu'une telle interaction technique soulève le délicat problème des relations et du partage des tâches entre un **organisme d'informatique centralisée** et une administration, qui en dépend pour ses réalisations informatiques.

Si l'organisme d'informatique centralisée ne coopère pas, l'administration qui veut mettre en oeuvre une solution GED se privera de ressources de données précieuses, devra développer des solutions à part pour générer automatiquement les mises à jour des bases de données centralisées, et son projet de rationalisation risque de ne pas fournir les résultats escomptés ou théoriquement possibles.

Si l'organisme d'informatique centralisée coopère, il risque d'accaparer le projet à son compte et de concevoir une solution centralisée commune à toutes les administrations qui en dépendent, sans nécessairement se préoccuper des particularités spécifiques d'une administration donnée.

Quelle que soit l'attitude de l'organisme d'informatique centralisée, l'administration devra prévoir les ressources humaines locales suffisantes et compétentes pour gérer informatiquement son projet GED. Il faudra recourir à des **informaticiens professionnels**, prévoir les locaux techniques et les bureaux nécessaires. Ceci peut poser un problème si les agents-informaticiens ne sont pas prévus dans le cadre du personnel administratif. La solution qui consiste à les recruter via l'organisme d'informatique centralisée et à les détacher à l'administration concernée pose le problème de la double dépendance hiérarchique des informaticiens en question et d'un partage de responsabilités pas toujours évident entre l'administration et l'organisme d'informatique centralisée. La solution du sous-traitement à un prestaire de services privé externe peut soulever des problèmes de sécurité et de confidentialité.

La technologie risque de poser d'autres problèmes non prévus: **l'infrastructure bureautique** en place actuellement n'est pas nécessairement appropriée pour une mise en oeuvre de la GED. En effet, la numérisation de documents consiste à en faire des images; or le traitement d'images nécessite des ressources informatiques beaucoup plus puissantes que le traitement de textes: il faut donc des ordinateurs personnels suffisamment puissants et rapides, des réseaux locaux à large bande passante, des écrans de grande taille et de très bonne qualité. L'inventaire de l'existant montrera si cette infrastructure de base est disponible, ou s'il faut l'acquérir en plus.

4.2. Les aspects organisationnels

La gestion électronique des documents ne se limite pas à un changement de technologie. Avant de pouvoir gérer électroniquement des documents, il est indispensable de faire préalablement l'analyse de l'existant, d'établir une catégorisation des documents, de définir la structure des dossiers électroniques et de réfléchir à la meilleure façon d'utiliser l'outil GED dans la gestion quotidienne.

Les procédures administratives ont souvent été mises en place longtemps avant l'époque de l'informatique. Par la suite, elles ont évolué, de façon parfois ponctuelle, en fonction des besoins momentanés du travail administratif (rapports à produire, statistiques à fournir, changements de réglementation, remise en cause par des décisions de juridictions administratives, automatisation de certaines parties). Lorsqu'on veut les mettre à l'heure de la GED, on constate souvent qu'elles n'ont jamais été décrites de façon rigoureuse et selon des méthodes éprouvées. Il se peut même qu'il n'y ait personne dans toute l'administration qui maîtrise une procédure donnée depuis l'entrée d'un document jusqu'à la clôture d'une affaire.

L'analyse des procédures et des documents constitue un travail de longue haleine, qui requiert une grande expérience en modélisation et une bonne connaissance des possibilités techniques à mettre en oeuvre. Généralement, ce n'est pas le maître d'oeuvre intégrateur, choisi par l'administration pour la réalisation technique, qui sera à même de faire ce travail. Tout comme l'entrepreneur de génie civil se concentre sur la construction physique d'un bâtiment, il faut un architecte et des bureaux d'ingénieurs pour définir et étudier correctement les besoins et les solutions potentielles. Pour un projet GED, l'administration, maître d'ouvrage, se fera assister par un conseiller, expert en modélisation et en définition de solutions administratives.

Mais le décideur doit être conscient du fait que, même si cet expert coûte beaucoup d'argent, on ne peut pas simplement lui sous-traiter le travail d'analyse et de conception de la solution, car il ne pourra produire des résultats que s'il est assisté dans son travail par des experts internes à

l'administration, maîtrisant à fond l'organisation actuelle et les règles appliquées. Le décideur devra donc évaluer s'il dispose de ces ressources internes, et s'il peut les libérer pendant un temps suffisamment long pour s'impliquer à fond dans le projet GED. Aussi est-il indispensable que ces correspondants internes soient motivés par le projet.

Une erreur courante consiste à transposer les façons de procéder actuelles vers une solution de gestion électronique qui correspond exactement à la procédure manuelle. Ce n'est pas en automatisant une mauvaise procédure qu'elle sera améliorée. Ce qu'il faudra, c'est réexaminer toutes les procédures d'une façon critique et les remettre en cause s'il y a des raisons convaincantes pour le faire. La modélisation des procédures en place fait souvent apparaître des tâches redondantes ou bien des tâches qui n'ont plus de raison d'être, mais qui sont réalisées par tradition, ou bien des tâches de contrôle qui pourraient être réalisées de façon beaucoup plus simple en bénéficiant de l'apport technique du système de GED. Ainsi p.ex. l'analyse d'une procédure dans une grande administration a montré que toutes les demandes passaient par le bureau du chef, qui voulait de cette façon se tenir informé de ce qui était traité dans son service; malheureusement, comme le chef était souvent accaparé par des missions plus urgentes ou plus importantes, les dossiers en attente de traitement s'accumulaient sur son bureau, et après un temps plus ou moins long, lorsque le chef avait finalement décidé d'évacuer les affaires en attente, ils continuaient leur chemin à travers le service, sans avoir subi le moindre traitement dans le bureau du chef. A cause du désir de supervision du chef, le traitement des demandes était allongé de façon significative, sans pour autant en accroître la qualité. Il a fallu beaucoup de travail de persuasion pour convaincre le chef que le système de GED lui donnait à tout moment la possibilité de savoir qu'elles étaient les affaires en cours et où en était leur traitement et qu'il n'était donc pas nécessaire que chaque demande passe d'abord par son bureau.

La modélisation d'une procédure peut aussi en révéler toute la complexité et ce n'est que l'étalement du schéma complet, souvent impressionnant par sa taille, qui arrive à faire prendre conscience aux responsables administratifs qu'il est nécessaire de simplifier certaines choses. La complexité des procédures provient souvent du fait que tous les cas, des plus simples aux plus complexes, sont traités de la même façon, alors qu'on aurait intérêt à mettre en place des procédures séparées pour les cas courants ne posant pas le moindre problème, même à un agent peu expérimenté, et pour les cas plus délicats, qui nécessitent l'intervention d'un ou de plusieurs agents expérimentés et plus spécialisés.

Bien plus qu'un projet de nature technique, la mise en place de la GED se révèle être un projet de changement d'organisation et, en tant que tel, il sera confronté à toutes les résistances qu'on rencontre habituellement dans les entreprises en cours de réorganisation. Nous reviendrons plus en détail sur ces problèmes sous un point ultérieur.

L'art de la mise en place d'un système de GED consiste à améliorer les procédures tout en s'assurant l'adhésion des agents concernés. Ceci ne pourra se faire qu'en les impliquant étroitement dans le déroulement du projet.

Un autre risque organisationnel, c'est le changement de type " *big bang* ", en passant du jour au lendemain à une solution entièrement nouvelle. Il faudra au contraire arriver à planifier une mise en place progressive, en mettant d'abord en oeuvre des sous-ensembles de la solution globale prévue, afin de convaincre tous les acteurs que la solution fonctionne, et pour maîtriser progressivement les problèmes techniques inévitables de mise route. Ce sera aussi l'occasion d'impliquer davantage les agents concernés, en tenant compte de leurs suggestions d'amélioration et en adaptant même la solution globale si cela se révèle nécessaire.

4.3. Les aspects économiques

Pour justifier leurs choix, les décideurs recourent souvent à une analyse coûts/bénéfices, qui doit démontrer de façon quasi-scientifique l'opportunité de recourir à la solution proposée. Cette approche cache pourtant des risques non négligeables, car en essayant de " prouver " le gain économique de la solution envisagée, les décideurs sont souvent amenés à tricher ou du moins à négliger beaucoup d'aspects difficilement maîtrisables en début de projet. Il peut même arriver qu'une fois que les budgets prévus par l'étude coûts/bénéfices sont épuisés, le projet soit stoppé pour raison de non rentabilité économique.

Les décideurs doivent se rendre à l'évidence qu'il est pratiquement impossible de donner des prévisions budgétaires adéquates en début de projet et qu'il est tout aussi irréaliste de vouloir quantifier les bénéfices attendus par une solution GED.

Un projet GED résulte d'un choix stratégique, de la réflexion de l'administration sur sa position dans la société et sur son développement futur. Avant de pouvoir quantifier correctement le coût d'une solution technique déterminée, il faut savoir ce qu'on veut et cela nécessite une analyse préalable des procédures actuelles. La modélisation de ces procédures peut suggérer des améliorations significatives, même en ne réalisant pas en fin de compte la mise en oeuvre de la solution GED initialement prévue.

La difficulté de la quantification des coûts provient des nombreux facteurs qui interfèrent: personnels spécialisés à recruter, aménagements de bureaux supplémentaires à réaliser, modernisation du réseau téléinformatique en place, remplacement d'un certain nombre de stations de travail informatiques, mise en place de mesures de sécurité, non disponibilité temporaire d'agents accaparés par le projet, analyse des procédures et non prévisibilité des résultats de ces analyses, résistance de la part d'agents

concernés, adaptation d'un grand nombre de formulaires, sensibilisation du personnel et du public, évolution de la technologie en cours d'étude, évolution du marché, fiabilité du maître d'oeuvre et des conseillers en GED, etc.

La quantification des bénéfices attendus est tout à fait théorique, car une administration n'a pas pour mission de réaliser des bénéfices financiers; il sera dès lors très difficile de quantifier le service amélioré rendu à l'usager, l'impact d'une réduction des durées de traitement ou la diminution d'erreurs de traitement. On pourrait bien sûr estimer le gain apporté par la suppression de l'un ou de l'autre poste de personnel chargé du transport physique de documents; mais s'agit-il vraiment d'un gain ou plutôt d'une externalisation d'un coût qui se retrouvera sur un autre poste budgétaire de l'Etat?

Le projet GED devra se faire par étapes, en essayant de quantifier de façon aussi précise que possible le coût de l'étape en cours, tout en ayant une vue moins précise sur le coût des étapes suivantes, et ceci d'autant plus que l'étape est éloignée dans le temps. Il en résulte qu'un projet GED peut comporter une incertitude quant à l'impact financier global de l'opération; cette incertitude rend la décision délicate aux dirigeants de l'administration et ceci d'autant plus que les moyens financiers sont restreints.

4.4. Les problèmes de résistance du personnel

Un projet de GED est essentiellement un projet de changement des modes de travail, et en supprimant le cas échéant les documents papier, il engendre même un changement radical de la culture administrative. Il ne faut donc pas s'étonner si l'on rencontre des oppositions bien affirmées à ce type d'initiative.

Les opposants au projet auront des arguments solides, qui peuvent tout à fait se justifier.

Il y a tout d'abord ceux qui tiennent au support papier. Pour eux, le contact physique du papier, la possibilité de le prendre en main, de le lire en se déplaçant dans le bureau, de l'étaler horizontalement sur la table de travail, de l'annoter ou de le tamponner, constitue une habitude tellement naturelle, qu'ils ont de la peine à imaginer qu'ils devront à l'avenir recourir à un écran de visualisation pour réaliser de façon inconfortable ce qui était tellement simple auparavant. De plus le papier donne l'occasion de se rencontrer dans le bureau du chef, pour discuter ensemble d'un problème soulevé par le document en cours de traitement. D'un autre côté, l'accès des documents par écran aura comme conséquence un accroissement de l'isolement des agents administratifs, en faisant passer la plupart des communications humaines par des canaux techniques et indirects. La chaleur des relations humaines, issue du contact direct entre les intervenants, va probablement en souffrir, les chefs ayant moins l'occasion de rencontrer directement leurs collaborateurs, et connaître ainsi, non seulement leur travail au bureau, mais

aussi leurs préoccupations extra-professionnelles, qui peuvent parfois avoir une influence significative sur leur productivité au travail. A noter que des recherches scientifiques sont en cours pour concevoir des écrans du futur, qui pourraient fort bien ressembler à des feuilles de papier, mais les produits correspondants ne sont pas à attendre pour demain.

Il y a ensuite ceux qui ont des réticences à travailler avec des équipements informatiques. Certains agents n'ont même pas encore de station de travail informatisée dans leur bureau ou bien n'allument qu'occasionnellement leur ordinateur personnel. L'informatique n'était pas encore au programme d'études lorsqu'ils étaient à l'école et ils n'ont jamais vraiment réussi à en maîtriser l'utilisation. Pour eux, la suppression du papier les obligera à se lancer dans une entreprise qu'ils détestent et ils feront tout pour empêcher cette éventualité.

Il y a ceux qui n'aiment pas les écrans de visualisation, surtout lorsque ceux-ci sont de mauvaise qualité. Leur problème ne consiste pas nécessairement en une attitude anti-technologique, mais correspond plutôt à un problème physiologique. Avec l'âge, les possibilités d'accommodation de la vue sur l'écran diminuent et le travail à longueur de journée devant un tel écran peut devenir une véritable corvée, voire même devenir tout à fait impossible. Il en résulte qu'il n'est pas vraiment possible d'obliger tous les agents administratifs à travailler sur un équipement à écran de visualisation.[1)] Le décideur s'orientera plutôt vers une organisation où l'on aura conservé à tous les niveaux des emplois ne nécessitant pas un travail avec un équipement à écran de visualisation.

Les opposants décrits jusqu'à présent seront probablement des agents administratifs déjà plus âgés, ayant par conséquent une grande expérience administrative et probablement une position à haute responsabilité; il en résulte que ce sont aussi des personnes ayant une influence non négligeable dans l'administration et qui pourront tout à fait être à même de faire échouer un projet GED. Le décideur aura donc tout intérêt à avoir une attitude coopérative, en essayant de s'allier le support de ces agents-là.

La mise en place d'un système de gestion de dossiers et de flux de travaux appelle sur le plan d'autres catégories d'opposants.

---

1) Rappelons que l'administration doit de toute façon se conformer aux dispositions du règlement grand-ducal du 4 novembre 1994 concernant les prescriptions minimales de sécurité et de santé relatives au travail sur les équipements à écran de visualisation. [Mém. A 1994, n° 96, pp. 1853-1856], qui prévoient entre autres des examens ophtalmologiques réguliers des personnes concernées, des pauses ou des changements d'activité, ainsi que la consultation des représentants du personnel. Voir aussi le site web http://www.inrs.fr/ de l'Institut National de Recherche et de Sécurité français, qui met à disposition un dossier "Le travail sur écran".

Il y a ceux, et ils sont nombreux, qui s'opposent au changement des habitudes de travail. Pourquoi changer quelque chose qui a fourni ses preuves dans le passé? Des procédures remaniées peuvent avoir des conséquences pratiques importantes pour les personnes concernées: modification des relations de travail (p.ex. on n'a plus l'occasion de se rencontrer régulièrement), perte d'influence (certains renseignements, qui étaient gérés par un agent déterminé, sont à présent partagés entre tous les intervenants d'une procédure, d'où perte de pouvoir de l'agent), transparence des activités de chaque agent (d'autres ont la possibilité de voir de façon régulière les travaux réalisés par un agent déterminé).

Cette dernière crainte mobilise une autre catégorie d'opposants potentiels: les représentants du personnel (syndicalistes, délégation du personnel, comité mixte d'entreprise). En effet, un système de gestion de dossiers permet de savoir à la minute près (même à la seconde près) ce que fait chaque agent, combien de temps il met à traiter un dossier, comment il se situe par rapport à d'autres agents réalisant le même type de travail.[1)] Les représentants du personnel redoutent que cela ne puisse mener à l'établissement de normes pour le rythme de travail, en obligeant ceux qui travaillent plus lentement à se conformer au rythme des plus performants. Le décideur devra en tenir compte et évaluer sa capacité à trouver un accord raisonnable avec les représentants du personnel.

Les syndicalistes peuvent aussi être préoccupés par la suppression d'emplois, devenus superflus à cause de la disparition du papier; tous ceux qui étaient occupés à des travaux de photocopie, de classement, de transport de documents d'un bureau vers un autre, verront leur champ d'activité traditionnel se restreindre comme une peau de chagrin et sentiront leur emploi menacé. Souvent, il s'agit de personnes souffrant d'un handicap ou ayant un niveau de formation très réduit et il sera difficile de les recaser par après. Le décideur devra tenir compte de ce fait et trouver des occupations de rechange pour ces personnes ou bien trouver d'autres solutions au problème.

On peut constater que la mise en place d'un système GED constitue un projet délicat du point de vue du climat social dans l'administration. Le décideur a tout intérêt à pratiquer une politique de participation systématique de toutes les personnes concernées et à intégrer les représentants du personnel dès le départ dans la conception du projet. Un projet GED constitue aussi un processus d'apprentissage et de maturation de l'administration, et comme

---

1) Notons toutefois que la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (déjà citée) et notamment son article 11 (Traitement à des fins de surveillance sur le lieu du travail) impose à l'employeur des conditions extrêmement restrictives pour mettre en oeuvre de telles mesures: situations exceptionnelles, information du comité mixte d'entreprise et de la personne concernée. De plus l'article 14 (Autorisation préalable de la Commission nationale) soumet de telles mesures à l'autorisation préalable de la Commission nationale pour la protection des données.

tout apprentissage, la réussite dépend des efforts qui sont consentis pour le mener à bien. Le décideur commettrait une erreur en voulant forcer un calendrier de réalisation trop serré.

4.5. Les questions juridiques

La numérisation d'un document papier a pour objet d'en réaliser une copie fidèle dans l'ordinateur. Le document est représenté par des suites de chiffres binaires, des uns et des zéros, qu'on peut stocker sur un support informatique, et à partir desquels on peut reconstituer une image de l'original sur un écran de visualisation ou même produire une copie sur papier. Beaucoup de questions juridiques sont soulevées par ce procédé.

Ces questions ne se posent pas seulement pour la GED, mais sont soulevées chaque fois que le problème de place est résolu en remplaçant le papier par un support plus compact en espace de stockage. Elles se sont posées initialement lors de l'introduction par les instituts financiers de systèmes de microfilmage pour chèques, où les milliers de chèques traités par jour devaient être conservés uniquement sous forme de microfilm en détruisant l'original après un délai très court.

La question fondamentale à résoudre est: " *peut-on détruire les originaux, tout en conservant une valeur probante suffisante aux copies réalisées à partir de ces originaux?* ".

Des réponses de principe ont été fournies par le législateur en 1986[1)] et seront abordées de façon approfondie dans un autre article de ce fascicule.

Ces textes n'ont jamais été adaptés à l'évolution de la technologie, puisqu'on s'est contenté de les réinterpréter lors de l'introduction des techniques de stockage sur supports informatiques. Même la loi du 14 août 2000 relative au commerce électronique, qui a pourtant apporté des précisions importantes à la définition de la notion d'original, se réfère encore au textes de 1986 pour tout ce qui concerne la question de la valeur probante en cas de destruction de l'original.[2)]

En vue de conserver une valeur probante aux copies en cas de destruction de l'original, les soucis du législateur étaient de deux ordres:

a) comment garantir que la copie est vraiment fidèle et non falsifiée;

b) comment garantir que l'accessibilité de la copie soit au moins aussi longue que la durée de conservation légale requise.

---

1) Loi du 22 décembre 1986 sur la preuve des actes juridiques (Mém A 1986, n° 108, pp. 2745-2748) et règlement grand-ducal du 22 décembre 1986 pris en exécution des articles 1348 du code civil et 11 du code de commerce. (Mém A 1986, n° 108, pp. 2748-2749).

2) Voir les articles 12 et 13 de la loi du 14 août 2000 relative au commerce électronique (Mem A 2000, n° 96, pp. 2175-2188).

La première préoccupation est la plus délicate à satisfaire. Il faut garantir qu'il n'y a pas eu de dégradation ou de falsification lors de la transposition initiale sur le nouveau support. Il faut aussi garantir qu'il n'y a pas eu de possibilité par la suite de modifier la copie sur le nouveau support. Ce dernier point est résolu par l'exigence que le support de mémorisation doit être non réinscriptible, c'est-à-dire qu'une fois les données inscrites, on ne peut plus les modifier sans les détruire. L'autre point est résolu par l'exigence d'une procédure rigoureuse et systématique de saisie initiale, surveillée par une personne responsable et documentée par un protocole de saisie.

La deuxième préoccupation demande un support à durée de vie suffisamment longue, mais aussi le maintien en état de fonctionnement de tous les dispositifs techniques et logiciels nécessaires pour reconstituer l'image de l'original.

Ces exigences se rapportent au seul cas où les originaux ont été détruits au cours d'une procédure systématique. Aujourd'hui ce problème se pose un peu moins, car l'apport de la GED ne se limite pas à un gain de place d'archivage, mais présente de nombreux autres bénéfices, qui pourraient intéresser l'administration davantage que la destruction des originaux.

Si l'administration a décidé de conserver les originaux sous une forme moins coûteuse, elle n'a pas besoin de se préoccuper de toutes ces contraintes légales pour conserver la valeur probante; il suffira d'être à même de retrouver l'original en cas de besoin, ce qui peut se faire facilement si le lieu de stockage physique est consigné sous forme de descripteur avec la copie numérisée.

Si par contre l'administration procède à la destruction systématique des originaux papier, elle devra se conformer aux exigences des textes de 1986 et sera bien conseillée de mettre en place des procédures standardisées, qui règlent rigoureusement tous les aspects de l'archivage électronique, comme elles sont p.ex. prévues par la norme française NF Z42-013[1)], dont il sera question dans un autre article de ce fascicule.

Mais les documents papier numérisés ne constituent qu'un volet particulier des documents électroniques. De plus en plus, les décisions administratives sont conservées sous forme de fichiers électroniques (bulletins, extraits de compte, notifications de décisions et lettres diverses). Dans ce cas les textes de 1986 ne s'appliquent plus tels quels et il faudra se référer à la notion d'original, telle que définie dans la loi du 14 août 2000 relative au commerce électronique, qui fait elle aussi l'objet d'un article plus détaillé de ce fascicule. Ces mêmes dispositions s'appliquent à toutes les applications de *e-Government* où les usagers pourront communiquer avec l'administration sans l'existence

---

1) NF Z42-013: "Archivage électronique". Recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.

d'originaux en papier. Beaucoup de questions restent pourtant ouvertes dans ce domaine et il sera réservé aux juristes d'en mesurer toute l'étendue.

Le décideur aura donc à faire un choix fondamental: va-t-on, oui ou non, détruire les originaux des documents gérés par GED? Par le passé, certains instituts financiers ont pris l'option de détruire les originaux et d'assumer le risque d'une perte de valeur probante, si ce risque était considéré comme minime par rapport au gain financier dû à une GED simplifiée.

***

Nous venons de passer en revue les nombreux risques auxquels est confronté un projet de GED et le décideur en tiendra compte dans la mesure du possible. Mais il reste un dernier risque à présenter, le plus délicat de tous, car il concerne directement les décideurs et responsables de l'administration eux-mêmes:

Pour que le projet GED ait la moindre chance de réussite, il faudra que les dirigeants de l'administration s'impliquent réellement dans le projet; il ne suffit pas de prendre une décision. Par la suite il faudra aussi en assumer les conséquences, en garantissant un soutien sans faille à l'équipe projet et en signalant clairement à l'ensemble des agents administratifs concernés que la direction tient au projet et sera elle aussi disposée à utiliser les nouveaux outils, une fois qu'ils seront introduits. Si les opposants au projet ont l'impression que la direction ne soutient pas vraiment le projet, surtout dans ses phases les plus critiques, alors ils réussiront facilement à faire échouer l'ensemble du projet. D'un autre côté, comme il s'agit d'un projet de longue haleine, il y aura toujours dans l'administration des problèmes plus urgents à traiter avec effet immédiat; si la direction change souvent les priorités, en retirant momentanément ou définitivement des ressources au projet, celui-ci risque de mourir d'asphyxie.

Les décideurs analyseront donc s'ils ont la force et la persévérance pour maîtriser ce risque critique.

CONCLUSIONS

Dans cet article nous avons éclairé différentes facettes du processus de décision en vue de l'introduction de la gestion électronique des documents dans l'administration avec le but de montrer que cette décision était complexe et d'ordre stratégique.

Une décision complexe?

La décision est réellement complexe, car la nature de la solution envisagée est complexe: l'intégration d'un grand nombre de composants en provenance d'une variété de fournisseurs en fait un projet technologiquement complexe; le fait qu'il s'agit d'un projet de changement de la façon de travailler, voire même de la culture administrative, a comme conséquence une grande complexité dans la gestion des relations humaines et du changement.

Les projets complexes courent le risque d'échapper au contrôle des décideurs, et une évaluation correcte des risques potentiels, ainsi qu'une gestion de projet professionnelle s'avère indispensable. Le suivi régulier et l'adaptation flexible du projet aux circonstances permet d'éviter beaucoup d'écueils.

Une décision stratégique?

L'article a montré que finalement l'objet de la décision n'est pas tellement la mise en oeuvre d'une technologie nouvelle pour venir à bout des montagnes de papier dans l'administration, mais la question de savoir comment l'administration va se positionner dans la société de l'information, dans laquelle les usagers de l'administration demandent des relations conviviales par l'intermédiaire de canaux de communication électroniques, attentes stimulées par les instances politiques nationales et communautaires.

En reconsidérant la décision sous cet angle de vue et en appliquant une échelle de temps suffisamment large, on se rend compte que la mise en oeuvre progressive de solutions de type *e-Government* va réduire dans la même mesure le volume de papier à traiter et que le problème du papier va probablement se résoudre de soi-même, en se réduisant finalement aux interactions avec les usagers, qui, pour une raison ou une autre, n'ont pas accès aux canaux de communication modernes.[1)]

La question stratégique à résoudre, c'est de savoir s'il vaut mieux investir massivement pour numériser des documents en papier, dont l'importance va diminuer peu à peu, ou s'il vaut mieux passer immédiatement à des solutions encore plus modernes, en mettant en place des systèmes interactifs, qui ont pour but de supprimer complètement le papier et de transférer la charge de la saisie des données de l'administration vers l'usager.

---

1) L'article 18 (3) de la loi du 14 août 2000 relative au commerce électronique précise que "Nul ne peut être contraint de signer électroniquement"*; il en résulte que la signature manuelle sur papier pourra toujours être utilisée par l'usager dans les années à venir et le support papier ne pourra donc pas disparaître complètement. L'administration devra bien conserver aussi à l'avenir une chaîne de traitement de documents papier, même si le volume éventuellement faible ne justifie pas des solutions technologiques coûteuses pour ces traitements résiduels.*

Il est vrai qu'une solution GED n'empêche pas un passage vers des systèmes complètement interactifs, qu'elle en prépare même le terrain. Mais il faut bien se rendre à l'évidence que l'effet bénéfique ne provient pas du fait que les documents sont numérisés dès l'entrée dans l'administration, mais plutôt des systèmes de traitement d'affaires assistés par ordinateur qui leur sont associés. On peut donc tout à fait aborder la GED en se concentrant primairement sur des documents complètement électroniques, pour examiner ensuite seulement dans quelle mesure les solutions ainsi développées pourraient être complétées utilement par un système de transformation des documents papier vers une forme électronique.

Le présent article n'a pas étudié à fond les solutions complètement électroniques de type *e-Government*, pour la simple raison que ceux qui parlent de gestion électronique de documents ne l'envisagent pas sous cet angle de vue, du moins pas en ce moment. Pour ces approches nouvelles il y a aussi beaucoup de questions de nature technique, organisationnelle, économique, sociale et juridique à discuter et il serait certainement intéressant d'organiser dans les années futures un autre séminaire " aloss " complètement consacré à ce sujet.

Environnement juridique de l'archivage et de la gestion électronique de documents

Raphaël VUITTON

Chercheur,
Laboratoire de Droit Economique
Centre de Recherche Public Gabriel Lippmann

" *L'administration électronique ne saurait être efficace si elle est amnésique* "

Pierre TRUCHE

CHAPITRE I. - PROPOS INTRODUCTIFS

L'activité administrative de l'Etat et des organismes publics se déploie dans le temps et se matérialise par des flux documentaires constants. Loin d'être totalement libre, cette activité est encadrée par des contraintes juridiques qui imposent un formalisme dans l'édiction d'actes normatifs ou décisionnels: exigence de visas, de signature… D'autres contraintes sont quant à elles relatives aux échanges d'informations entre l'administration et les administrés[1)] et visent à assurer le respect de délais ou à la prise de connaissance de l'acte par son destinataire. Le principe de bonne administration gouverne ces exigences et, afin d'assurer l'effectivité de cet encadrement juridique, une double obligation de conservation pèse sur l'administration.

Conserver une trace de tous ces flux de documents est une tache essentielle afin de prouver l'échange d'information. Mais il importe aussi d'assurer la pérennité et l'intégrité d'un document: il s'agit alors de d'assurer la conservation du document dans le temps. Ces objectifs doivent être remplis indépendamment du support utilisé par le document ou le mode de transmission de celui-ci.

---

1) P. TRUCHE, J-P. FAUGERE, P. FLICHY, Administration électronique et protection des données personnelles: Livre blanc, Paris, février 2002, p. 45.

*Section 1 - **La problématique du support informatique***

La problématique relative à cette double obligation de conservation doit être envisagée sous un angle nouveau dès lors que, en raison de l'avènement de la société de l'information, de nombreux organismes publics, entreprises ou simples citoyens utilisent les systèmes informatiques afin de produire, diffuser ou conserver des documents électroniques. Ce caractère électronique du support et du flux de l'information bouleverse la conception traditionnelle prévalant en matière d'archivage.

Le support papier est considéré comme étant relativement intangible; sa pérennité est assurée de manière aisée en dehors d'éventuels accidents ou incidents pouvant le cas échéant altérer l'intégrité du texte inscrit à sa surface. De surcroît, aucun équipement spécifique n'est nécessaire pour rendre intelligible le document sur support papier. Or, ces prémisses ne sont plus valables dans le monde électronique.

La conservation dans le long terme de documents établis et stockés sur support informatique ne peut être assurée que quelques dizaines d'années au maximum. Nous sommes donc loin des deux millénaires séparant l'écriture, par la communauté de Qumrân, des Manuscrits de la mère morte de leur découverte en 1947[1)].

Au-delà de la problématique posée par la durée de conservation et de la vulnérabilité aux agressions du temps, le second problème posé par l'archivage des documents électroniques réside dans le fait que, contrairement au format papier, l'information stockée électroniquement nécessite un équipement spécifique pour la rendre intelligible à tout moment. Cette retranscription doit bien entendu être fidèle et être effectuée en toute intégrité vis-à-vis de l'état initial du document. Toutefois, les évolutions technologiques induisent un renouvellement permanent et particulièrement rapide des ressources matérielles. Sauf à vouloir constituer un musée de l'informatique, il est quasiment impossible de pouvoir s'assurer que la technique permettant de rendre intelligible une information dans 10 ou 20 ans assurera la retranscription fidèle du document initial.

Liée à ce problème de restitution au-delà des âges, la question de l'authenticité et l'intégrité du document archivé, quel que soit son mode de conservation, se pose. En effet, garantir l'authenticité et l'intégrité d'une information n'est pas chose aisée. Dans l'environnement électronique, il est facile - même pour un *hacker* novice - d'accéder et de modifier les informations contenues dans un fichier. Juridiquement, cette éventuelle dénaturation induira des conséquences notoires et altérera, par exemple, la valeur probante d'un document stocké électroniquement.

---

1) A. PAUL, Les manuscrits de la mer Morte, Paris, Bayard, 2000.

Malgré ces inconvénients, l'archivage électronique et la gestion électronique de documents sont une réponse à la prolifération du support papier dans l'activité administrative. Ils permettent de ne plus stocker dans des volumes de plus en plus importants des documents originaux, et autorisent désormais les administrations à conserver et diffuser le fruit de leur activité sous des formes plus maniables pour un coût assez limité.

En outre, la gestion électronique de documents permet un traitement plus facile et plus rapide des dossiers. Il ne s'agit plus ici d'assurer la mémoire d'une information et de son flux entre l'administration et l'administré mais d'assurer, à l'intérieur de l'administration, le traitement rationalisé de l'activité administrative par le biais d'un instrument de gestion électronique. Le préalable nécessaire à une telle organisation des services consiste en la définition d'une politique de gestion électronique des documents et des archives qui exprime, *mutatis mutandis*, le pouvoir de l'administration d'organisation de ses services dans le cadre de la société de l'information.

De ces remarques introductives ressort la nécessité pour la gestion et l'archivage électronique de s'inscrire dans un cadre législatif, réglementaire et organisationnel assurant la conservation de la valeur juridique et probatoire d'un document. Les critères de fidélité, de pérennité, d'identification, d'authenticité et d'intégrité sont primordiaux mais il convient aussi de ne pas négliger les exigences tenant à la lisibilité, l'intelligibilité et la traçabilité des documents électroniques.

Section 2 - ***Les dimensions de la gestion électronique de documents appliquées aux organismes de sécurité sociale***

Il est possible à ce stade de distinguer trois axes d'analyses: ils correspondent respectivement à la conservation dans le temps d'un document[1)]; à la gestion en interne des flux de documents et enfin à la gestion des flux de documents entre administration et administrés[2)]. C'est sur ces trois strates que devront se greffer les analyses juridiques qui affecteront spécifiquement l'activité des organismes de sécurité sociale. En effet, de par leur activité, ils doivent faire face aux trois dimensions précitées.

La dimension " archivage " est induite par la nécessité d'assurer la conservation de documents - voir d'un dossier[3)] - dans le temps afin, par exemple, de pouvoir en assurer la production en justice en cas de contestation devant le conseil arbitral de la sécurité sociale d'une décision d'une caisse.

---

1) Il s'agit de l'archivage en tant que tel.

2) Ces deux derniers éléments constituent la GED dans sa composante interne et externe.

3) Voir à cet égard l'initiative française de " Dossier médical partagé ", ainsi que le rapport de M. Fieschi remis au Ministre de la Santé, " Les données du patient partagées: la culture du partage et de la qualité des informations, pour améliorer la qualité des soins ", le 24 juin 2003.

Au-delà de cet aspect contentieux, il faut garder à l'esprit que règlement grand-ducal du 8 juin 1979 relatif à la procédure à suivre par les administrations relevant de l'Etat et des communes[1)] prévoit, en son article 11, que tout administré a droit à la communication intégrale du dossier relatif à sa situation administrative, chaque fois que celle-ci est atteinte, ou susceptible de l'être, par une décision administrative prise ou en voie de l'être. Il peut demander, à cette occasion, le retrait de son dossier de toute pièce étrangère à l'objet du dossier, si elle est de nature à lui causer un préjudice. Au regard de cette obligation, il est nécessaire d'assurer un archivage cohérent des dossiers afin d'en permettre la consultation.

La seconde dimension de la gestion électronique de documents - la dimension interne - se manifeste lors de l'instruction d'un dossier. Par exemple, dans le cadre d'un accident du travail, le dossier doit être communiqué à différents intervenants, chacun acteur de la procédure à un stade différent. La gestion électronique de documents en interne, facilitera la consultation, la communication et l'instruction des ces dossiers.

Enfin, dans sa composante externe, la gestion électronique de documents a la potentialité d'améliorer les relations entre les organismes de sécurité sociale et les assurés. Quoi de plus simple désormais que de remplir " en ligne " un dossier de demande d'allocation familiale et de se voir communiquer, toujours par des voies électroniques, la décision afférente à cette demande? Bien entendu, cet aspect externe peut se coupler à l'aspect interne de la gestion électronique de documents pour le traitement du dossier.

En fonction de leurs besoins propres et de leur politique interne, les organismes pourront le cas échéant mettre en œuvre l'ensemble de ces aspects ou insister plus spécifiquement sur l'un ou l'autre. Ainsi, si le Centre commun de la Sécurité social a mis l'accent sur la GED dans sa composante interne et sur l'archivage de ses documents, les modalités de mise en œuvre pourront toutefois varier d'une entité à l'autre.

Ainsi, le département " Affiliation " du Centre Commun de la Sécurité Sociale scanne ses documents *après* traitement et le document papier est conservé et classé non par dossier mais par un numéro correspondant à son numéro de scanning. Les enregistrements électroniques réalisés à partir des documents papiers sont stockés sur des disques optiques numériques (CD-ROM) non-réinscriptibles. La dimension archivage est donc privilégiée.

A l'inverse, en matière d'assurance contre les Accidents, les documents papiers sont scannés avant traitement, dès leur arrivée. Le document papier est conservé et classé par dossier. L'enregistrement informatique réalisé à partir du document papier est stocké sur un CD-ROM non-réinscriptible placé dans un " juke-box " afin de pouvoir être accessible par les personnes

1) Mémorial A 1979, p. 1096.

chargées de son traitement, depuis leur poste de travail. Lors du traitement, le document peut faire l'objet d'annotations, qui seront conservées dans un index qui accompagne le document en question et rappelle les traitements dont il a fait l'objet. Ici, la dimension interne de la gestion électronique de documents est clairement privilégiée et est accompagnée par une politique d'archivage spécifique.

Ces brefs propos introductifs en sont la preuve: les organismes de sécurité sociale se présentent comme des acteurs naturels de la dématérialisation des échanges et du stockage de documents. Ils occupent d'ailleurs une place de choix dans le cadre du programme " *e-luxembourg* " et sont les fers de lance de multiples projets relatifs à la gestion électronique des documents.

Depuis le 31 juillet 1901, date de la création de la sécurité sociale au Luxembourg, les principes directeurs de l'assurance sociale - la solidarité et le dialogue entre les partenaires sociaux- ont été conservés. Toutefois, de nouveaux défis se font jour au regard de l'accroissement du volume de travail assumé par les organismes de sécurité sociale. Le passage à la gestion électronique des dossiers participe à traiter plus rapidement un nombre toujours croissant de demandes des assurés sociaux. Elle facilite aussi la consultation des dossiers sur écran, diminue le temps de traitement des multiples pièces et, *in fine*, améliore les relations entre les organismes et les assurés.

La gestion électronique des dossiers des assurés est désormais une activité quotidienne. Si les aspects pratiques - et les éventuels *bugs* qui peuvent altérer une telle politique de gestion -sont familiers au personnel des organismes de sécurité sociale, les implications juridiques le sont certainement moins. C'est la raison pour laquelle je propose de découvrir de manière synthétique l'environnement juridique de l'archivage et de la gestion électronique de documents. Les aspects internationaux (Chapitre II) précéderont et éclaireront de brèves considérations relatives à la situation du Grand-duché[1)] (Chapitre III).

---

1) Les aspects relatifs au droit luxembourgeois de l'archivage électronique seront développés dans la contribution de M. Corentin POULLET, " L'archivage électronique sécurisée ".

CHAPITRE II. -L'ENVIRONNEMENT JURIDIQUE SUPRANATIONAL DE LA GESTION ÉLECTRONIQUE DE DOCUMENTS ET DE L'ARCHIVAGE ÉLECTRONIQUE

Les sources internationales des normes relatives à la gestion électronique de documents ou à l'archivage électronique se trouvent soit dans des textes adoptés par des institutions à vocation universelle, telles que la CNUDCI ou l'UNESCO (section 1) soit à vocation régionale, telle que l'Union européenne (section 2). Les efforts internationaux de normalisation participent aussi à la définition de références pour les acteurs de cette gestion électronique (section 3).

*Section 1 - **L'environnement juridique international***

En ce qui concerne les organisations à vocation universelle, la réglementation des questions relatives à l'archivage et à la gestion électronique de documents est principalement issue de recommandations ou lois-type élaborées par la Commission des Nations unies pour le droit commercial international (CNUDCI).

A. La recommandation de la CNUDCI relative à la valeur juridique des enregistrements informatiques

Historiquement, le premier texte adopté par la CNUDCI concernant la problématique qui nous intéresse aujourd'hui est la recommandation relative à la valeur juridique des enregistrements informatiques, datant de 1985[1)].

Dans ce texte, la CNUDCI recommande aux gouvernements, sans toutefois obliger ceux-ci juridiquement, de réexaminer les règles juridiques touchant l'utilisation des enregistrements informatiques comme moyens de preuve en justice afin d'éliminer les obstacles superflus à leur recevabilité. Elle les incite aussi à s'assurer que ces règles sont compatibles avec les progrès techniques et vise à donner aux tribunaux les moyens leur permettant d'apprécier la fiabilité des données contenues dans ces enregistrements.

La recommandation appelle en outre de ses vœux le réexamen des règles juridiques en vertu desquelles certaines transactions commerciales ou certains documents ayant trait au commerce doivent être établis sous forme écrite et ce, que cette forme écrite soit ou non une condition requise pour que la transaction ou le document soit valide ou s'impose aux parties. Ce réexamen vise notamment l'élimination de certaines règles juridiques nationales afin de faire en sorte que la transaction ou le document puisse être enregistré et transmis sur un support informatique.

Dans le même esprit et se positionnant en précurseur de la signature électronique, la CNUDCI demande de réexaminer l'exigence légale d'une

1) Recommandation relative à la valeur juridique des enregistrements informatiques (1985), http://www.uncitral.org/french/texts/electcom/computerrecords-f.htm

signature manuscrite ou de toute autre méthode d'authentification sur papier pour les documents commerciaux afin de permettre l'utilisation de moyens électroniques d'authentification.

Enfin, signalons que dès 1985, la CNUDCI incite les Etats à réexaminer les règles juridiques selon lesquelles les documents à soumettre à l'administration doivent être présentés par écrit et doivent porter une signature manuscrite. La recommandation vise ainsi à autoriser la présentation de ces documents sur support informatique à des services administratifs qui doivent, par conséquent, acquérir les équipements nécessaires et mettre en place des procédures adéquates.

A cet égard, la problématique du formalisme en matière de requêtes introductives d'instance, devant les juridictions chargées de connaître des litiges en matière de sécurité sociale est d'une acuité toute particulière.

Il ressort de l'article 1, alinéa 2 du règlement grand-ducal déterminant la procédure à suivre devant le conseil arbitral et le conseil supérieur des assurances sociales[1)] que la requête introductive d'instance devant le conseil arbitral des assurances sociales doit être " signée " par le demandeur ou son représentant légal ou son mandataire. Il est de jurisprudence constante que la signature de la requête constitue une formalité substantielle qui est de l'essence de l'acte en question, et est indispensable pour son existence. Une requête non signée doit donc être déclarée inexistante et non susceptible de saisir le conseil arbitral d'un litige pour cause d'inobservation d'une formalité substantielle[2)].

Or, si la signature de l'auteur du recours est obligatoire, c'est parce qu'elle garantit l'authenticité du recours en ce qu'elle permet de contrôler si l'acte déposé dans le délai émane bien du requérant qui, par sa signature, se trouve engagé et qui par là oblige le juge à statuer sur la demande dont il se trouve saisi. Partant, le dépôt d'une télécopie non signée ne constitue dès lors pas l'acte de procédure prévu par l'article 1er du règlement précité et se trouve pour cela dénoué de tout effet[3)].

Mais quelle doit être cette signature? La recommandation de la CNUDCI semblait déjà en 1985 inciter les Etats à supprimer l'exigence de la seule signature manuscrite et admettre ainsi la signature électronique. La loi du 14 août 2000 relative au commerce électronique va dans ce sens et élabore la

---

1) *Règlement grand-ducal du 24 décembre 1993 déterminant en application de l'article 294 du code des assurances sociales la procédure à suivre devant le conseil arbitral et le conseil supérieur des assurances sociales, ainsi que les délais et frais de justice. Mémorial A 1993, p. 2320.*

2) *C.A.A.S. du 21.07.2003, Aff. GALLETTI c/CPEP, No. du reg.: E 47/01.*

3) *C.S.A.S. 20 novembre 1996, Aff. WALLENDORFF A. C/AAI, No du reg: GE 21/96 No: 198/96. Il en va de même pour le dépôt d'une photocopie non signée en original d'une requête: C.A.A.S. du 07.07.2003, Aff. BOUCHE c/CPEP, No. du reg.: E 19/03.*

reconnaissance des signatures électroniques, sous réserve de certaines conditions.

Le conseil supérieur des assurances sociales (CSAS) a récemment considéré que ces conditions sont remplies par l'apposition de l'image scannée d'une signature manuscrite sur la requête introductive. En l'espèce, cette recevabilité est subordonnée au fait que le requérant a créé sur l'ordinateur réservé à son usage exclusif, dont l'accès était protégé par un mot de passe connu de lui seul, une signature (qualifiée d'électronique par le CSAS) qu'il apposait depuis lors sur tous les papiers rédigés par lui et dont les autres employés de la société n'avaient pas la possibilité théorique de s'emparer.

En outre, le CSAS considère que la signature scannée du requérant ne lui est pas opposée par un autre consommateur ou utilisateur d'Internet afin de voir reconnaître des effets juridiques à la signature litigieuse. Le requérant est donc seul concerné par son litige l'opposant à la Caisse de pension des employés privés. Le CSAS estime suite à ces constats que la signature en question répond aux exigences de l'article 1322-1 du code civil[1)].

Cette affaire est juridiquement critiquable[2)] mais permet toutefois d'illustrer les enjeux soulevés par la recommandation de la CNUDCI de 1985 et notamment sur la levée des obstacles liés au formalisme dans le cadre des relations avec l'Etat et spécifiquement les organismes de sécurité sociale. D'ailleurs, prenant toute la mesure de l'importance de ces enjeux de la recommandation, l'exécutif luxembourgeois est intervenu et a adopté le règlement grand-ducal du 22 décembre 1986 pris en exécution des articles 1348 du code civil et 11 du code de commerce[3)] dont il ne fait guère de doutes qu'il est directement inspiré de cette recommandation.

Toutefois, plus encore aura été déterminante, en droit luxembourgeois, l'influence de la loi-type sur le commerce électronique.

B. La loi-type de la CNUDCI sur le commerce électronique

Poursuivant ses efforts afin d'éliminer les obstacles juridiques au commerce international, la CNUDCI a adopté en 1996 une loi type sur le commerce électronique[4)]. Malgré son intitulé, cette loi type n'a pas uniquement pour objet de poser des règles applicables au commerce électronique et au flux d'informations qu'il génère. Elle vise également à traiter de l'archivage de l'information sous forme de messages de données[5)] qui n'ont pas

---

1) C.S.A.S. du 08.12.2003, Aff. BOUCHE c/ CPEP, No. du reg.: E 2003/0108 No.: 2003/0198.

2) Voir la présentation y relative de Melle Maryline Durin dans le présent Bulletin.

3) Mémorial A 1986, p. 2748. Voir infra la présentation de ce texte.

4) Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996, http://www.uncitral.org/french/texts/electcom/ml-ecomm-f.htm

5) Il s'agit de documents électroniques.

uniquement vocation à être communiqués[1)] mais aussi, plus simplement, conservés et archivés.

De telles dispositions se retrouvent spécifiquement à l'article 10 de la loi type qui énonce un ensemble de nouvelles règles relatives aux exigences actuelles concernant l'archivage de l'information (p. ex. pour la comptabilité ou les impôts) qui pourrait constituer des obstacles au développement du commerce.

Selon cet article, intitulé " *Conservation des messages de données* ", lorsqu'une règle de droit exige que certains documents, enregistrements ou informations soient conservés, cette exigence est satisfaite si ce sont des messages de données qui sont conservés, sous réserve que l'information que contient le message de données soit accessible pour être consultée ultérieurement mais aussi que le message de données soit conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues.

Enfin, la loi-type impose que les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception soient conservées[2)].

La loi type énonce donc les conditions dans lesquelles la conservation des messages de données doit être menée, afin notamment que les messages de données conservent leur éventuelle valeur juridique. A cet effet, la loi-type envisage le recours à des tiers archiveurs[3)]. La conservation d'informations peut être en effet assurée avec qualité par un tiers de confiance, spécialisé dans ce domaine et qui possède les installations techniques ainsi que le savoir faire requis.

Mettant l'accent sur la méthode dites des " *équivalents fonctionnels* " et l'appliquant aux documents écrits sous forme électronique ainsi qu'aux signatures électroniques, la loi type de 1996 permet d'assurer la conservation des messages de données d'une manière fiable afin que ceux-ci conservent toute leur valeur juridique.

---

1) Voir Guide pour l'incorporation de la loi type de la CNUDCI sur le commerce électronique, 1996, sp. note 13.

2) Seulement si de telles données existent.

3) Voir article 10, paragraphe 3.

C. La loi-type de la CNUDCI sur les signatures électroniques

En 2001, la CNUDCI a parachevé son oeuvre d'harmonisation par l'adoption de la loi type sur les signatures électroniques[1)]. En effet, si la loi type sur le commerce électronique est utile en ce qu'elle rend possible ou facilite le recours au commerce électronique, la CNUDCI a estimé que la sécurité juridique de ce commerce se trouverait renforcée par l'harmonisation des règles applicables à la reconnaissance légale des signatures électroniques[2)].

D. L'UNESCO et l'archivage numérique

Indépendamment de la CNUDCI, d'autres textes ont été adoptés par des instances internationales, et notamment l'UNESCO.

Ainsi, le Conseil international des archives[3)] - organisation dépendant de l'UNESCO- a élaboré un Guide pour la gestion archivistique des documents électroniques[4)].

D'autres textes ont aussi été élaborés sous les auspices de l'UNESCO et du Conseil international des archives[5)]. Ces deux organisations coopèrent notamment afin de fournir des solutions aux problèmes posés par les archives électroniques et ce, spécifiquement dans leur dimension juridique. Divers projets et rapports, dont certains portent sur l'authentification des archives électroniques des administrations[6)] ont été rendus et mis en œuvre.

Parallèlement, l'UNESCO élabore une Charte internationale sur la conservation du patrimoine numérique, les données informatives et les oeuvres produites sous forme numérique uniquement. Conformément à la résolution 31 C/34 de la Conférence générale de 2001[7)], un rapport sur la conservation du patrimoine numérique, accompagné d'un projet de Charte ont été présentés à la Conférence générale[8)] en 2003.

---

1) *http://www.uncitral.org/french/texts/electcom/ml-elecsign.pdf*

2) *Pour une présentation exhaustive de la signature électronique et des textes applicables, il convient de se référer à la contribution de Melle Maryline DURIN au présent Bulletin.*

3) *www.unesco.org/webworld/ica_sio*

4) *Conseil international des Archives, Comité sur les documents électroniques, Guide pour la gestion archivistique des documents électroniques, ICA Study 8, 1997. Voir aussi: K. GAVREL, Conceptual Problems Posed by Electronic Records: A RAMP Study, PGI-90/WS/12, Paris, UNESCO, 1990 et L. AUER, Les Contentieux archivistiques, analyse d'une enquête internationale: une étude RAMP, CII.98/WS/9, Paris, UNESCO, 1998. Textes et- rapports disponibles à partir de: http://www.unesco.org/webworld/portal_archives/ramp_studies_list.html*

5) *http://www.ica.org*

6) *L. MILLAR, Authenticity of Electronic Records: A Report Prepared for UNESCO and the International Council on Archives, ICA Study 13-2, 2004.*

7) *Voir Actes de la Conférence générale, 31ème session, vol. 1, Paris, 2001.*

8) *http://unesdoc.unesco.org/images/0013/001311/131178f.pdf*

Ce texte consiste en une déclaration de principes axée sur les questions de sensibilisation et de politique d'archivage. Les questions d'ordre technique sont traitées dans les Principes directeurs pour la préservation du patrimoine numérique de la Charte. Celle-ci devrait en principe aider les Etats à définir leurs politiques nationales d'archivage numérique en leur inspirant des mesures répondant à l'intérêt général pour assurer la préservation du patrimoine numérique et l'accès à ce patrimoine.

Section 2 - ***L'environnement juridique communautaire***

Au niveau communautaire, rares sont les dispositions concernant la gestion électronique de documents. Il faut prendre conscience comme prémisse à toute analyse que cette matière ne semble pas *a priori* faire partie du champ de compétence de la Communauté européenne.

A. La directive relative au cadre communautaire pour les signatures électroniques

Toutefois, considérant que les communications et le commerce électroniques nécessitent des signatures électroniques et des services permettant d'authentifier les données, la Commission a proposé l'adoption d'une directive relative aux signatures électronique.

Cette directive, adoptée en 1999, permet d'éviter que des divergences concernant la reconnaissance juridique des signatures électroniques et à l'accréditation des " *prestataires de service de certification* " ne constituent un obstacle à l'utilisation des communications électroniques et au commerce électronique[1)]. Les signatures électroniques permettent au destinataire de données transmises électroniquement de vérifier l'origine de ces données et de vérifier qu'elles sont complètes et non viciées. La directive établit les critères de la reconnaissance juridique des signatures électroniques, en se concentrant sur les services de certification.

Elle énonce ainsi les obligations pesant sur les prestataires de services de certification afin d'assurer la reconnaissance transfrontière des signatures et des certificats dans la Communauté européenne. Elle traite aussi des règles de responsabilité contribuant à assurer la création de la confiance, tant en ce qui concerne les consommateurs qui se fondent sur les certificats que pour les prestataires de services. La directive met aussi en œuvre des mécanismes de reconnaissance transfrontalière des signatures et des certificats avec les pays tiers[2)].

---

1) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JOCE L, n° 13, du 19 janvier 2001, p. 12.

2) Ces dispositions feront l'objet de développements dans le cadre de la contribution de Marilyne DURIN.

Sans vouloir empiéter sur la présentation dédiée à la signature électronique, il suffit de signaler à ce stade que ce procédé est un outil d'identification et d'authentification des acteurs du processus de gestion électronique de documents. Cette technique permet aussi de s'assurer de l'intégrité d'un document archivé: elle s'avère donc essentielle pour les organismes de sécurité sociale.

B. Les conclusions concernant une coopération accrue dans le domaine des archives

Toujours à l'échelon européen, il convient de citer les conclusions du Conseil du 17 juin 1994 concernant une coopération accrue dans le domaine des archives[1)]. Ces conclusions ont été adoptées sur la base de l'ex-article 128 CE (depuis devenu l'article 151 CE) en considérant notamment que les archives constituent une partie significative du patrimoine culturel européen. Le Conseil a ainsi estimé que l'exploitation des archives peut contribuer à d'améliorer la connaissance de la culture et de l'histoire des peuples européens.

Dans ce texte, dont il convient de préciser qu'il est peu (ou pas) contraignant juridiquement, le Conseil invite la Commission à étudier l'organisation d'un forum multidisciplinaire relatif aux problèmes de gestion, de stockage de conservation et de récupération des données lisibles par machine.

Le Conseil invite à participer à ce forum les administrations publiques, les services nationaux d'archives ainsi que les représentants de l'industrie et de la recherche. Le Conseil marque enfin son intérêt pour la publication d'informations sur le contenu des archives, notamment par voie électronique.

C. Les travaux du " DLM Forum "

Sur la base de ces conclusions a été crée le DLM Forum[2)] qui s'est réuni en 1996, 1999 et pour la dernière fois en 2002.

Parmi les résultats obtenus par cette instance, on doit noter le souhait de développer un modèle de référence de gestion des documents et des archives électroniques. Lors de sa cession de 1999, le DLM Forum a ainsi souhaité que ce modèle tienne " *compte du continuum des documents et archives, depuis leur réception de l'extérieur ou leur création interne, leur gestion courante jusqu'à leur archivage et accessibilité* " et notamment, " *des principaux critères pour les documents et archives électroniques spécifiques aux administrations publiques et aux archives. Ces critères concernent la transparence et l'accessibilité de l'information électronique, les possibilités de conservation à court et à long terme de documents authentiques, des*

---

1) 94/C 235/03.

2) DLM est l'acronyme de " Données Lisible par machine ".

standards et spécifications ouverts et des lignes directrices interdisciplinaires des bonnes pratiques".

Cet objectif a reçu une concrétisation par la création du " *Model Requirements for the Management of Electronic Records* " (MOREQ)[1] qui est un modèle indiquant la manière dont les classifications de dossiers, les disques, les documents, les programmes de conservation, etc. peuvent être organisées et interconnectées.

En outre, aux fins d'associer les opérateurs économiques intéressés, le DLM Forum a incité la Commission européenne et les Etats membres en 1999[2] à mettre à jour et à transmettre un " Message DLM " à l'industrie des technologies de l'information et de la communication (TIC)[3].

Par ce message, le DLM Forum a demandé à l'industrie de fournir des méthodes simples et sécurisées pour le transfert d'informations, sans perte de contenu ou de présentation entre les différentes versions de logiciels ou entre des logiciels similaires produits par le même fabricant; des standards ouverts d'échange entre les différents logiciels; et des standards et des lignes directrices interdisciplinaires pour la conservation et l'accessibilité à court et à long terme.

Même si lors de sa réunion de 2002, le DLM Forum a exposé un certain nombre de bonnes pratiques actuellement employées en Europe dans le domaine de l'archivage, il ne fait aucun doute que la législation communautaire concernant la gestion électronique de documents ou l'archivage électronique ainsi que les initiatives y relatives sont pour l'heure à un stade embryonnaire.

D. Le livre vert sur l'information émanant du secteur public dans la société de l'information

Pourtant, le livre vert de 1998 sur l'information émanant du secteur public dans la société de l'information[4], insiste sur le rôle de l'utilisation des NTIC[5] qui, selon la Commission, facilite non seulement les opérations internes des administrations publiques mais renforce également la communication entre différentes administrations ainsi que l'interaction avec les citoyens et les entreprises.

---

1) *Projet financé dans le cadre du programme IDA2 de la Commission européenne, http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=2303&parent=chapter&preChapterID=0-17*

2) *Voir second DLM-Forum européen sur "Le citoyen européen et l'information électronique: la mémoire de la Société de l"information", Bruxelles, 18 -19 octobre 1999.*

3) *La réponse de l'industrie peut être consultée à l'adresse suivante: http://europa.eu.int/historical_archives/dlm_forum/doc/ictindustryresponse-fr.pdf*

4) *COM (1998) 585.*

5) *Nouvelles technologies de l'information et de la communication.*

Pour l'heure, aucune initiative législative communautaire n'est venue traduire en termes concrets ce constat, même dans le domaine de la protection sociale, domaine dans lequel la Communauté européenne joue pourtant un rôle essentiel, notamment pour la gestion des droits des travailleurs exerçant leur activité professionnelle de manière transfrontalière.

Reste donc à constater que les sources de réglementation les plus efficaces au niveau international proviennent en fait de standards de normalisation, dans le domaine de la gestion électronique des documents et de l'archivage électronique.

*Section 3 - **Les efforts de normalisation***

Diverses initiatives ont été menées afin d'assurer la normalisation internationale de l'archivage et la gestion électronique des documents. Ce sont principalement les normes de l'Organisation internationale de la normalisation (ISO) qui en sont à l'origine. Elles sont élaborées sous les auspices du groupe de travail TC 171 de l'ISO nommé " *Applications en gestion des documents* ".

A. La norme ISO 15489

Ainsi la norme ISO 15489[1)] a été adopté en 2001. Elle représente " *l'ossature de toute bonne gestion des enregistrements* "[2)] et constitue un guide pour l'organisation et la gestion des documents et des archives des organismes, publics ou privés[3)].

Elle organise la gestion des documents de leur création à leur archivage afin d'en rationaliser et d'en sécuriser le processus, indépendamment de la forme ou du support du document. Sur le plan organisationnel, elle est un guide pour la conception et la mise en oeuvre d'un système d'archivage. Elle définit, par ailleurs, les méthodes et procédures nécessaires pour organiser et gérer ces documents, gérer ces procédures, les contrôler et les auditer. A cet égard, elle recommande la mise en place d'une " *Charte de l'archivage* " qui synthétise les consignes générales d'archivage et la liste des documents à archiver. Cette charte doit formaliser notamment les contraintes légales, organisationnelles et techniques et énonce les procédures relatives à la sélection des documents à archiver, la durée de leur conservation, leur enregistrement, leur indexation, leur accès etc …. La norme élabore en outre

---

1) Voir ISO 15489-1 - Information et documentation - "Records management" - Partie 1 : principes directeurs et ISO/TR 15489-2 - Information et documentation - "Records management " - Partie 2: guide pratique.

2) Selon M. Marsh, Liaison européenne, ARMA Genève, Séminaire inaugural sur l'ISO 15489 consacrée à la gestion des enregistrements, 2003, http://www.iso.ch/iso/fr/commcentre/events/2003/armaiso15489.html

3) Elle exclut toutefois de son champ les archives historiques.

les procédures internes qui organisent la collecte, la conservation et la communication des archives au sein d'une organisation donnée.

Bref, elle donne l'ensemble des indications nécessaires à la mise en œuvre d'une politique de gestion et d'archivage électronique de documents.

Les obligations issues de la norme ISO 15489 sont précisées dans son guide pratique[1)]. Ce dernier énonce les bonnes pratiques et les méthodes à suivre. Il fournit la méthodologie pour faciliter la mise en œuvre de la norme. Il donne, enfin, une vision générale des processus et des facteurs à prendre en considération dans les organismes qui souhaitent se conformer à la norme ISO 15489.

B. La norme NF Z 42-013 et la future norme ISO 18509

En France, des "*recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes*" ont été publiées par l'Association française de normalisation (AFNOR) le 20 juillet 1999. Il s'agit en fait de la norme dite NF Z 42-013[2)].

Celle-ci vise à énoncer l'état de l'art en matière de support d'archivage électronique. Elle s'applique indifféremment aux documents archivés de manière électronique dont l'original était sur support papier ou sur support électronique.

Cette norme précise les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer leur conservation et leur intégrité. A cette fin, elle privilégie l'utilisation de systèmes " WORM " (acronyme anglais pour " Ecrire une fois, lire plusieurs fois ") notamment au regard de l'objectif de pérennisation et d'intégrité des documents.

Ce détour vers une norme nationale se justifie en raison de la reprise future de ce texte français par une norme ISO: la norme ISO 18509[3)]. Cette dernière établira les références pour la conception et l'exploitation de systèmes informatiques destinés à la conservation de documents. Elle est donc plus spécifique et technique que la norme ISO 15489, qui est quant à elle plus générale et tournée vers une démarche organisationnelle de maîtrise de l'information.

---

1) *Les procédures propres à assurer l'organisation et la gestion des documents selon les principes et les éléments constitutifs de la présente partie de l'ISO 15489 sont présentées dans l'ISO/TR 15489-2 (Guide pratique).*

2) *Elle est antérieure à la norme ISO 15489.*

3) *ISO/WD 18509-1, Electronic archival storage -- Specifications relative to the design and operation of information processing systems in view of ensuring the storage and integrity on recordings stored in these systems -- Part 1: Long term access strategy.*

Si, l'élaboration de la norme 18509 est à l'heure actuelle au stade de la mise à l'étude du projet de travail, il faut préciser que le législateur luxembourgeois tente, lui-aussi, de reprendre à son compte les spécifications de la norme française afin d'organiser l'archivage électronique de la Caisse nationale des prestations familiales[1)].

C. La recommandation EIDE

En ce qui concerne plus particulièrement la gestion électronique de documents, la recommandation EIDE *(Echange d'Informations et de Documents Electroniques)* doit être signalée. Elle a été transmise par l'APROGED (Association des professionnels de la gestion électronique de documents) à l'ISO afin de l'étudier dans le cadre d'un document de travail au niveau international.

La recommandation EIDE se base sur la technologie XML[2)] pour fournir un ensemble de recommandations concernant les mesures techniques à mettre en œuvre pour la génération de fichiers d'échange entre systèmes de gestion électronique afin d'assurer la compatibilité des transferts d'informations et de documents. Les travaux afin de transposer cette recommandation en norme ISO sont actuellement en cours.

D. Quelques autres normes…

Ces quelques exemples de normes ne constituent pas une analyse exhaustive. D'autres normes internationales existent, telles que la norme ISO 10918 relative à la compression numérique et le codage des images fixes de nature photographique, la norme ISO 9594 sur l'interconnexion des systèmes ouverts, l'ISO 13490 et 13346 sur la structure de volume et de fichier de support disques compact WORM (ou non WORM pour la 13346).

L'existence de la norme ISO 14721 doit aussi être signalée. Cette norme élabore un modèle de référence pour les systèmes d'archivage. Ce modèle dresse une gamme complète des fonctions de conservation de l'information (archivage, gestion des données, accès, et diffusion) et traite du transfert des archives sur d'autres supports et fournit aussi des illustrations et quelques recommandations de bonnes pratiques.

Citons enfin les normes ISO 10196 relative à la préparation des documents en vue de leur micro-filmage ou de leur numérisation et ISO 9735 sur l'échange de données pour l'administration et les règles de syntaxes au niveau de l'application.

Les normes ISO constituent les principales sources d'inspiration des politiques d'archivage et de gestion électronique de documents détenus par les entreprises ou les organismes publics. Bien que non mises en œuvre au

1) Voir infra.

2) Extensible Markup Language.

niveau du Luxembourg, les organismes de sécurité sociale devront en tenir compte dans l'élaboration de leur politique d'archivage. L'exemple de la caisse nationale des prestations familiales et du projet de loi n°5161 est à cet égard exemplaire[1)].

CHAPITRE III. - PROPOS CONCLUSIFS SUR L'ENVIRONNEMENT JURIDIQUE LUXEMBOURGEOIS DE LA GED ET DE L'ARCHIVAGE ÉLECTRONIQUE

En 1999, le DLM Forum a publié, sous l'égide de la Commission européenne, une étude relative au cadre législatif de l'archivage électronique dans les Etats membres[2)]. A cette occasion, si l'on résume la position du Grand-duché de Luxembourg par rapport à ces partenaires européens, il appert qu'aucune législation spécifique sur l'archivage électronique n'existe.

Au-delà de cette lacune normative, diverses dispositions législatives et réglementaires parcellaires tendent, toutefois, à régir la situation de l'archivage et, de manière moindre, la gestion électronique de documents. Voici une présentation succincte de cet environnement juridique en devenir.

Il convient de débuter par celles contenues dans le désormais bicentenaire code civil ainsi que dans le code de commerce.

*Section 1 - **Le code civil et le code de commerce***

Le code civil et le code de commerce contiennent, depuis leur modification par la loi du 14 août 2000 relative au commerce électronique[3)], diverses dispositions relatives à l'acte sous sein privé électronique ainsi qu'à la conservation sous forme de copie d'un acte original, et notamment de documents comptables.

Il convient de préciser que la loi du 14 août 2000 relative au commerce électronique a opéré une large refonte des dispositions relatives à la preuve littérale en conférant notamment et sous réserves de certaines conditions la même valeur probante à l'acte original établi sur support électronique que celui établit sur support papier.

Pour ce faire, elle abroge l'article 1348 alinéa 2 du code civil qui prévoyait que lorsqu'une partie ou le dépositaire n'a pas conservé les titres originaux et présente des reproductions micrographiques et enregistrements informatiques effectués à partir de ces originaux sous la responsabilité de la personne qui en a la garde, alors les reproductions et enregistrements ont la

---

1) Voir infra.

2) DLM Survey on the Relationship between Public Administration and Archives Services concerning electronic records management in the EU Member States, http://www.europa.eu.int/ISPO/dlm/Schuerer/htms/luxembourg.htm.

3) Mémorial A 2000, p. 2176.

même valeur probante que les écrits sous seing privé dont ils sont présumés, sauf preuve contraire, être une reproduction ou un enregistrement fidèles lorsque les originaux ont été détruits dans le cadre d´une méthode de gestion régulièrement suivie et qu'ils répondent aux conditions fixées par un règlement grand-ducal.

Cette disposition n'était en effet guère en phase avec les techniques actuelles en ce qu'elle ne s'appliquait qu'aux seuls enregistrements informatiques réalisés à partir d'originaux (c'est-à-dire d'écrits signés sur support papier)[1)] et ne pouvait donc tenir compte de copie de document établit originellement sur support informatique. La loi du 14 août 2000 comble cette lacune sans toutefois modifier le règlement de 1986, pris en application de l'article 1348.

Suite à ce bref rappel à caractère historique, il convient de présenter- toujours brièvement, les quelques dispositions du code civil et du code de commerce susceptibles d'intéresser la question de l'archivage et de la gestion électronique de documents au sein des organismes de sécurité sociale.

Commençons par l'article 1322-1 du code civil. Selon ce dernier, la signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte. Elle peut être manuscrite ou électronique. La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article. Nous avons vu précédemment l'interprétation large que le juge des affaires sociales a donné de cette disposition: nous n'y reviendrons pas[2)].

Aux termes de l'article 1322-2 du code civil[3)], introduit par la loi relative au commerce électronique, l'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive.

En outre, selon l'article 1333[4)], les copies, lorsque le titre original ou un acte faisant foi d'original au sens de l'article 1322-2 subsiste, ne font foi que de ce qui est contenu au titre ou à l'acte, dont la représentation peut toujours être exigée.

---

1) La Chambre de commerce, dans son avis du 22 février 1984 sur le projet de loi n° 2866 sur la preuve des actes juridiques, avait déjà souligné qu'elle ne pourrait être utilisée lorsque l'enregistrement informatique constitue lui-même l'original.

2) Voir les commentaires développés de Melle Maryline DURIN dans cette revue à ce propos.

3) Voir article 7 de la loi du 14 août 2000 relative au commerce électronique.

4) Voir rédaction issue de l'article 12 de la loi du 14 août 2000 relative au commerce électronique.

Enfin, la lecture de l'article 1334[1)] nous apprend que lorsque le titre original ou l'acte faisant foi d'original au sens de l'article 1322-2 n'existe plus, les copies effectuées à partir de celui-ci, sous la responsabilité de la personne qui en a la garde, ont la même valeur probante que les écrits sous seing privé dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal.

Par ailleurs, l'article 11 du code de commerce énonce désormais[2)] qu' " à l'exception du bilan et du compte des profits et pertes, les documents ou informations visés aux articles 8 à 10[3)] peuvent être conservés sous forme de copie. Ces copies ont la même valeur probante que les originaux dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par un règlement grand-ducal".

Ces dispositions, si elle sont fort éparses, constituent toutefois une base juridique permettant de procéder à un archivage électronique de documents établis sur support papier ainsi qu'à l'archivage de document originellement établis sur support informatique, sous réserve de la nature même du document[4)].

*Section 2 - **Le règlement de 1986 sur la copie***

Initialement pris sur le fondement de l'article 1348 alinéa 2 du code civil et 11 du code de commerce, le règlement grand-ducal du 22 décembre 1986 trouve désormais sa base juridique dans l'article 13 de la loi du 14 août 2000 relative au commerce électronique[5)]. Il énonce les conditions auxquelles doivent répondre la reproduction et l'enregistrement des copies afin que ces dernières puissent valoir comme copies fidèles et avoir la même valeur probante que leurs originaux.

---

1) *Voir rédaction issue de l'article 13 de la loi du 14 août 2000 relative au commerce électronique.*

2) *Voir rédaction issue de l'article 15 de la loi du 14 août 2000 relative au commerce électronique.*

3) *Il s'agit notamment du livre journal retraçant les opérations du commerçant (article 8) des pièces justificatives, des lettres reçues et les copies des lettres envoyées (article 9) ainsi que le bilan des comptes au regard des données de l'inventaire annuel de ses avoirs, droits, dettes, obligations et engagements de toute nature (article 10).*

4) *En présence d'un acte administratif, il conviendra de vérifier si ces sources juridiques sont applicables. Voir à ce propos, la contribution de M. Corentin POULLET dans ce bulletin.*

5) *Voir article 14 de la loi du 14 août 2000 relative au commerce électronique, qui renvoie à l'article 13 de la même loi; ce dernier modifiant l'article 1334 du code civil prévoyant l'adoption d'un règlement grand ducal.*

Outre les conditions de type législatif précitées[1)], les copies doivent être la reproduction ou l'enregistrement fidèle et durable du document original ou de l'information à l'origine de l'enregistrement. Le règlement pose à cet effet une présomption selon laquelle est réputée durable toute reproduction indélébile de l'original et tout enregistrement qui entraîne une modification irréversible du support.

Le règlement de 1986 précise par ailleurs que les copies devront être effectuées de façon systématique et sans lacunes et ce, selon des instructions de travail conservées aussi longtemps que les reproductions ou enregistrements. Bien entendu, les copies doivent être conservées avec soin, dans un ordre systématique, et protégés contre toute altération.

Il s'agit donc ici d'énoncer les conditions organisationnelles dans lesquelles devront s'effectuer les copies des documents originaux et d'assurer la mise en place d'une politique d'archivage, éventuellement gérer de manière sécurisée et externe par un " tiers-archiveur ". Cette politique ne saurait d'ailleurs être complète si l'ensemble de la documentation relative aux programmes et systèmes informatiques ayant permis la copie fidèle et durable devait disparaître.

Section 3 - ***Quelques textes spécifiques aux organismes de sécurité sociale***

En ce qui concerne le rôle de l'informatique au sein des organismes de sécurité sociale, deux règlements grand-ducaux doivent être signalés.

Il s'agit en premier lieu du règlement grand-ducal du 12 mai 1975 portant organisation et fonctionnement du centre d'informatique, d'affiliation et de perception des cotisations commun aux institutions de sécurité sociale[2)]. Ce texte définit la mission de ce Centre informatique comme ayant un caractère essentiellement technique. Il a en effet pour mission de gérer les équipements communs de saisie et de traitement de l'information; d'effectuer sur ordinateur leurs travaux; de promouvoir et d'organiser de façon rationnelle et coordonnée leur automatisation, notamment en ce qui concerne la programmation des applications, la collecte, la transmission et le traitement des données sur ordinateur; de constituer, de gérer et de tenir à jour leurs fichiers communs; d'enregistrer les affiliations aux différents régimes de sécurité sociale; de procéder aux calculs, à la perception, au recouvrement et à la répartition des cotisations; de leur fournir les informations individuelles ou statistiques qui sont nécessaires à l'exécution de leurs tâches.

C'est ainsi au Centre que revient la tâche de consigner et dater sur un registre spécial toutes les entrées et sorties de documents, bordereaux et supports informatiques. Cela constitue la base de l'archivage électronique auquel le

1) Celles de l'article 1334 du code civil.

2) Mémorial A 1975, p. 701.

Centre se doit de procéder et dont il constitue l'acteur essentiel au sein des organismes de sécurité sociale.

Le second texte dont il doit être fait mention est le règlement grand-ducal du 22 décembre 1989 concernant la comptabilité et les comptes annuels des organismes de la sécurité sociale et du fonds national de solidarité[1)]. Ce texte prévoit en effet que les documents et informations visés aux articles 2 et 5 (soit les opérations comptables des organismes de sécurité sociale ainsi que les livres comptables), à l'exception du bilan et du compte de résultat, peuvent être conservés sur support informatique, à condition que les reproductions ou les enregistrements correspondent au contenu des documents ou des informations à conserver et qu'ils peuvent être produits pendant la durée de la conservation.

Des règles juridiques concernant l'archivage électronique au sein des organismes existent donc bel et bien. Pour l'heure, elles ne concernent que les documents comptables. Elles permettent en outre l'archivage électronique sous des conditions de fidélité et de durabilité des archives, sans toutefois renvoyer à plus de détails techniques (comme c'est le cas du code civil avec le renvoi au règlement de 1986) quant à la mise en œuvre pratique de cet archivage.

*Section 4 - **Le projet de loi no 5161***

Pour conclure et sans vouloir anticiper l'adoption du projet de loi no 5161[2)], il convient de signaler une disposition que ce texte contient, et qui intéresse tout particulièrement les organismes de sécurité sociale et qui répond à l'attente précédemment exprimée.

En effet, ce projet propose la mise en place du cadre législatif de l'archivage et la gestion électronique de documents pour la Caisse nationale des prestations familiales. Il permet, sur la base de la norme française NF Z 42-013 d'admettre le système d'archivage électronique mis en place par cette caisse dans le cadre de la mission et pour ses besoins spécifiques. Il vise principalement à conserver une valeur légale des documents scannés (suivant les prescriptions de la norme NF) identique aux orignaux.

---

1) Mémorial A 1989, p. 1726.

2) Voir projet de loi n° 5161 portant modification de la loi du 12 février 1999 portant création d'un congé parental et d'un congé pour raisons familiales; la loi modifiée du 19 juin 1985 concernant les allocations familiales et portant création de la caisse nationale des prestations familiales; la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Le projet d'article II dispose ainsi, sur le modèle de l'article 1334 du code civil[1)], que: " *Les images électroniques archivées définitivement sur disque optique numérique non réinscriptible dans le cadre du système de gestion électronique de documents de la caisse Conformément à la norme AFNOR Z 42-013 ont la même valeur probante que les documents papier dont elles sont issues par numérisation sans la moindre altération par rapport à l'original et dont elles sont présumées, sauf preuve contraire, être une copie fidèle. La banque d'images constituée de copies numérisées de documents papier et de copies directes de documents électroniques, a valeur d'archives légales de la caisse. Celle-ci est autorisée à détruire chaque document original sur support papier six mois après l'archivage définitif de l'image correspondante tel que défini à l'alinéa qui précède. Lorsqu'elles sont certifiées conformes à l'original par la Caisse nationale des prestations familiales, les images visées ci-avant ou la copie imprimée sur papier de ces images sont recevables en justice à l'égal des documents originaux.* ".

Si le texte se rapproche de la systématique mise en place par l'article 1334 du code civil, une référence est faite à la norme française Z 42-013, elle-même faisant référence, selon les auteurs du projet de loi, à de nombreuses normes notamment ISO[2)].

Cette modification législative est motivée par " la croissance extrêmement rapide des archives du congé parental qui contribue pour une large part à la saturation de l'espace d'archivage disponible à la caisse ". Les auteurs du projet de loi précisent que dans la mesure où la Caisse est obligée de garder les dossiers afférents pendant 5 années au minimum en vue de l'examen du droit au deuxième congé parental, le recours aux archives électroniques représente un gain considérable en temps de recherche.

Il fait peu de doutes que les autres organismes sont confrontés à des problèmes identiques à ceux de la CNAF et que des réformes législatives prochaines tenteront de leur donner des bases juridiques aussi fermes.

***

---

1) Cet article procède par voie de modification de l'article 6 de la loi modifiée du 19 juin 1985 concernant les allocations familiales et portant création de la caisse nationale des prestations familiales, en insérant à celui-ci un alinéa 13 nouveau.

2) Le Conseil d'Etat se rallie à cet aspect du projet. Toutefois, il estime qu'il n'est pas opportun de se référer dans un texte de loi à une norme spécifique et c'est la raison pour laquelle il propose de remplacer les termes " norme AFNOR Z 42-013 " par les termes " norme standard ".

Voici brièvement tracés quelques points saillants de la réglementation luxembourgeoise en matière d'archivage électronique. Peu de mots ont été prononcés sur la gestion électronique des documents: il appert en effet que la réglementation à ce sujet est largement lacunaire. Gageons que le développement de l'administration en ligne suscitera l'adoption de normes législatives et réglementaires adaptées à ces nouvelles pratiques. Peut-être est alors venu le temps d'organiser, au niveau législatif et réglementaire, la mise en œuvre pour tous et, si possible, de manière harmonisée, d'un archivage et d'une gestion électronique des documents des organismes de sécurité sociale.

La signature électronique

Maryline DURIN

Chercheur
Laboratoire de Droit Economique
Centre de Recherche Public Gabriel Lippmann

I. INTRODUCTION

La signature électronique est tout à la fois un thème très à la mode et mystérieux qui évoque des images très différentes selon les personnes interrogées. Chez le commun des internautes, elle équivaut à ce fameux clic de souris par lequel il s'engage dans les liens d'un contrat avec un prestataire de service: " je clique donc je signe donc je m'engage ". Chez le prestataire de service, la signature électronique n'est pas loin d'évoquer un imbroglio technico-juridique dont il se serait bien passé. Chez l'informaticien, la signature électronique évoque des lignes et des lignes de calculs mathématiques complexes. Enfin, chez le juriste, elle est devenue, depuis que la loi l'a introduite dans le Code civil, une réalité dont il lui faut prendre toute la mesure - tâche pour laquelle il se voit contraint de s'adjuger les services d'un technicien sous peine de produire une analyse en totale déconnexion avec la réalité technologique.

En résumé, les choses ne sont pas simples et la consécration légale de la signature électronique, si elle a répondu à un important besoin, n'a pas aplani toutes les difficultés. Un travail d'explication, de vulgarisation, de mise à la portée de tous et d'une manière adaptée aux besoins de chacun attend encore le juriste dans les années à venir. Tâche ambitieuse s'il en est, mais ô combien intéressante!

Il s'agit donc tout d'abord de voir pourquoi une législation sur la signature électronique était devenue nécessaire **(II)** puis d'expliquer précisément ce qu'est une signature électronique **(III)**. Enfin la signature électronique n'est qu'un instrument, un outil, " créé " par le droit au service de la pratique. Il faudra donc dire très concrètement ce qu'elle vaut ou, plus exactement, ce que vaut le document qui en est revêtu **(IV)**.

II. Pourquoi une nouvelle législation sur la signature électronique?

Jusqu'à la loi du 14 août 2000 relative au commerce électronique[1)], le droit luxembourgeois connaissait certes la notion de signature, mais n'en comportait aucune définition. Cette situation, pour étonnante qu'elle puisse paraître, n'avait cependant rien d'isolée. Il en était de même par exemple en France et en Belgique.

Le silence de la loi avait été suppléé par le juge qui avait élaboré une conception formelle de la signature basée sur un support particulier: le papier. La signature était alors conçue comme " une marque distinctive, personnelle et manuscrite qui devait permettre d'individualiser son auteur sans doute possible, et traduisant la volonté non équivoque de celui-ci de consentir à l'acte "[2)].

Cette conception stricte se trouvait en quelque sorte conforter par le code de procédure civile. En effet, il prévoit que lorsqu'une partie dénie la signature qui lui est opposée, une procédure de vérification d'écriture peut être ordonnée en justice. Cette procédure est basée sur la soumission par les parties au juge chargé de trancher de différentes pièces de comparaison[3)]. Or l'article 302 du nouveau code de procédure civile dispose que lorsque le juge-commissaire estime ne pas être en présence d'éléments de comparaison suffisants, il peut ordonner qu'*un texte soit dicté* par les experts au défendeur, en présence du demandeur ou celui-ci ayant été appelé[4)]. Autrement dit, on en revient à l'idée selon laquelle la signature ne peut être qu'un signe *manuscrit*.

La conception formelle de la notion de signature a pendant longtemps été considérée comme légitime et satisfaisante. Légitime car on estimait que seule l'apposition par une personne d'une mention, d'un signe, de sa main permettait de garantir qu'elle avait bel et bien pris conscience de l'engagement qu'elle avait ainsi souscrit. Satisfaisante car il n'existait pas d'autres modes d'extériorisation de la volonté qui permettent tout à la fois d'éliminer tout risque d'équivoque quant au sens et à la portée de la volonté exprimée et de conserver, à toutes fins utiles, une trace fiable de cette manifestation.

---

1) Loi du 14 août 2000 relative au commerce électronique (Mém. 2000, 2176).

2) La France avait également adopté une telle conception. Voir à ce propos : cour d'appel de Paris, 22/05/1975, D. 1976. SC. 8.

3) Voir les articles 289 et suivants du nouveau code de procédure civile.
On rappellera qu'il appartient à celui qui se prévaut d'un acte sous privé qui a été dénié, de démontrer qu'il émane bien de la personne à qui il l'oppose.

4) Article 302 du nouveau code de procédure civile: " A défaut ou en cas d'insuffisance des pièces de comparaison, le juge-commissaire pourra ordonner qu'il sera fait un corps d'écritures, lequel sera dicté par les experts, le demandeur présent ou appelé. "

Mais les progrès technologiques aidant, il est apparu de nouveau modes d'extériorisation de la volonté juridique, en particulier lorsque l'auteur de cette volonté, au moment où il la manifeste, ne se trouve pas en présence de celui auquel elle est destinée. L'avènement des communications électroniques et d'Internet a ouvert de nouvelles perspectives dans le cadre de relations se nouant à distance. L'envoi et l'échange de documents sous forme électronique ont considérablement modifié " la donne ".

Dès lors, plusieurs raisons expliquent l'adoption de dispositions légales consacrant la signature électronique au côté de la signature manuscrite.

La première raison tient aux appels pressants de la pratique. En effet, d'un point de vue juridique, à la lumière de l'interprétation jurisprudentielle de la notion de signature, chaque fois que la loi exige qu'un document soit signé, ce document ne pouvait se présenter que sur un support papier puisqu'il devait recevoir " la marque distinctive, personnelle ET manuscrite " de celui dont la signature était requise. En d'autres termes, un document électronique ne pouvait être valablement signé. On comprend alors que la pratique, naturellement encline à tirer profit des potentialités offertes par l'apparition des échanges électroniques, ne se soit plus satisfaite de la situation juridique. L'insécurité juridique liée au recours à aux réseaux électroniques et à Internet devait trouver une réponse. La jurisprudence n'ayant pas montré au Luxembourg de signe de changement quant à sa manière d'appréhender la notion de signature[1)], cette réponse ne pouvait venir que du législateur.

Une autre raison importante, et peut-être plus impérieuse encore, explique l'intervention du législateur. Le Luxembourg, tenu par ses obligations communautaires, se devait de transposer dans son droit la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[2)].

---

1) *A titre de comparaison, la jurisprudence française avait montré quelques signes d'évolution notamment dans un important arrêt de la chambre commerciale de la Cour de cassation du 2 décembre 1997 (à ce propos, voir Pierre, Catala, Pierre-Yves, Gautier, L'audace technologique de la Cour de cassation: vers la libéralisation de la preuve contractuelle, JCP E 1998. 884). Cependant, il avait été bien délicat d'en analyser avec certitude la portée. C'est pourquoi, en France également, on a estimé nécessaire une intervention du législateur. Voir à ce sujet, la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux nouvelles technologies et relative à la signature électronique, JO, n° 62, 14 mars 2000, p. 3968.*

2) *Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, JO, n° L 013, du 19/01/2000, p. 0012 - 0020.*

Or le texte communautaire impose aux Etats membres de veiller à ce qu'une signature électronique, si elle répond à certaines conditions de sécurité (que fixe le texte), se voit reconnaître la même valeur juridique sur le plan de la preuve qu'une signature manuscrite (principe d'assimilation)[1]. Bien plus, la directive 1999/93/CE leur demande également de faire en sorte que les signatures électroniques qui ne répondent pas aux conditions nécessaires pour avoir la même valeur juridique qu'une signature manuscrite, ne soient pas rejetées par le juge pour le seul motif qu'elles sont sous forme électronique (principe de non-discrimination)[2]. En conséquence, le Luxembourg n'avait d'autre choix que de modifier sa législation afin d'intégrer ces nouveaux principes, sous peine de faire l'objet d'un recours en manquement pour violation de ses obligations communautaires.

Les nouvelles règles juridiques concernant la signature électronique sont issues d'une loi et d'un règlement grand-ducal. Il s'agit de la loi du 14 août 2000 relative au commerce électronique (qui a récemment été modifiée) et du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique"[3].

La loi du 14 août 2000 comporte un titre II intitulé " De la preuve littérale et de la signature électronique " dont le premier article (l'article 6) modifie le Code civil en introduisant une définition générale de la signature, quelle que soit sa forme, puis une définition spéciale de celle-ci lorsqu'elle est électronique **(Cf. III)**. Il est par ailleurs une autre disposition fondamentale dans la loi qui est très utile pour déterminer ce que vaut une signature électronique: il s'agit de l'article 18 intitulé " Des effets juridiques des signatures électroniques " **(Cf. IV)**.

---

1) *Article 5. 1 de la directive 1999/93/CE:*
" Les États membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature:
a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier
et
b) soient recevables comme preuves en justice. "

2) *Article 5. 2 de la directive 1999/93/CE: " Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que:*
- la signature se présente sous forme électronique
ou
- qu'elle ne repose pas sur un certificat qualifié
ou
- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification
ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature. "

3) *Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique" (Mém. 2001, 1429).*

Quant au règlement grand-ducal du 1er juin 2001, il décrit très précisément les conditions qu'une signature électronique doit satisfaire pour se voir reconnaître la même valeur juridique qu'une signature manuscrite. Il complète également la loi relativement aux règles applicables en matière de services de certification électronique - une nouvelle activité qui est apparue avec le développement de l'utilisation des signatures électroniques en réseaux ouverts, tels Internet, et dont on mesurera toute l'importance au moment où l'on présentera ce qu'est une signature électronique.

Enfin, avant d'aborder le cœur du sujet, il est essentiel d'avoir à l'esprit le point suivant. Dans le domaine des actes juridiques, deux questions doivent être clairement distinguées: celle de leur validité et celle de leur preuve.

La validité d'un acte juridique s'apprécie par rapport aux conditions de formation que la loi a pu poser à son égard. Ainsi la requête introduisant un recours devant le Conseil arbitral des assurances sociales ou le Conseil supérieur des assurances sociales doit contenir différentes mentions obligatoires parmi lesquelles la signature du requérant[1)]. Cette formalité de la signature est une formalité substantielle à peine de nullité de l'acte introductif d'instance et donc d'irrecevabilité du recours[2)]. La question de la validité d'un acte juridique doit être envisagée au moment de son établissement.

La question de la preuve d'un acte juridique invite quant à elle à s'interroger sur la manière dont une personne se prévalant d'un acte juridique peut démontrer son existence. Elle ne préjuge pas de sa validité. La loi impose parfois le respect de certaines conditions de forme pour cette démonstration.

---

1) *Voir à ce propos le règlement grand-ducal du 24 décembre 1993 déterminant en application de l'article 294 du code des assurances sociales la procédure à suivre devant le conseil arbitral et le conseil supérieur des assurances sociales, ainsi que les délais et les frais de justice (Mém. 1993, 2320), modifié par le règlement grand-ducal du 23 décembre 1999 (Mém. 1999, 2935), et en particulier l'article 1er:*
" Les recours concernant les contestations visées à l'article 293, alinéa 1 du code des assurances sociales doivent être formés, sous peine de forclusion, dans un délai de quarante jours à dater de la notification de la décision attaquée, par simple requête sur papier libre à déposer au siège du conseil arbitral. La requête est présentée en autant d'exemplaires qu'il y a de parties en cause.
Elle indique les noms, prénoms, numéros d'identité, profession et domicile du demandeur, ainsi que la qualité en laquelle il agit, et énonce l'objet de la demande et l'exposé sommaire des moyens. La requête doit être signée par le demandeur ou son représentant légal ou son mandataire qui peut être le représentant de son organisation professionnelle ou syndicale. Il en est de même des autres pièces produites en cours de la procédure. Si la requête est présentée par un mandataire, ce dernier, s'il n'est pas avocat doit justifier d'une procuration spéciale. Cette dernière doit être présentée au plus tard lors du débat oral et avant que celui-ci ne soit entamé. "

2) *La jurisprudence des juridictions sociales est constante sur ce point. Voir notamment: Décision du CSAS du 13/10/1993, n° 141/93; Décision du CSAS du 21 avril 1999, Steinberg M. c/ CPEP; Décision du CAAS du 31/03/2003, Affaire Wiersbowsky c/ CPEP.*

Ainsi lorsque l'acte juridique porte sur une valeur supérieure à 2 500 euros, l'article 1341 C. civ. exige qu'il soit prouvé par un écrit signé (acte sous seing privé[1)] ou acte authentique[2)]).

Afin de bien montrer toute l'importance de la distinction validité / preuve d'un acte juridique, il suffit d'en indiquer l'un des enjeux. Dans le cas où un acte serait valable au regard des conditions que la loi a posées pour sa formation valable, il se peut qu'il puisse être malgré tout dépourvu de tout effet juridique en cas de contestation, si la personne qui s'en prévaut échoue à en rapporter la preuve. En effet, " un droit n'est rien s'il ne peut être prouvé ". Aussi cette personne verra sa prétention rejetée par le juge.

Les nouvelles dispositions relatives à la signature électronique introduites par la loi du 14 août 2000 relative au commerce électronique ont une portée doublement limitée. Tout d'abord, elles ne concernent pas la question de la validité de l'acte juridique. La signature électronique n'a reçu une existence légale que pour les cas où la loi requiert que la preuve d'un acte juridique soit rapportée au moyen d'un écrit signé. La seconde limite de la consécration légale de la signature électronique est qu'elle ne concerne qu'une catégorie d'écrits: les actes sous seing privé.

Toutefois, la directive 2000/31/CE sur le commerce électronique[3)], qui constitue un socle de règles visant à harmoniser les législations des Etats membres dans le domaine des services de la société de l'information et notamment du commerce électronique, impose aux Etats membres de procéder à un examen complet de leur législation afin de supprimer tous les obstacles directs ou indirects à l'utilisation des contrats électroniques[4)].

---

1) *Un acte sous seing privé est un écrit signé, établi par les parties elles-mêmes, en dehors de la présence d'un officier public.*

2) *Un acte authentique est un écrit reçu par un officier public et signé par lui ainsi qu'a minima par les parties à cet acte.*

3) *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique"), Journal officiel n° L 178 du 17/07/2000 p. 0001 - 0016.*

4) *Article 9 de la directive sur le commerce électronique:*
" 1. Les États membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les États membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique.
2. Les États membres peuvent prévoir que le paragraphe 1 ne s'appliquent pas à tous les contrats ou à certains d'entre eux qui relèvent des catégories suivantes:
a) les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location;
b) les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique;
c) les contrats de sûretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale;
d) les contrats relevant du droit de la famille ou du droit des successions.
3. Les États membres indiquent à la Commission les catégories visées au paragraphe 2 auxquelles ils n'appliquent pas le paragraphe 1. Ils soumettent tous les cinq ans à la Commission un rapport sur l'application du paragraphe 2 en expliquant les raisons pour lesquelles ils estiment nécessaire de maintenir les catégories visées au paragraphe 2, point b), auxquelles ils n'appliquent pas le paragraphe 1. "

Or le Luxembourg, en ne reconnaissant pas la signature électronique dans les cas où une signature est requise par la loi pour la validité d'un acte juridique, a laissé dans son système juridique un important obstacle direct au recours au média électronique. La loi portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique, modification de la loi modifiée du 30 juillet 2002 réglementant certaines pratiques commerciales, sanctionnant la concurrence déloyale et transposant la directive 97/55/CE du Parlement européen et du Conseil modifiant la directive 84/450/CEE sur la publicité comparative afin d'y inclure la publicité comparative et abrogation de l'article 1135-1, alinéa 2 du Code civil (non encore publiée) a cependant remédié à cette lacune en disposant purement et simplement que: " Les exigences légales et réglementaires, notamment de forme, qui empêchent ou limitent la conclusion de contrats par voie électronique, y compris celles qui privent d'effet ou de validité juridique des contrats du fait qu'ils ont été passés par voie électronique, sont inapplicables aux contrats [électroniques]"[1)] . Aussi il faut comprendre désormais que toutes les exigences de forme incompatibles avec l'environnement électronique doivent être écartées sans autre forme de procès dés l'instant où il est question d'un contrat conclu par voie électronique[2)]. Par contre, la nouvelle disposition ne concerne pas les actes juridiques qui ne sont pas des contrats[3)]. Pour ces derniers, les exigences de forme imposées par la loi ou le règlement comme une condition de leur validité continuent à s'appliquer de même que par le passé.

Signalons par ailleurs que le Conseil supérieur des assurances sociales (CSAS) a donné récemment quelques signes d'une évolution de la conception jurisprudentielle de la signature requise ad validitatem. En effet, dans une décision du 8 décembre 2003, il admet que la signature de la requête introduisant un recours devant le Conseil arbitral des assurances sociales puisse être électronique[4)].

Si dans son esprit cette décision doit être saluée pour son ouverture, elle n'échappe pas à toute critique dans sa forme. En effet, le CSAS a formellement fondé sa décision sur les articles 1322-1, 1322-2 C. civ. et 18 de la loi du 14 août 2000 relative au commerce électronique alors que ces

---

1) *Voir l'article 50 (2) de la loi modifiée du 14 août 2000 relative au commerce électronique.*

2) *La solution adoptée est vivement critiquable dans la mesure où elle prive les parties à un contrat électronique notamment de tout le formalisme protecteur dont il aurait bénéficié s'il avait contracté " hors ligne ". Il aurait très certainement été préférable de repenser les exigences classiques de forme afin de les adapter aux particularités de l'environnement électronique.*

3) *On pense par exemple à une décision d'un organisme de sécurité sociale d'accorder un droit à un assuré.*

4) *Décision du Conseil supérieure des assurances sociales du 8 décembre 2003, statuant sur un jugement du Conseil arbitral des assurances sociales du 7 juillet 2003, Affaire Bouche c/ CPEP. La décision peut être consultée sur le site de la Sécurité sociale, http://www.secu.lu*

textes ont un champ d'application expressément restreint à la preuve des actes. Ils ne peuvent donc, en tout état de cause, être utilisés pour résoudre un problème juridique ayant trait à la validité d'un acte introductif d'instance.

Quoi qu'il en soit, la consécration légale de la signature électronique est susceptible d'entraîner d'importantes conséquences pour les organismes de sécurité sociale dans la manière dont ils gèrent les questions relatives à la preuve de l'existence d'un document dont la production en justice pourrait s'avérer nécessaire en cas de litige avec un assuré. Aussi, il est temps à présent de dire ce qu'est précisément une signature électronique.

III. Qu'est ce qu'une signature électronique?

La loi du 14 août 2000 relative au commerce électronique aborde la question de la signature nécessaire à la perfection d'un acte sous seing privé dans son article 6 qui a introduit dans le Code civil un nouvel article 1322-1 ainsi formulé:

"La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.

Elle peut être manuscrite ou électronique.

La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article."

L'article 1322-1 C. civ. a un triple objet. Il introduit dans le Code civil une définition générale de la notion signature quelle que soit sa forme. Il indique que la signature peut être manuscrite ou électronique. Enfin, il donne une définition spéciale de la signature quand elle est électronique.

L'article 1322 al. 1 C. civ. fournit une définition fonctionnelle de la signature: la signature identifie son auteur et manifeste son adhésion au contenu de l'acte qui en est revêtu.

Quant à l'article 1322-1 al. 3 C. civ., il définit la signature lorsqu'elle se présente sous forme électronique. Il s'agit d'un ensemble de données qui doit bien entendu tout d'abord satisfaire aux deux fonctions mises en avant par l'alinéa premier - à savoir les fonctions d'identification du signataire **(C)** et de manifestation de son approbation au contenu signé **(D)**. Le texte pose cependant deux conditions supplémentaires: l'ensemble de données en question doit également être lié de façon indissociable à l'acte **(A)** et en garantir l'intégrité **(B)**.

A. Une signature électronique est un ensemble de données liées de façon indissociable à l'acte

Une signature électronique est en premier lieu un ensemble de données (c'est-à-dire un ensemble d'informations créées et conservées par des moyens électroniques) liées *de façon indissociable* à l'acte (au document).

Il est important de préciser que l'exigence d'un lien indissociable ne doit pas s'entendre du point de vue matériel. Il n'est pas nécessaire que l'ensemble de données constituant la signature électronique soit " physiquement " attaché au document: ils peuvent être contenus dans deux fichiers distincts. Ce lien indissociable qui unit l'ensemble de données au document est un lien d'ordre intellectuel, logique. Il faut comprendre par-là que l'ensemble de données ne constitue une signature au sens de l'article 1322-1 C. civ. que lorsqu'il accompagne le document auquel il se rattache. En d'autres termes, on peut dire qu'il y a un lien indissociable entre l'ensemble de données et le document lorsque l'ensemble de données, s'il est détaché du document auquel il se rapporte, ne peut être réutilisé en tant que signature. Ainsi le scanne d'une signature manuscrite jointe au document électronique auquel elle se rattache, n'est pas une signature électronique au sens de l'article 1322-1 al. 3 C. civ. car elle n'est pas liée de manière indissociable à ce document puisqu'elle peut être réutilisée de la même manière pour d'autres documents.

Dans le cas particulier où la signature électronique est basée sur la cryptographie[1)], le lien indissociable entre elle et le document signé provient du fait que l'ensemble de données constituant la signature est le résultat de l'application de fonctions mathématiques au document.

Mais la signature électronique est un ensemble de données qui doit également remplir trois autres fonctions.

B. Une signature électronique est un ensemble de données liées à l'acte, qui garantit l'intégrité de l'acte

Un document est dit intègre s'il n'a subi aucune modification ou altération à partir du moment où il a été créé pour la première fois sous sa forme définitive. Il est important de préciser que l'intégrité du document doit être garantie non seulement au moment de sa transmission, mais également au-delà de celle-ci et ce, aussi longtemps que l'acte peut faire l'objet d'un recours.

---

1) La cryptographie peut être définie comme " toute transformation par un algorithme mathématique de signes intelligibles en signes inintelligibles, de façon à ce que seules les personnes autorisées soient en mesure de procéder au décryptage, par la transformation mathématique inverse " *: A. BERENBOOM et E. JOORIS, " Etude pour une législation sur la Signature Electronique pour le Grand-Duché de Luxembourg ", Bruxelles 1998.*

L'article 1322-1 al. 3 C. civ. attribue une fonction d'intégrité à la signature électronique. En d'autres termes, la signature électronique doit permettre de garantir que le document auquel elle est liée n'a pas été modifié ou altéré à partir du moment où il a été créé pour la première fois sous sa forme définitive.

En l'état actuel de la technique, seule la cryptographie, et plus précisément la cryptographie asymétrique assure une telle fonction.

Il existe (principalement) deux systèmes de cryptographie: la cryptographie symétrique et la cryptographie asymétrique.

Dans le cadre du premier système, une seule et même clé est utilisée pour crypter et décrypter un document. Ce système est adapté pour une utilisation en réseau fermé, entre des partenaires qui se connaissent et se font mutuellement confiance. Il ne l'est pas pour un fonctionnement en réseau ouvert de type internet car les personnes qui entrent en contact ne se connaissent pas nécessairement. En outre, se poserait le problème de la communication de la clé entre ces personnes, dans des conditions permettant d'éviter qu'elle ne soit interceptée par un tiers. Rapporté à notre hypothèse, nous nous rendons compte que dans le système de la cryptographie symétrique, toutes les personnes auxquelles la clé a été communiquée ont les moyens de modifier à volonté les documents " signés " au moyen de cette clé, puis de les re-signer de telle sorte à ce que la modification ne puisse être détectée par les autres. Aussi la fonction d'intégrité ne pourrait être satisfaite par une telle signature électronique.

Quant au système de la cryptographie asymétrique, il repose sur une paire de clés: l'une, appelée clé privée, doit rester secrète et sert à crypter et donc à signer le document, l'autre, appelée clé publique, qui sert à décrypter et peut être connue par tous ceux qui reçoivent un document signé au moyen de la clé privée. Dans le cadre de ce système, seul le signataire connaît la clé qui sert à signer. Lui seul peut donc en principe modifier son propre document. C'est pourquoi on peut dire qu'il y a là une importante garantie quant à l'absence de modification du document postérieurement à sa création par son auteur.

Dans la pratique, la signature électronique est créée sur la base de la cryptographie asymétrique, associée à ce que l'on appelle une fonction de hachage[1)]. En effet, ce ne sera pas l'ensemble du document qui sera crypté au moyen de la clé privée du signataire mais seulement un résumé, un

---

1) Une fonction de hachage est une fonction mathématique connue. Le condensé qui est obtenu par son application à un document est toujours de même longueur, quelle que soit la longueur du document. Par ailleurs, il est impossible de retrouver le document initial à partir du condensé (opération inverse) car la fonction de hachage est une fonction à sens unique. Elle joue ainsi un rôle important dans la fonction d'intégrité que la signature électronique doit remplir.

condensé (un " hash ") de celui-ci, ce qui permet notamment un gain de temps.

DESCRIPTION DU PROCESSUS DE CRÉATION D'UNE SIGNATURE ÉLECTRONIQUE AINSI QUE DE CELUI DE LA VÉRIFICATION DE L'INTÉGRITÉ DU DOCUMENT ÉLECTRONIQUE SIGNÉ

Le processus de création d'une signature électronique

1) La génération d'une paire de clés cryptographiques

Cette première étape, préalable à la création d'une signature électronique, peut être accomplie soit par la personne qui souhaite signer le document électronique, soit être confiée par cette dernière au prestataire de service de certification qu'elle aura choisi pour lui délivrer un certificat électronique (dont nous verrons par la suite le rôle essentiel dans la réalisation de la fonction d'identification de la signature électronique).

La génération d'une paire de clés cryptographiques est réalisée par un logiciel.

La clé privée constitue ce que le règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique" appelle " la donnée afférente à la création de signature "[1)] : elle permet la création de la signature électronique.

Quant à la clé publique, elle est " la donnée afférente à la vérification de la signature "[2)] : elle sert à vérifier la signature et plus particulièrement l'intégrité du document électronique signé.

---

1) *Article 1 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique" : " Au sens du présent règlement, on entend par : 1° Données afférentes à la création de signature : des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique. "*

2) *Article 1 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique" : " Au sens du présent règlement, on entend par : 4° Données afférentes à la vérification de signature : des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisés pour vérifier la signature électronique. "*

2) Le choix d'un dispositif de création de signature

Le dispositif de création de signature est essentiellement constitué par un logiciel qui met en application la donnée de création de la signature (à savoir la clé privée) et permet ainsi la création de la signature[1)]. En d'autres termes, il permet de crypter (de chiffrer) le condensé obtenu par l'application d'une fonction de hachage au document électronique. Le résultat obtenu constitue la signature électronique.

Il existe sur le marché une multitude de dispositifs de création de signature. Tous ne garantissent pas à l'utilisateur le même degré de sécurité. Aussi, nous verrons que le législateur a posé que seules les signatures électroniques (considérées du point de vue technique) qui ont été créées au moyen d'un dispositif sécurisé de création de signature sont présumées répondre à la définition de l'article 1322-1 al. 3 C. civ.

C'est pourquoi, il est vivement conseillé à celui qui envisage d'utiliser une signature électronique de recourir à un dispositif considéré comme sécurisé de création de signature. La notion a été définie par le règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique" comme étant un dispositif de création de signature qui satisfait à des exigences spécifiques de sécurité énumérées par l'article 4 du règlement grand-ducal du 1er juin 2001[2)].

L'article 4 du règlement grand-ducal du 1er juin 2001 nous apprend ainsi que le dispositif de création de signature doit " garantir, par les moyens techniques et les procédures appropriés, que les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée; que l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles et enfin que les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire

---

1) *Article 1 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique": " Au sens du présent règlement, on entend par: 2° Dispositif de création de signature: un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature. "*
Pour être tout à fait exact, le dispositif de création de signature est constitué en pratique non seulement par le logiciel qui met en œuvre la donnée de création de signature, mais aussi par l'ordinateur qui héberge ce logiciel: cela forme un " tout ".

2) *Article 1 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique": " Au sens du présent règlement, on entend par: 3° Dispositif sécurisé de création de signature: dispositif de création de signature qui satisfait aux exigences prévues à l'article 4 du présent règlement grand-ducal. "*

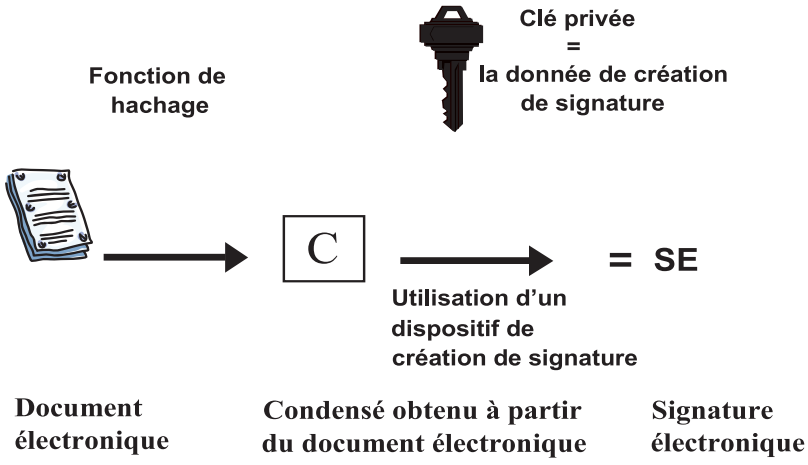
légitime contre leur utilisation par des tiers ". En outre, le dispositif de création de signature ne doit pas " modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature ".

Le législateur est intervenu pour faciliter la tâche de ceux qui élaborent de tels dispositifs, en précisant que:

" **Le Ministre ayant la normalisation dans ses compétences publie au Mémorial les références des normes ou réglementations techniques généralement admises y compris nationales relatives aux produits de signature électronique, avec renvoi au présent règlement**, à l'exception des normes relatives aux produits de signature électronique, dont les numéros de référence ont été publiés au Journal officiel des Communautés européennes.

Sont également publiés au Mémorial avec renvoi au présent règlement **la référence aux dispositifs sécurisés de création de signature électronique qui ont été certifiés conformes aux exigences définies au présent article par un organisme désigné à cet effet par un Etat membre de la Communauté européenne**. "

3) La création de la signature électronique



Le processus de vérification de l'intégrité du document électronique signé

1) Le dispositif de vérification de signature

Le dispositif de vérification de signature est essentiellement constitué par un logiciel qui met en application la donnée de vérification de la signature (à savoir la clé publique du signataire). Autrement dit, il permet de décrypter (de déchiffrer) la signature électronique (le cryptogramme) qui accompagne le document électronique[1)].

Sa finalité principale est de permettre au destinataire du document électronique de vérifier l'intégrité du document reçu.

2) Schéma explicatif

Concrètement, le destinataire du document électronique signé, ayant pris connaissance de la clé publique du signataire, procède au décryptage du condensé chiffré qui accompagne le document. Il obtient le condensé "en clair" (Etape n° 1). Comme la fonction de hachage est une fonction " irréversible ", il ne peut retrouver le message à partir du condensé et le comparer à celui reçu. Aussi l'étape suivante de la vérification de l'intégrité du document électronique consiste pour lui à appliquer à son tour la fonction de hachage au document électronique reçu (Etape n° 2). La comparaison des deux condensés permet de conclure à la préservation, ou non, de l'intégrité du document électronique (Etape n° 3).

Le document électronique accompagné de la signature électronique:

+

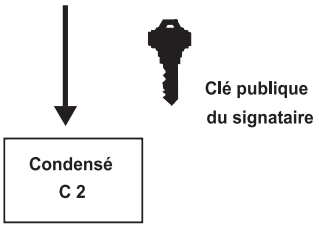
Condensé

Chiffré

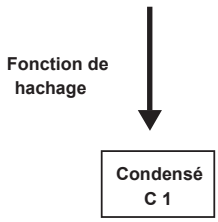
(= SE)

1) *Article 1 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique": " Au sens du présent règlement, on entend par: 5° Dispositif de vérification de signature: un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature.* "

Etape n° 1: mise en œuvre de la clé publique au moyen du dispositif de vérification de signature



Etape n° 2: application de la fonction de hachage au document électronique



Etape n° 3: comparaison des deux condensés obtenus à partir du document électronique

C 1 = C 2 ?

Si oui, alors l'intégrité du document électronique a été préservée. Si non, le document électronique a subi une altération.

C. Une signature électronique est un ensemble de données liées à l'acte, qui identifie le signataire

La signature électronique doit identifier la personne qui l'a " apposée " sur le document électronique.

Les éléments permettant d'identifier une personne sont en principe son nom et prénom pour une personne physique et sa dénomination sociale pour une personne morale. Cependant, plusieurs niveaux dans l'identification d'une personne sont concevables[1)]. On peut dire en fait qu'une personne est identifiée dès l'instant où elle seule est désignée, à l'exclusion de toute autre, par le procédé d'identification.

---

1) On pense par exemple à l'identification d'une personne par un pseudonyme.

Dans le cas visé par la loi, la signature électronique reposant sur la cryptographie asymétrique, il faut rechercher comment cette fonction d'identification est satisfaite.

Chaque paire de clés est unique et correspond à une seule personne déterminée. Par ailleurs, la signature électronique étant un cryptogramme qui ne peut être décrypté qu'au moyen de la clé publique correspondant à la clé privée du signataire, on peut donc dire, dans une certaine mesure, que ce dernier est identifié par sa clé publique[1)].

Toutefois, le destinataire du document ne peut faire seul, avec certitude, le lien entre cette clé publique et son titulaire: il ne sait pas (ou en tous les cas sans garantie), à partir d'une clé publique, qui est la personne qui a signé le document.

Il manque en quelque sorte un dernier maillon à la chaîne. Ce maillon, ce lien entre une clé publique et une personne (le signataire) est en fait réalisé par un certificat électronique qui est délivré au signataire, préalablement à la signature d'un document, par un prestataire de service de certification **(1)**.

Si l'article 1322-1 al. 3 C. civ. n'impose pas le recours au certificat électronique, la loi lui accorde une importance et un rôle particulier puisque seules " les signatures électroniques " reposant sur un certificat électronique qualifié sont présumées identifier le signataire. Pour les autres, il appartient à la partie qui s'en prévaut de démontrer qu'elles remplissent cette fonction d'identification[2)].

Enfin, l'examen de la fonction d'identification que doit remplir une signature électronique au sens de l'article 1322-1 al. 3 C. civ. invite à s'interroger sur l'hypothèse particulière du document électronique devant être signé par plusieurs personnes **(2)**.

1. Le prestataire de service de certification et la délivrance de certificats électroniques

Lien entre une personne et sa signature électronique, le certificat constitue le complément indispensable pour l'utilisation efficace de la signature électronique qui, contrairement à la signature manuscrite, ne contient pas *per se* d'éléments permettant de la rattacher à une personne plutôt qu'à une autre.

---

1) Bien sûr, le signataire peut avoir saisi ses nom et prénom à la fin du document électronique. Mais cette mention ne fournit aucune garantie, aucune sécurité quant à son origine.

2) On rappellera ici l'affaire précitée, jugée par le CSAS le 8 décembre 2003, où l'intimé contestait que " la signature électronique " invoquée identifie réellement le requérant et où les juges ont considéré qu'il revenait au requérant d'en apporter la preuve puisqu'il ne bénéficiait pas la présomption de l'article 18 al. 1 de la loi du 14 août 2000 relative au commerce électronique.

Ce certificat est délivré et géré par un prestataire de service de certification qui peut également fournir d'autres services liés aux signatures électroniques.

Le PSC[1)] est soumis à certaines obligations en raison de sa profession (obligation de secret professionnel et obligation de respect des dispositions régissant le traitement des données à caractère personnel), et éventuellement à certaines obligations supplémentaires en raison du type de certificat qu'il délivre[2)]. Ainsi des obligations complémentaires s'imposent à lui lorsqu'il émet un certificat électronique qualifié. Il en est de même lorsqu'il est accrédité[3)] car il offre alors des garanties supplémentaires à ses clients.

En pratique, un niveau de sécurité plus ou moins important correspond à chaque certificat, étant entendu que le certificat qualifié émis par un prestataire présente les garanties les plus élevées[4)].

2. Le cas particulier de la pluralité de signataires

Si un document électronique doit être signé par plusieurs personnes, la procédure exposée précédemment est répétée autant de fois que de signataires. Autrement dit, chaque signataire doit appliquer la fonction de hachage au document électronique, crypter le condensé obtenu au moyen de sa clé privée et y joindre son certificat électronique.

Au final, le document électronique sera accompagné d'autant de certificats électroniques et de condensés cryptés que de signataires.

D. Une signature électronique est un ensemble de données liées à l'acte, qui manifeste l'approbation du signataire au contenu de l'acte

La signature électronique doit enfin remplir une dernière fonction qui est de manifester le consentement de la personne à l'acte signé.

Cette fonction est considérée comme réalisée dés l'instant où une personne prend l'initiative de déclencher le processus de création de signature.

---

1) Voir les articles 19 à 33 de la loi du 14 août 2000 relative au commerce électronique.

2) Sur les obligations des prestataires de service de certification, voir les articles 19 à 30 (à l'exception de l'article 21) de la loi du 14 août 2000 relative au commerce électronique.

3) Sur l'accréditation des prestataires de service de certification, voir les articles 30 à 33 de la loi du 14 août 2000 relative au commerce électronique. L'autorité d'accréditation est l'OLAS (Office Luxembourgeois d'Accréditation et de surveillance). A ce propos, voir http://www.olas.public.lu

4) Article 1 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique":
" 7° Certificat qualifié: un certificat qui satisfait aux exigences visées à l'article 2 du présent règlement et qui est fourni par un prestataire de service certification satisfaisant aux exigences de l'article 3 du présent règlement. "

La fonction d'adhésion pose cependant quelques difficultés particulières dans le cadre d'un document électronique. En effet, elle implique que le signataire voit effectivement le contenu de l'acte qu'il veut signer. Or s'agissant d'un document électronique, ce que le signataire voit à l'écran peut ne pas être ce qu'il s'apprête à signer. Il existe également un autre risque, inconnu dans le monde des signatures manuscrites, qui est celui d'une signature électronique " involontaire " qui serait " apposée " automatiquement sous l'action par exemple d'un virus.

En conséquence, il est nécessaire que des garanties en terme de sécurité soient apportées par l'équipe technique en charge du parc informatique des organismes de sécurité sociale afin de prévenir de tels risques.

IV. QUE VAUT UNE SIGNATURE ÉLECTRONIQUE?

Notre propos se limitera à l'hypothèse où une signature est exigée pour la preuve d'un document électronique puisque la loi n'a reconnu expressément pour l'instant la signature électronique que dans ce cadre précis.

Il est important tout d'abord de dire que la loi n'exige pas toujours que la preuve soit rapportée devant le juge par un document signé[1)].

Il faut en effet distinguer si l'objet de la preuve est un fait[2)] ou un acte juridique[3)]. En d'autres termes, le document en question constate-t-il un fait juridique (se contente-t-il par exemple de relater un accident) ou constate-t-il un acte juridique? Dans le premier cas, la preuve est libre et il n'est pas nécessaire que le document qui relate le fait juridique soit revêtu d'une quelconque signature pour être recevable en tant qu'élément de preuve. Dans le second cas par contre, cela dépendra (principalement) de la valeur en litige. Si l'acte juridique porte sur une valeur supérieure à 2 500 euros, alors le document qui le constate devra être signé par la ou les parties qui se sont engagées sous peine d'être rejeté pour irrecevabilité. Sinon une telle démarche ne sera pas nécessaire.

Précisons encore que dans les cas où la preuve est libre (système de la preuve libre), le juge n'est pas lié par les éléments de preuve qui lui sont soumis et apprécie souverainement leur valeur juridique, tandis que dans les cas où la loi exige un document signé (système de la preuve légale), le juge

---

1) Quelques définitions utiles relativement à la problématique de la preuve:

- *Recevabilité: un mode de preuve est dit recevable lorsque la loi autorise son utilisation dans l'espèce considérée;*
- *Force probante: la force probante d'un mode de preuve s'entend de son potentiel de conviction, de son efficacité.*

2) Un fait juridique est tout fait, toute circonstance produisant des conséquences juridiques.

3) Un acte juridique est toute manifestation de volonté en vue de produire des effets de droit.

est lié par le document signé qui lui a été apporté et ce dernier constitue une preuve parfaite de l'acte juridique qui fait l'objet du litige.

Cependant, il est bien évident qu'un juge sera enclin à être davantage convaincu par l'élément de preuve qui lui est soumis lorsque ce dernier présente d'importantes garanties quant à son origine et son intégrité - ce qui est le cas des documents signés. C'est pourquoi la question de la valeur juridique de la signature électronique dépasse le seul cadre des hypothèses où la loi exige la présentation au juge d'un document signé en guise de preuve.

Aussi, dans le système de la preuve libre, une signature électronique vaut ce que le juge veut bien lui reconnaître, c'est-à-dire preuve complète ou simple indice ou encore… rien du tout.

Il n'y a donc véritablement d'intérêt présentement de traiter de la question de la valeur juridique de la signature électronique que dans l'hypothèse où on se trouve dans le système de la preuve légale.

Dans le cadre de ce système, le document électronique revêtu d'une signature électronique répondant à la définition légale donnée par l'article 1322-1 al. 3 C. civ. vaut preuve parfaite et lie le juge. Examinons donc comment il est possible d'obtenir une telle preuve ainsi que les conséquences juridiques lorsque le demandeur à la preuve ne peut présenter au juge cette preuve parfaite.

Si la loi du 14 août 2000 relative au commerce électronique a consacré la signature électronique, toutes les " signatures électroniques " d'un point de vue technique ne présentent pas le même degré de fiabilité. Comme il serait bien difficile à un plaideur d'apporter la preuve positive que telle " signature électronique " (considérée du point de vue technique) répond à la définition de la signature électronique (du point de vue juridique) de l'article 1322-1 al. 3 C. civ., le législateur lui est venu en aide en posant une présomption (simple[1)]). Sont présumées constitutives d'une signature électronique au sens de l'article 1322-1 al. 3 C. civ. les " signatures électroniques " qui sont créées par un dispositif sécurisé de création de signature que le signataire peut garder sous son contrôle exclusif et qui reposent un certificat qualifié (Article 18 al. 1 de la loi du 14 août 2000 relative au commerce électronique).

Pour les autres " signatures " par contre, la partie qui s'en prévaut doit apporter la preuve (difficile) qu'elles satisfont aux conditions posées par l'article 1322-1 al. 3 C. civ. On soulignera à ce propos un important texte de la loi du 14 août 2000 relative au commerce électronique (article 18 al. 2) qui garantit que le juge auquel un document revêtu d'une telle signature est soumis, ne le rejettera pas pour le seul motif que la signature se présente

---

1) Lorsqu'une présomption est simple, la preuve contraire peut en être rapportée par tout moyen.

sous forme électronique, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

Dans le cas enfin où le plaideur ne dispose pas d'un document revêtu d'une " signature électronique " reconnue comme répondant à la définition donnée par l'article 1322-1 al. 3 C. civ., il doit en principe être considéré comme ayant échoué dans sa tâche probatoire et donc supporté le risque de la preuve. Il doit voir en conséquence sa prétention rejetée par le juge.

Un tel sort serait néanmoins bien sévère, a estimé le législateur qui a prévu un certain nombre d'exceptions (articles 1347 et 1348 C. civ.) dont l'intérêt est d'autoriser la partie à prouver librement l'acte juridique litigieux. On verra en fait que seule l'exception prévue par l'article 1347 C. civ. (le commencement de preuve par écrit) peut être d'une réelle utilité s'agissant de la preuve d'un acte juridique constaté par un document électronique.

L'article 1348 C. civ. prévoit trois situations autorisant le demandeur à la preuve à prouver par tout moyen l'acte juridique dont il se prévaut. Il y a le cas où une preuve parfaite (un écrit signé au sens des articles 1322 à 1322-2 C. civ.) a été établie mais a été perdue à la suite d'un cas fortuit ou de force majeure. Cette hypothèse ne nous est d'aucune utilité ici puisque précisément nous nous trouvons dans le cas où aucun écrit signé n'a été réalisé. L'article 1348 C. civ. envisage ensuite le cas où il a été impossible d'établir un écrit signé soit en raison d'une impossibilité matérielle, soit en saison d'une impossibilité morale. Or il ne peut être question d'une impossibilité matérielle lorsque les parties se sont elles-mêmes placées dans cette situation, ce qui est le cas dans notre hypothèse puisque la ou les parties ont fait le choix de recourir à un support électronique pour constater un acte juridique. De même, il ne peut être question d'une impossibilité morale car cette dernière suppose soit l'existence de liens d'affection ou de confiance particuliers entre les parties, soit un usage en raison de leur appartenance à telle profession qui les dispenserait d'établir une preuve parfaite des actes juridiques dont elles conviennent. Or force est de constater que rien de tel ne se rencontre dans notre cas.

Reste donc l'article 1347 C. civ. qui prévoit le cas où la partie qui se prévaut de l'acte juridique litigieux dispose d'un commencement de preuve par écrit, c'est-à-dire d'un écrit émanant de la partie à laquelle il est opposé et qui rend vraisemblable le fait allégué. Le texte pose trois conditions pour qu'un document puisse être qualifié de commencement de preuve par écrit. La première est que ce document soit un écrit quelconque (c'est-à-dire non signé ou tous les cas pas revêtu d'une signature répondant aux définitions de l'article 1322-1 C. civ.). Depuis la réforme opérée dans le Code civil par la loi du 14 août 2000 relative au commerce électronique, un document électronique peut être qualifié d'écrit quelconque au sens de l'article 1347 C.

civ. puisque la notion d'écrit en général a été détachée de toute référence à un support en particulier. Ensuite, le document électronique doit rendre vraisemblable le fait allégué par celui qui s'en prévaut. Tout dépend donc de son contenu. Par ailleurs, cette condition étant laissée à l'appréciation souveraine des juges du fond, nous n'en dirons pas plus si ce n'est qu'elle est également susceptible d'être satisfaite par un document électronique. Enfin, le document électronique doit émaner de la partie à laquelle il est opposé. Cette dernière condition est celle qui pose le plus de difficultés dans l'hypothèse où le document électronique a été établi par un organisme de sécurité sociale qui s'en prévaut ensuite devant le Conseil arbitral des assurances sociales. En effet, dans un tel cas, le document électronique ne pourra valoir commencement de preuve par écrit parce qu'il n'émane pas de l'assuré auquel l'organisme entend l'opposer. En réalité, un document électronique présenté par un organisme de sécurité sociale comme élément de preuve dans le cadre d'un procès l'opposant à un assuré ne pourra être qualifié de commencement de preuve par écrit que dans l'hypothèse où il émane de l'assuré et non dans celle où il a été établi pas l'organisme lui-même.

Enfin, dans le cas où un document électronique serait reconnu par le juge comme valant commencement de preuve par écrit, il appartient encore à l'organisme de sécurité sociale de prouver par tout moyen **extérieur** à ce document l'acte juridique dont il se prévaut. Il est en effet très important de souligner que le commencement de preuve par écrit ne se suffit jamais à lui-même: il ne vaut pas preuve de l'acte juridique litigieux et doit toujours être complété. Aussi, l'organisme de sécurité sociale devra faire face à une dernière difficulté qui est celle de trouver à présenter au juge un autre élément de preuve établissant l'existence de l'acte juridique en question.

Tableaux récapitulatifs concernant la valeur juridique d'une signature électronique

Tableau n° 1

	Valeur juridique du document électronique signé
Système de la preuve libre: **- le document constate un acte juridique et porte sur une valeur inférieure ou égale à 2 500 euros** **OU** **- le document constate un fait juridique**	**- recevabilité: OUI** **- force probante: elle est laissée à l'appréciation souveraine des juges du fond**

Tableau n° 2

Système de la preuve légale:

Le document constate un acte juridique portant sur une valeur supérieure à 2 500 euros

	Valeur juridique du document électronique signé
Le document électronique est signé au moyen d'une signature électronique: **- qui bénéficie de la présomption de l'article 18 de la loi du 14/08/2000** **OU** **- dont il a été démontré qu'elle satisfait à la définition de l'article 1322-1 al. 3 C. civ.**	**- recevabilité: OUI** **- force probante: le document électronique vaut preuve parfaite et le juge est lié par cette preuve**
Le document électronique est signé au moyen d'une "signature électronique" qui ne répond pas à la définition de l'article 1322-1 al. 3 C. civ.	**- recevabilité: OUI si le document peut être qualifié de commencement de preuve par écrit / SINON: le document est irrecevable en tant qu'élément de preuve et il n'a aucune valeur juridique** **- force probante: le document électronique qualifié de commencement de preuve par écrit doit être complété par tout moyen de nature à prouver l'acte juridique allégué**

L'archivage électronique sécurisé

Corentin POULLET

Chercheur
Laboratoire de Droit Economique
Centre de Recherche Public Gabriel Lippmann

I. INTRODUCTION

Dans le cadre de leurs missions, les organismes de sécurité sociale (OSS) luxembourgeois génèrent régulièrement des documents et ils en reçoivent tout aussi fréquemment de leur assurés sociaux. Ces documents doivent, en principe, être conservés pendant une période plus ou moins longue afin de préserver les informations contenues dans les documents et de constituer des éléments de preuve en vue de prévenir des contestations ultérieures. Une telle conservation est assurée depuis toujours par les OSS en suivant des procédures et méthodes bien définies au fil des ans. Ces méthodes varient selon les fonctions dévolues à chaque organisme: classement individuel, classement chronologique, etc.[1)] Elle s'est avérée précieuse à de multiples reprises: en matière de contentieux administratif, la charge de la preuve est partagée entre les parties et le plus simple reste pour l'OSS de produire devant le juge le document initial indexé.

Mais, l'archivage traditionnel sur support papier présente des inconvénients majeurs: il mobilise une grande superficie, un personnel abondant[2)] et surtout il interdit toute simultanéité dans l'accès au dossier lors de son traitement.

---

1) *Pour une présentation des méthodes traditionnelles d'archivage, voir: D. PONSOT, " Valeur juridique des documents conservés sur support photographique ou numérique ",* Rapport à l'Observatoire Juridique des Technologies de l'Information, *septembre 1995, La Documentation Française, p. 4.*

2) *Voir notamment sur ce point l'exposé des motifs du projet de loi n° 5161 portant modification de la loi du 12 février 1999 portant création d'un congé parental et d'un congé pour raisons familiales, la loi modifiée du 19 juin 1985 concernant les allocations familiales et portant création de la caisse nationale des prestations familiales, la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel déposé le 20 mai 2003, Doc. Parl. 5161/0. Ce texte précise que* " l'espace actuellement occupé par les archives de la caisse *[nationale de prestations familiales]* se chiffre à près d'1,4 km de rangées et n'est plus extensible sauf recours à des réserves externes au bâtiment occupé par la caisse. Le besoin en personnel pour gérer ces archives et pour assurer la circulation des dossiers, calculé à l'occasion de l'audit auquel la caisse a fait procéder en 1998, se chiffre à 6 postes à temps plein ".

Il n'est dès lors pas surprenant que ces mêmes OSS s'intéressent particulièrement aujourd'hui à l'archivage électronique sécurisé qui peut être défini comme un procédé dynamique permettant de conserver, à moyen ou long terme et de manière fiable, des informations sur support électronique afin de pouvoir les exploiter à tout moment.[1)]

L'avènement de la société de l'information, caractérisé par une multiplication des documents sous forme dématérialisée, un accroissement des capacités de stockage et une fluidité inégalée du transfert d'informations expliquent en partie cette démarche tant il est vrai que les possibilités en terme d'archivage sont désormais décuplées. A cela, s'ajoutent les avantages indéniables procurés par la gestion électronique de documents, à savoir un gain de temps en terme de recherche de l'information, la possibilité de consulter à plusieurs un même document archivé électroniquement, une sécurité accrue, une plus grande efficacité des contrôles et des processus d'acheminement. Il ne faut pas non plus oublier la volonté politique de parvenir progressivement à une administration électronique.[2)] Sa réussite repose notamment sur la capacité des OSS à traiter les besoins de chaque assuré dans le cadre d'échanges électroniques sécurisés, tout en respectant sa vie privée.

Toutefois, l'archivage électronique n'est pas la panacée. Les technologies en perpétuelle évolution ne garantissent pas forcément la stabilité et la lisibilité future des données conservées électroniquement. La consultation ultérieure de ces données nécessite pourtant qu'elles puissent être retrouvées, traduites par un système automatisé (e.g. une application informatique) et lues par l'oeil humain.[3)] En pratique, il convient d'archiver correctement le document sous forme électronique de sorte qu'il soit intelligible et qu'il puisse être retrouvé intact à tout moment, et cela indépendamment d'un éventuel transfert de support.

L'ensemble de ces préoccupations nous amène à une réflexion sur les procédures et méthodes de conservation qui devraient gouverner tout archivage électronique sécurisé de documents.

---

1) On note que la norme ISO 15489 définit le système d'archivage comme un " système d'information qui intègre les documents, les organise, les gère et les rend accessibles à terme " (chapitre 3, termes et définitions, 3.17).

2) Voir le plan d'action " e-Luxembourg " présenté par le ministre des communications au Conseil de Gouvernement du 26 janvier 2001 et disponible à l'adresse suivante: http://www.eluxembourg.lu/eLuxembourg/documents_de_base/eLuxembourg_.pdf
Voir également pour la France: G. CHATILLON, " L'administration électronique: enjeux pratiques, défis juridiques ", Cahiers Lamy droit de l'informatique et des réseaux, n° 167, Mars 2004, pp 8-14.

3) Sur les garanties de lisibilité et d'intelligibilité des données conservées électroniquement, voir: Th. PIETTE-COUDOL, " Conservation et archivage de l'écrit sous forme électronique ", Communication Commerce Electronique, Mai 2002, p. 12.

En l'absence de loi spécifique, le droit luxembourgeois appréhende ce procédé par diverses normes législatives et réglementaires.[1] On pense notamment aux articles 1322-2, 1333, 1334, 1348 du Code civil et 11 du Code de commerce, au règlement grand ducal du 22 décembre 1986 pris en exécution de l'article 1348 alinéa 2 du Code civil et de l'article 11 du Code de commerce[2], aux règlements grand ducaux du 12 mai 1975 portant organisation et fonctionnement du centre d'informatique, d'affiliation et de perception des cotisations commun aux institutions de sécurité sociale [3] et du 22 décembre 1989 concernant la comptabilité et les comptes annuels des organismes de la sécurité sociale et du fonds national de solidarité[4] ainsi qu'au projet de loi n° 5161[5].

Ces dispositions permettent d'apporter des éléments de réponse à la question essentielle de savoir comment assurer la fidélité et la durabilité de l'information conservée?[6] Pour le juriste, il s'agit de résoudre deux difficultés: d'une part, comment conserver la même valeur probante au document initialement établi sur support papier et au document archivé électroniquement (II) et, d'autre part, comment conserver dans le temps de la valeur probante du document électronique (III).

II. COMMENT CONSERVER LA VALEUR PROBANTE DU DOCUMENT SUR SUPPORT PAPIER À ARCHIVER?

L'enjeu juridique premier de l'archivage électronique sécurisé d'un document initialement établi sur support papier est de donner au document archivé la même valeur sur le plan de la preuve que celle du document initial.

Sur le terrain du droit, la problématique est complexe car la nature juridique des documents initialement établis sur support papier va déterminer le régime de la preuve qui s'y applique et leur valeur probante subséquente (A). La tâche est d'autant plus malaisée que des règles particulières sont parfois

---

1) *Pour une analyse fouillée des normes internationales relatives à l'archivage électronique, voir R. VUITTON, " Environnement juridique de l'archivage et de la gestion électronique de documents ", cette revue.*

2) *Mémorial A, n° 108, du 30/12/86, p. 2748.*

3) *Mémorial A, n° 32, du 04/06/75, p. 701.*

4) *Mémorial A, n° 87, du 30/12/89, p. 1726.*

5) *Doc. Parl. 5161/0.*

6) *Cette double difficulté est qualifiée par Philippe Bazin comme le " syndrome de Champollion “ chez les juristes. Cet auteur précise qu' " on désigne par-là une double crainte: celle de perdre les codes de déchiffrement du document, comme la manière de déchiffrer les hiéroglyphes égyptiens avait été perdue au fil du temps, et celle de perdre le document électronique tout court, qui est propre au document électronique " (in Ph. BAZIN, " approche juridique de l'archivage électronique ", Cahiers Lamy droit de l'informatique et des réseaux, n° 167, Mars 2004, pp 2-4.*

prévues lorsque le document initial vient à disparaître (B). Il est néanmoins permis de s'interroger plus globalement sur les conditions et les modalités à respecter lors de tout archivage électronique sécurisé (C).

A. Quelle est la valeur probante du document à archiver?

La première étape de tout archivage électronique sécurisé consiste à étudier la valeur probante du document établi initialement sur support papier.

Pour cela, il faut commencer par déterminer la nature juridique de ce dernier: s'agit-il d'un document administratif ou non?

La question est d'importance car le droit administratif admet le système de la preuve libre tandis que le droit civil adopte pour les actes juridiques le système de la preuve légale en vertu duquel un acte juridique doit être prouvé par écrit et les différents moyens de preuve n'ont pas la même force probante.

Le régime administratif de la preuve diverge également sensiblement des règles du code civil et du code de commerce: " *si le régime administratif de la preuve fait en premier lieu peser le fardeau de la preuve sur le demandeur, lequel doit effectivement combattre et démentir le contenu et la légalité de l'acte administratif critiqué, il n'en reste pas moins que l'administration, c'est-à-dire la partie défenderesse, ne saurait rester purement passive* "[1)] Ainsi, lorsqu'une administration détient les pièces ou les informations nécessaires à la connaissance de la vérité ou lorsqu'elle a pris l'initiative de l'acte soumis au contrôle du juge, sa collaboration est exigée pour l'établissement des preuves.

Cette distinction n'est toutefois pas absolue car " *le droit administratif au sens de droit des relations entre personnes publiques et personnes privées est un droit composite qui pour partie emprunte au droit privé, à ce qu'il est convenu d'appeler le droit commun, et pour partie déroge à ce droit* "[2)]. Il faut, en effet, noter que les règles du code civil s'appliquent entièrement aux contrats de l'administration[3)] et à titre supplétif aux contrats administratifs[4)] sous réserve qu'elles ne soient pas incompatibles avec la nature spécifique de l'action administrative.

---

1) *TA 20-02-04 (n° 15278, X contre le règlement grand-ducal du 28 mars 2002 déclarant zone protégée la réserve naturelle " Wëngertsbierg ").*

2) *Voir: J.C. VENEZIA, " le droit administratif français est-il encore dérogatoire au droit commun? " in* Etat, Loi, Administration - Mélanges Ep. Spiliotopoulos*, Bruylant, Bruxelles, 1998, p. 453.*

3) *Contrats entre une personne et une administration dans lesquels la personnalité de droit public de l'administration importe peu.*

4) *Contrats entre une personne et une administration dans lesquels l'administration agit en tant que puissance publique et utilise son pouvoir de commandement.*

Le Code civil offre ainsi un support intéressant pour réfléchir sur l'archivage électronique sécurisé de documents.[1)]

B. Les règles de preuve du Code civil et l'archivage électronique sécurisé

Aux termes du code civil, l'acte juridique que constitue le document initial peut être soit un acte sous seing privé (ce qui suppose l'apposition d'une signature)[2)], soit une simple copie du document original[3)], soit un commencement de preuve par écrit à la double condition qu'il émane de celui contre lequel la demande est formée ou de celui qu'il représente, et qu'il rende vraisemblable le fait allégué[4)], soit une présomption[5)].

La remarque est importante car la valeur probante du document initialement établi sur support papier diffère sensiblement:

- L'acte sous seing privé vaut comme original.
- La simple copie fait foi uniquement de ce qui est contenu au titre original s'il subsiste.[6)]
- Le commencement de preuve par écrit autorise seulement la partie qui s'en prévaut à déroger aux règles des articles 1341 et suivants du Code civil.
- Les présomptions de l'homme sont abandonnées aux lumières et à la prudence du magistrat.[7)]

Cette disparité n'est pas sans conséquences dans le cadre de l'archivage électronique sécurisé attendu que le caractère original d'un document initialement établi sur support papier n'est jamais préservé en raison du transfert de support réalisé.

Il convient dès lors de vérifier si le document initial et le document archivé conservent la même valeur probante.

Dans les trois derniers cas, le législateur n'a rien prévu à ce propos. Par contre, lorsque le document initial est un acte sous seing privé, il a prévu deux dispositions spéciales visant à garantir au document archivé la même valeur probante que le document initial.

---

1) Voir également la théorie générale de l'acte juridique, D. ALLAND et St. RIALS, Dictionnaire de la culture juridique, PUF, Paris, 2003, p. 8.

2) Voir l'article 1322-1 al. 1 du Code civil.

3) Voir l'article 1333 du Code civil.

4) Voir l'article 1347 du Code civil.

5) Voir l'article 1349 du Code civil.

6) Il faut rappeler qu'il peut toujours être exigé la représentation de ce titre ou de cet acte.

7) Voir l'article 1353 du Code civil.

Si le document initialement établi sur support papier subsiste, le document archivé électroniquement constitue une simple copie du document initial faisant foi du contenu de ce dernier.[1)] Une valeur probante identique est - pour ainsi dire - subordonnée à la subsistance de l'original.

S'il a disparu, le Code civil contient plusieurs dispositions visant à assurer la même valeur probante aux documents initialement établis sur support papier et aux documents archivés.

L'article 1348 du Code civil concerne la perte du titre qui servait de preuve littérale par suite d'un cas fortuit ou d'une force majeure. On pense notamment à un incendie dans un lieu de stockage de documents originaux établis sur support papier. En cette hypothèse de disparition fortuite, les règles classiques en matière de preuve sont écartées et la preuve testimoniale est admise.

L'article 1334 du Code civil vise en outre l'hypothèse où le document a été détruit mais qu'il subsiste une copie fidèle. Tel serait, par exemple, le cas d'un acte sous seing privé détruit après un archivage électronique sécurisé. Il énonce en effet que " *lorsque le titre original ou l'acte faisant foi d'original au sens de l'article 1322-2 n'existe plus, les copies effectuées à partir de celui-ci, sous la responsabilité de la personne qui en a la garde, ont la même valeur probante que les écrits sous seing privé dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisée dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand ducal* ". Outre la destruction du document initial, le législateur impose donc trois conditions cumulatives pour que le document initial ayant disparu et sa copie ait une même valeur probante.

i) Il faut tout d'abord que la copie soit " *effectuée sous la responsabilité de la personne qui en a la garde* ".

Une telle exigence implique l'identification précise d'une personne identique ayant pour mission de reproduire le document initialement établi sur support papier et de le conserver.[2)]

---

1) Voir l'article 1333 du Code civil.

2) Voir sur ce point: V. GAUTRAIS, Le contrat électronique international: encadrement juridique, Bruylant, Bruxelles, 2001, p. 114. Cette auteur souligne que " l'intervention d'un trop grand nombre de personnes et la perte de confidentialité qui en découlerait, sont des éléments nuisant à la fiabilité du traitement des documents ".

Conformément au Code civil, cette personne pourrait être soit l'organisme lui-même, soit un employé désigné en son sein, soit un tiers de confiance qu'il choisit[1)].

ii) Il faut ensuite que la copie ait été " *réalisée dans le cadre d'une méthode de gestion régulièrement suivie* ".

Une telle exigence suppose l'adoption d'une " politique " en matière d'archivage électronique sécurisé. Sa définition nécessite souvent une démarche préalable d'analyse du patrimoine documentaire de l'organisme[2)], de la structure de gestion utilisée[3)] et des obligations légales en matière de conservation des documents[4)]. Elle requiert au minimum une définition des supports et modes d'archivage retenus ainsi que des modalités de mise en œuvre de cet archivage. Elle doit notamment formaliser le processus d'archivage dans un document de spécifications. A cet égard, la norme ISO 15489 recommande l'élaboration d' " une charte d'archivage " regroupant aussi bien les aspects techniques que juridiques, organisationnels et pratiques.[5)]

Par ailleurs, une maintenance et une veille technologique sont nécessaires pour adapter cette méthode de gestion aux évolutions techniques et autres qui surviennent.

Il faut enfin signaler le rôle dévolu au centre d'informatique, d'affiliation et de perception des cotisations commun aux OSS.[6)]

iii) Il faut enfin que la copie réponde " *aux conditions fixées par règlement grand ducal* ".

L'idée est de prévoir par voie réglementaire un certain nombre de conditions techniques, procédurales et organisationnelles pour qu'une copie puisse être considérée comme fidèle au sens de l'article 1334 du Code civil.

---

1) Certains auteurs préconisent l'intervention d'un " tiers archiveurs ", voir sur ce point: S. LIPOVETSKY et F. PERBOST, " L'archivage des documents dématérialisés ", http://www.legalbiznext.com, 08/02/02. Voir également sur cette problématique: E. CAPRIOLI, " Variations sur le thème du droit de l'archivage dans le commerce électronique ", Petites affiches, 18 août 1999, n° 164, pp. 4 et ss. Sur le statut du " tiers archiveur " en droit belge, voir: M. DEMOULIN et D. GOBERT, " l'archivage dans le commerce électronique: comment raviver la mémoire ", Commerce électronique de la théorie à la pratique, Cahiers du CRID, n° 23, Bruylant, Bruxelles, 2003, pp. 123 et ss.

2) Il conviendrait par exemple d'étudier l'origine, l'utilisation et la destination des documents à archiver.

3) La définition de la politique d'archivage est en principe consécutive à la détermination, au sein d'une infrastructure à clé publique, d'une politique de certification, d'une politique de signature, d'une politique de confidentialité et d'une politique d'horodatage.

4) On pense notamment aux délais de prescription.

5) Voir sur ce point: C. PIERRE-BEAUSSE, " Le point sur les principaux moyens de preuve électronique en droit luxembourgeois ", Ann. Dr. Lux., 2002, p. 352.

6) Voir le règlement grand ducal du 12 mai 1975, précité.

Bien qu'aucun règlement grand ducal spécifique n'ait été adopté en exécution de cette disposition, l'article 14 de la loi relative au commerce électronique[1] précise que " *le règlement grand-ducal du 22 décembre 1986, pris en exécution de l'article 1348 du Code civil, continue à produire ses effets sur la base de l'article 13 de la présente loi [modifiant l'article 1334 du Code civil]* ". On en déduit que le règlement grand ducal du 22 décembre 1986[2], s'applique désormais à la copie fidèle.[3] L'enregistrement électronique reproduisant l'original doit donc respecter les exigences du règlement à savoir être (a) la copie fidèle et durable du document original ou de l'information à l'origine de l'enregistrement, (b) effectué de façon systématique et sans lacune, (c) réalisé selon des instructions de travail conservées aussi longtemps que les reproductions ou enregistrements, (d) conservé avec soin, dans un ordre systématique, et protégé contre toute altération, et (e) conforme aux exigences particulières propres aux programmes d'enregistrements informatiques.

a) La première condition concerne la fidélité à l'original et la durabilité de la copie.

Il s'agit d'une condition d'ordre technique relative aux méthodes de reproduction utilisées et au support qui vise à assurer une conservation dans le temps d'une copie sincère.

Le caractère fidèle de la copie s'apprécie en fonction de l'original. " *Du point de vue pratique, la meilleure manière de réaliser une copie fidèle d'un original implique de limiter au maximum l'interprétation qui est faite de l'original par le système informatique* "[4].

Le caractère durable de la copie doit être entendu raisonnablement dans la mesure où aucun support n'est à l'abri d'une altération à travers le temps. Lors de l'adoption du texte en 1986, l'idée était d'éviter l'utilisation de supports réinscriptibles (notamment les supports magnétiques) permettant d'effacer et de réenregistrer les données. En principe, sont ainsi exclus les disquettes, les clés USB, les CD-RW et les DVD-RW. A l'époque, le règlement entendait favoriser les supports de type WORM[5] qui permettent d'enregistrer une seule fois mais de lire plusieurs fois les données. Il pose ainsi la présomption suivant laquelle " *est réputée durable toute reproduction indélébile de l'original et tout*

---

1) Précitée.

2) Précité.

3) L'intention du législateur ne fait en effet aucun doute en dépit d'un procédé législatif contestable et d'une formulation discutable. Il faut en effet noter que l'article premier du règlement grand ducal (modifié par une loi) vise " les reproductions et enregistrements visés à l'article 1348 du Code civil ". Or, le deuxième alinéa de cette disposition a été supprimé par l'article 13 de la loi relative au commerce électronique.

4) Voir : C. PIERRE-BEAUSSE, précité, p. 351.

5) Acronyme anglais pour " Write Once Read Many ".

enregistrement qui entraîne une modification irréversible du support ". On pense notamment aux CD-R et aux DVD-R. Des disques optiques dont la surface est gravée de manière indélébile et non-réinscriptible à l'eau forte. Ces supports présentent l'avantage d'avoir une durée de conservation sensiblement plus longue que celles des supports magnétiques.

Toutefois, la formulation technologiquement neutre du règlement permet de prendre aujourd'hui en considération les supports réinscriptibles si la technique d'archivage utilisée permet de garantir l'intégrité du document à travers le temps au moyen par exemple d'une signature électronique.

b) La seconde condition porte sur la systématisation de la conservation.

Il s'agit d'une condition d'ordre organisationnel qui vise à assurer une diligence particulière dans la conservation des copies.

Aucune lacune n'est admise dans l'enregistrement électronique. Les précautions à prendre doivent avoir été préalablement définies dans un document reprenant la politique en matière d'archivage électronique sécurisé. Elles doivent ensuite être appliquées systématiquement et minutieusement pour assurer la régularité de l'enregistrement.

c) La troisième condition a trait aux instructions de travail nécessaires à la copie devant être conservées aussi longtemps que les enregistrements.

Il s'agit d'une condition d'ordre procédural qui entend permettre une vérification du respect de l'ensemble du processus d'archivage.

Les différentes phases de la reproduction doivent s'opérer strictement selon le schéma arrêté, aux instructions de travail et sous la surveillance du responsable de la conservation. En fait, il convient de démontrer que "*l'opération d'enregistrement des données s'est effectuée correctement et ceci à toutes les étapes de son traitement*"[1)]. Cela suppose, selon nous, que les opérations techniques effectuées lors de tout enregistrement électronique sur un document puissent être retrouvées. L'archivage électronique sécurisé de chaque document pourrait par exemple faire l'objet d'un procès verbal contenant les indications suivantes: la nature et l'objet du document initial, le numéro du document archivé, la date de l'opération, le nom du responsable de la garde, une déclaration que les documents ont été saisis de façon complète, régulière et sans altération signée par le responsable de la conservation.

---

1) Voir: V. SEDAILLAN, " L'archivage de l'acte électronique ", www.juriscom.net, 8 juillet 2002.

d) La quatrième condition intéresse l'indexation et l'exactitude des données conservées.

Il s'agit d'une condition d'ordre essentiellement technique relative aux données conservées qui a pour but d'assurer la pérennité de l'accès aux documents archivés et l'intégrité des données conservées[1)].

L'objectif est de permettre une consultation ultérieure du document archivé avec la garantie que les données qu'il contient n'ont pas été modifiées.[2)] Cela présuppose une protection des copies contre toute altération. La loi québécoise contient, à cet égard, deux éclairages importants: elle précise, d'une part, que " l'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction[3)] " et, d'autre part, que " dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie "[4)].

e) La cinquième condition est le respect des exigences particulières propres aux programmes d'enregistrements informatiques.

En plus de ces quatre conditions générales, le règlement grand ducal du 22 décembre 1986[5)] énonce toute une série de conditions particulières en ce qui concerne les applications informatiques permettant d'enregistrer un document.

La personne ayant la garde des données enregistrées doit tout d'abord pouvoir démontrer la concordance de ces données avec celles qui auraient été transférées sur un autre support informatique, quelle qu'en soit la raison.

Cette personne doit aussi être en mesure de communiquer à tout moment la documentation du programme, les descriptions des fichiers et les instructions des programmes tant que les copies auxquels ils se réfèrent subsistent.

Ces documents doivent parallèlement être régulièrement mis à jour et rendu immédiatement lisible.

---

1) La norme française NF Z42-013 définit cette intégrité comme la " caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification ".

2) Il est intéressant de noter qu'au sens de la législation québécoise, le concept d'intégrité recouvre la possibilité de vérifier que l'information du document n'est pas altérée, qu'elle est maintenue dans son intégralité et que le support sur lequel elle est stockée lui procure la stabilité et la pérennité voulue (Voir l'article 6, alinéa premier de la loi québécoise concernant le cadre juridique des technologies de l'information, L.Q. 2001, c. 32).

3) Voir l'article 6, alinéa 2, de la loi québécoise concernant le cadre juridique des technologies de l'information, précitée.

4) Voir l'article 6, alinéa 3, de la loi québécoise concernant le cadre juridique des technologies de l'information, précitée.

5) Précité.

Les systèmes informatiques doivent enfin " *comporter les sécurités nécessaires pour éviter une altération des enregistrements* " et " *permettre de restituer à tout instant les informations enregistrées sous une forme directement lisible* "[1)].

***

Lorsque les trois conditions cumulatives de l'article 1334 du Code civil sont réunies, le document archivé est présumé être une copie fidèle de l'écrit sous seing privé dont il est la copie. Il possède dès lors la même valeur probante que ce dernier.

Cette présomption n'est toutefois pas irréfragable: la preuve contraire est admise. Il appartient néanmoins à la personne qui entend renverser la présomption de rapporter cette preuve contraire.

Il faut finalement noter que les conditions fixées par le règlement grand ducal du 22 décembre 1986[2)] ne jouent que pour la présomption de copie fidèle au sens de l'article 1334 du Code civil. La question de la conservation de la valeur probante des copies simples, des commencements de preuve par écrit et des présomptions reste par conséquent ouverte.

C. Quelles sont les conditions et les modalités à respecter lors de tout archivage électronique sécurisé?

Les (trop) rares interventions législatives[3)] pour assurer une même valeur sur le plan de la preuve aux documents initialement établis sur support papier et aux documents archivés électroniquement à partir de ces derniers, ne signifient pas pour autant qu'aucune règle ne s'applique à l'archivage électronique sécurisé d'un acte administratif unilatéral ou à un commencement de preuve par écrit.

Au contraire, tout archivage électronique sécurisé doit respecter un certain nombre de conditions sous peine de voir la valeur probante d'un document archivé être moindre que celle du document initial. Le silence relatif du législateur ne doit pas éclipser l'enjeu essentiel sous-jacent à tout archivage que constitue la fidélité dans le temps de l'information conservée. A défaut de texte légal contraignant, les conditions de cet archivage devront être établies par la jurisprudence qui s'inspirera vraisemblablement de l'article 1334 du Code civil.

---

1) Voir l'article 3 du règlement grand ducal du 22 décembre 1986, précité.

2) Précité.

3) Dans l'arsenal législatif, on dénombre tout au plus l'article 1334 du Code civil et l'article 11 du Code de commerce.

Le législateur a d'ores et déjà repris des conditions similaires pour l'archivage de certains documents commerciaux. L'article 11 du Code de commerce prévoit en effet qu' " *à l'exception du bilan et du compte des profits et pertes, les documents ou informations visés aux articles 8 à 10* [notamment les documents comptables, les pièces justificatives, les lettres reçues et les copies des lettres envoyées] *peuvent être conservés sous forme de copie. Ces copies ont la même valeur probante que les originaux dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal* [du 22 décembre 1986] ".

Dans le même sens, il s'apprête également à combler le vide législatif concernant les documents de la caisse nationale de prestations familiales en raison de " *la croissance extrêmement rapide des archives du congé parental qui contribue pour une large part à la saturation de l'espace disponible à la caisse* "[1]. Le projet de loi n° 5161[2] prévoit, en effet, l'insertion d'un treizième paragraphe[3] à l'article 6 de la loi modifiée du 19 juin 1985 concernant les allocations familiales et portant création de la caisse nationale des prestations familiales ayant un premier alinéa avec la teneur suivante: "*les images électroniques archivées définitivement sur disque optique numérique non réinscriptible dans le cadre du système de gestion électronique de documents de la caisse conformément à la norme AFNOR Z 42-013 ont la même valeur probante que les documents papier dont elles sont issues par numérisation sans la moindre altération par rapport à l'original et dont elles sont présumées, sauf preuve contraire, être une copie fidèle* ". L'exposé des motifs de ce projet de loi précise que " *le système de gestion électronique de documents ne trouve son sens que si les images numérisées acquièrent la même force probante que le document original et sont acceptées au même titre par les juridictions, afin que la caisse soit autorisée à détruire les documents papiers et à abandonner un archivage très consommateur tant en espace de stockage qu'en ressources humaines* "[4]. La référence à l'hypothèse de destruction du document initial de l'article 1334 du Code civil est évidente même si le texte proposé préfère renvoyer à la norme française en ce qui concerne les règles techniques et de gestion de l'archivage électronique plutôt qu'au règlement grand ducal du 22 décembre 1986 moins

---

1) Voir Doc. Parl. 5161/5.

2) Voir le projet de loi portant modification de la loi du 12 février 1999 portant création d'un congé parental et d 'un congé pour raisons familiales, la loi modifiée du 19 juin 1985 concernant les allocations familiales et portant création de la caisse nationale des prestations familiales, la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel déposé le 20 mai 2003, Doc. Parl. 5161/0.

3) Curieusement le texte proposé parle d'un " alinéa 13 ".

4) Voir Doc. Parl. 5161/0.

précis.[1] Ce renvoi est néanmoins critiqué par le Conseil d'Etat qui estime le qu'il n'est pas opportun de se référer dans un texte de loi à une norme spécifique. En conséquence, il propose - judicieusement - de remplacer les termes " norme AFNOR Z 42-013 " par les termes " norme standard ".[2]

Sans anticiper sur l'adoption de ce projet, il faut reconnaître son mérite: il pose la question de l'identité entre la valeur probante du document archivé et celle du document initialement établi sur support papier indépendamment de sa qualification comme acte sous seing privé au sens du Code civil.

L'existence de conditions diverses selon le type de documents à archiver électronique ne paraît pas souhaitable et il est fort à parier que la jurisprudence reprendra à son compte les conditions de l'article 1334 du Code civil en l'absence de texte légal fixant d'autres conditions.

Ainsi, dans la perspective d'assurer la sécurité juridique d'un système de gestion électronique de document, il est primordial de se préoccuper de l'archivage électronique des documents dès la phase de conception du système. Il convient par ailleurs de respecter certaines conditions et certaines modalités afin d'archiver électroniquement un document initialement établi sur support papier même si ce dernier n'est pas un acte sous seing privé.[3] C'est le meilleur moyen pour s'assurer que la valeur probante du document archivé est équivalente à celle du document initial dont il est la copie. Il faut ensuite établir une politique d'archivage aussi précise que possible en détaillant les aspects techniques, procéduraux, juridiques et organisationnels. Le cas échéant, il pourrait s'avérer utile de recourir à un " tiers archiveur " pour se décharger des contraintes liées à l'archivage et rationaliser les coûts y attachés.[4] On pense spécialement aux contraintes techniques.

Pour rappel, ces conditions n'imposent pas l'utilisation de la signature électronique pas plus qu'ils ne l'interdisent dans la mesure où cette signature est un ensemble de données liées de façon indissociable à l'acte qui garantit son intégrité et qui manifeste l'approbation du signataire au contenu de l'acte. Toute modification ultérieure du contenu de l'acte serait ainsi détectable.

En tout état de cause, que la politique d'archivage soit basée ou non sur la signature électronique, il convient d'assurer la conservation dans le temps de la valeur du document électronique.

---

1) Précité.

2) Voir l'avis du Conseil d'Etat du 30 mars 2004, Doc. Parl. 5161/4.

3) Dans un souci de cohérence, voire d'économie, il serait également préférable que la politique d'archivage de chaque OSS respecte les conditions prévues dans le cadre de l'article 1334 du Code civil.

4) On peut imaginer que l'archivage électronique sécurisé des documents de l'ensemble des organismes de sécurité sociale sera assuré à l'avenir par le centre commun de sécurité sociale ou le centre informatique de l'état.

III. COMMENT CONSERVER DANS LE TEMPS LA VALEUR PROBANTE D'UN DOCUMENT ÉLECTRONIQUE?

Avec l'écoulement du temps, un document électronique risque de ne pas présenter les mêmes garanties de sécurité et de fiabilité que celles qu'il possédait le jour où il a été établi pour la première fois dans sa forme définitive. Se pose alors inévitablement l'épineuse question de la conservation dans le temps de la valeur probante d'un document électronique.

Cette question doit cependant s'analyser en deux étapes: il convient de distinguer selon que le document électronique a été initialement établi sur support papier (A) ou sous forme électronique (B).

A. Le document initial a été établi sur support papier

Lorsque le document a été initialement établi sur support papier, le document électronique auquel on se trouve confronté ne peut en constituer qu'une copie. En cette hypothèse, la valeur probante du document électronique n'est la même que celle du document initial que s'il a été archivé correctement. L'archivage électronique sécurisé d'un document initialement établi sur support papier doit en effet satisfaire à un certain nombre de conditions.[1)]

Il peut néanmoins s'opérer de différentes manières. Les règles relatives à la conservation de la valeur probante du document vont ainsi varier selon que celui-ci a été archivé (i) en utilisant la signature électronique ou (ii) non.

i) le document archivé n'a pas été signé électroniquement

La fidélité des informations conservées sur un document électronique non-signé mais archivé dans les règles de l'art va dépendre du respect des règles techniques, procédurales et organisationnelles mises en œuvre dans le cadre de la politique d'archivage.

Outre les normes à respecter quant à l'environnement de conservation[2)], une attention toute particulière doit être portée au support utilisé. Il peut s'agir par exemple d'un disque optique inscriptible de type WORM. Un tel support n'a cependant une durée de vie que de dix ou vingt ans. Il convient ainsi de réécrire périodiquement les documents électroniques archivés. Cette réécriture s'effectue dans le cadre d'une migration vers un nouveau support.

Lors de chaque migration, il est indispensable de garantir à nouveau la fidélité et la durabilité des informations conservées. Un choix doit être effectué sur la

---

1) Voir supra II.

2) On pense notamment aux normes ayant trait à la température moyenne de conservation, à l'humidité relative de conservation.

méthode à utiliser. Il est tout à fait possible d'envisager que des documents archivés sur disque optique non réinscriptible soient ensuite signés électroniquement et conservés sur support magnétique ou sur disque numérique polyvalent (DVD).

ii) le document archivé est signé électroniquement

Si la politique d'archivage prévoit l'utilisation d'une signature électronique pour la conservation des données, il faut s'assurer que cette signature garde au fil de temps des garanties fiables quant au maintien de l'intégrité du document électronique.

Or, cette signature est créée à partir d'algorithmes mathématiques complexes qui peuvent être cassés. Un tel événement priverait la signature de toute fiabilité. Avant sa survenance, il convient en conséquence d'apposer une nouvelle signature électronique suffisamment fiable sur le document qui garantisse son intégrité pour l'avenir.

B. Le document initial a été établi sous forme électronique

Le développement de la société de l'information devrait conduire les OSS à traiter de plus en plus de documents sous forme électronique et ceci dès leur création. Il n'est pas utopiste d'imaginer que, dans les prochaines années, les assurés pourront remplir certains formulaires en ligne ou recevoir les réponses d'un organisme via un recommandé électronique.

Le problème de la conservation de la valeur probante de tels documents électroniques générés ou reçus par l'OSS ne se pose toutefois pas dans les mêmes termes si le document électronique est (i) revêtu d'une signature électronique ou (ii) non.

i) Le document est signé électroniquement

L'article 1322-2 du Code civil précise que " *l'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment ou il a été crée pour la première fois sous sa forme définitive* ".

Il faut s'assurer que cette signature garde au fil de temps des garanties fiables quant au maintien de l'intégrité du document électronique et, à défaut, signer à nouveau le document électronique ou utiliser une autre technique permettant de garantir son intégrité à travers le temps.

ii) le document n'est pas signé électroniquement

Un document peut également être établi sous forme électronique sans être signé électroniquement. En effet, " *nul ne peut être contraint de signer électroniquement* "[1]. Or, même dépourvu de signature électronique, ce document pourrait présenter sur le plan de la preuve, une valeur qu'il convient de préserver. Il pourrait ainsi être nécessaire d'opérer un archivage électronique sécurisé du document électronique en vue de garantir son intégrité.

IV. Conclusion

L'archivage électronique sécurisé est à la croisée des chemins: " *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 des besoins d'archivage des documents de l'organisation en cause (entreprise, administration)* "[2].

Dans ce dédale de normes juridiques, techniques, procédurales et organisationnelles à respecter, les OSS ne sont pas réellement guidés par le législateur. Il semble, en effet, que " *le monde de l'électronique et qui plus est, celui de l'écrit électronique est trop récent pour que le législateur s'aventure à donner des indications sur l'esprit qui doit présider à la conservation légale et sur les pratiques à déployer lors de l'archivage* "[3].

Néanmoins, le législateur est intervenu pour adapter les exigences de la preuve littérale aux documents électroniques. Il consacre notamment la copie fidèle[4] et l'acte sous seing privé électronique[5].

Certes, la solution n'est pas toujours idoine: " *Les récentes évolutions législatives et réglementaires dans le domaine de la valeur probante de l'écrit électronique supposent le recours à des techniques qui sont difficilement compatibles avec les méthodes de conservation à long terme des documents électroniques* "[6]. Mais, il est tout à fait possible aujourd'hui pour les OSS de mettre en place un archivage électronique sécurisé de leurs documents.

---

1) *Voir l'article 18, paragraphe 3, de la loi relative au commerce électronique, précitée.*

2) *E. CAPRIOLI et G. WEISZ, " archivage électronique : des contraintes juridiques et technologiques ", www.journaldunet.com*

3) *Voir : Th. PIETTE-COUDOL, " Conservation et archivage de l'écrit sous forme électronique ", Communication Commerce Electronique, Mai 2002, p. 10 .*

4) *Voir l'article 1334 du Code civil.*

5) *Voir l'article 1322-2 du Code civil.*

6) *Voir : J. POIVRE, " Archivage des documents électroniques et authenticité : les dilemmes de l'archiviste ", Cahiers Lamy droit de l'informatique et des réseaux, n° 151, octobre 2002, p. 18.*

Le passage à l'administration électronique devrait d'ailleurs les inciter à s'interroger sur la conservation dans le temps des documents initialement établis sous forme électronique.

Parmi les questions essentielles à débattre, il faut certainement citer, d'une part, celle de l'utilisation de la signature électronique et/ou des disques optiques inscriptibles et, d'autre part, celle de savoir si cet archivage doit être opéré par chaque organisme ou par un " tiers archiveur " qui leur est commun.

Sur ce dernier point, l'exemple belge de la Banque Carrefour de la Sécurité Sociale[1)] qui prévoit la répartition fonctionnelle des tâches d'enregistrement est édifiant. Les OSS belges[2)] sont, en effet, tenus d'enregistrer dans leurs banques de données sociales et de tenir à jour les données dont la conservation leur est confiée par la Banque carrefour.

Gageons, finalement, à la lumière des développements qui précèdent, que l'archivage électronique sécurisé est promis à un bel avenir auprès des OSS à l'aune de l'administration électronique.

---

1) Loi belge modifiée du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale, M.B., 22 février 1990.

2) Appelés en Belgique, institutions de sécurité sociale.

Loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE du 20 mai 1997 concernant la vente à distance des biens et des services autres que les services financiers

TITRE I. DISPOSITIONS GENERALES

Art. 1. Définitions

Au sens de la présente loi, on entend par:

«Services de la société de l'information»: tout service presté, normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services.

Aux fins de la présente définition, on entend par:

les termes «à distance»: un service fourni sans que les parties soient simultanément présentes;

«par voie électronique»: un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques;

«à la demande individuelle d'un destinataire de services»: un service fourni par transmission de données sur demande individuelle;

«prestataire»: toute personne physique ou morale qui fournit un service de la société de l'information; «prestataire établi»: prestataire qui exerce d'une manière effective une activité économique au moyen d'une installation stable pour une durée indéterminée. La présence et l'utilisation des moyens techniques et des technologies utilisées pour fournir le service ne constituent pas en tant que telles un établissement du prestataire;

«destinataire du service»: toute personne physique ou morale qui, à des fins professionnelles ou non, utilise un service de la société de l'information, notamment pour rechercher ou pour rendre accessible une information.

Art. 2. Champ d'application

(1) La présente loi ne s'applique pas:

- à la fiscalité, sans préjudice des dispositions de l'article 16 de la présente loi;
- aux accords ou pratiques régis par la législation relative aux ententes.

(2) Les dispositions de la présente loi ne s'appliquent pas à la représentation d'un client et la défense de ses intérêts devant les tribunaux.

(3) Les dispositions de la présente loi s'appliquent sans préjudice des dispositions relatives à la protection des données personnelles.

(4) La loi du lieu d'établissement du prestataire de services de la société de l'information s'applique aux prestataires et aux services qu'ils prestent, sans préjudice de la liberté des parties de choisir le droit applicable à leur contrat.

(5) Quel que soit le lieu d'établissement du prestataire de services de la société de l'information, la loi luxembourgeoise est applicable aux activités de jeux d'argent qui impliquent des enjeux monétaires dans des jeux de hasard, ce qui comprend les loteries et les transactions portant sur les paris.

(6) L'autorité nationale d'accréditation et de surveillance visée à l'article 17 peut restreindre la libre circulation d'un service de la société de l'information en provenance d'un autre Etat membre lorsque ledit service représente un risque sérieux et grave d'atteinte à l'ordre public, la sécurité publique, la santé publique ou la protection des consommateurs, en observant par ailleurs les exigences posées par le droit communautaire à l'exercice de cette faculté.

Art. 3. De l'usage de la cryptographie

L'usage des techniques de cryptographie est libre.

Art. 4. De l'accès à l'activité de prestataires de services

Sans préjudice des dispositions de la loi d'établissement, l'accès à l'activité de prestataire ne fait, en tant que telle, pas l'objet d'une autorisation préalable.

Art. 5. De l'obligation générale d'information des destinataires

(1) Le prestataire de services de la société de l'information doit permettre aux destinataires des services et aux autorités compétentes un accès facile, direct et permanent aux informations suivantes:

a) son nom;
b l'adresse géographique où il est établi;
c les coordonnées permettant de le contacter rapidement et de communiquer directement et effectivement avec lui, y compris son adresse de courrier électronique;

d le cas échéant, son titre professionnel et les références de l'ordre professionnel auquel il adhère, son numéro d'immatriculation au registre du commerce, son numéro d'identification à la TVA et l'autorisation dont il bénéficie pour exercer son activité ainsi que les coordonnées de l'autorité ayant donné cette autorisation.

(2) Lorsque les services de la société de l'information font mention de prix et conditions de vente ou de réalisation de la prestation, ces derniers doivent être indiqués de manière précise et non équivoque. Il doit aussi être indiqué si toutes les taxes et frais additionnels sont compris dans le prix. Ces dispositions s'appliquent sans préjudice de la législation sur la protection des consommateurs.

TITRE II. DE LA PREUVE ET DE LA SIGNATURE ELECTRONIQUE

Chapitre 1er. - De la preuve littérale

Art. 6. «Signature»

Après l'article 1322 du Code civil, il est ajouté un article 1322-1 ainsi rédigé: «La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.

Elle peut être manuscrite ou électronique.

La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article.»

Art. 7. Après l'article 1322 du Code civil, il est ajouté un article 1322-2 ainsi rédigé: «L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive.»

Art. 8. L'article 292 du Nouveau code de procédure civile est modifié comme suit: les mots «signée et paraphée» sont remplacés par «signée et, en cas de signature manuscrite, paraphée.»

Art. 9. L'article 1325 du Code civil est complété par l'alinéa suivant: «Le présent article ne s'applique pas aux actes sous seing privé revêtus d'une signature électronique.»

Art. 10. L'article 1326 du Code civil est modifié comme suit: «L'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention de la somme ou de la quantité en toutes lettres. Cette mention doit être écrite de sa main ou être revêtue spécifiquement d'une signature électronique; si elle est indiquée également en chiffres, en cas de différence,

l'acte sous seing privé vaut pour la somme écrite en toutes lettres, à moins qu'il ne soit prouvé de quel côté est l'erreur.»

Art. 11. A la section première du Chapitre VI du Code civil, l'intitulé du Paragraphe III est remplacé par l'intitulé suivant: «Des copies des actes sous seing privé.»

Art. 12. L'article 1333 du Code civil est réintroduit avec le libellé suivant: «Les copies, lorsque le titre original ou un acte faisant foi d'original au sens de l'article 1322-2 subsiste, ne font foi que de ce qui est contenu au titre ou à l'acte, dont la représentation peut toujours être exigée.»

Art. 13. L'article 1334 du Code civil est inséré au paragraphe III et est remplacé par la disposition suivante: «Lorsque le titre original ou l'acte faisant foi d'original au sens de l'article 1322-2 n'existe plus, les copies effectuées à partir de celui-ci, sous la responsabilité de la personne qui en a la garde, ont la même valeur probante que les écrits sous seing privé dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal.»

Art. 14. L'article 1348, alinéa 2 du Code civil est supprimé. Le règlement grand-ducal du 22 décembre 1986, pris en exécution de l'article 1348 du Code civil, continue à produire ses effets sur la base de l'article 13 de la présente loi.

Art. 15. Les deux premiers alinéas de l'article 11 du Code de commerce sont remplacés par l'alinéa suivant: «A l'exception du bilan et du compte des profits et pertes, les documents ou informations visés aux articles 8 à 10 peuvent être conservés sous forme de copie. Ces copies ont la même valeur probante que les originaux dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par un règlement grand-ducal.»

Art. 16. Toute personne à charge de laquelle la loi prévoit l'obligation de délivrer ou de communiquer des documents et données à la requête d'un agent d'une administration fiscale doit, lorsque ces documents et données n'existent que sous forme électronique, les délivrer ou communiquer, sur requête d'un agent d'une administration fiscale, dans une forme lisible et directement intelligible, certifiée conforme à l'original, sur support papier ou, par dérogation, suivant toutes autres modalités techniques que l'administration fiscale détermine.

Constitue un manquement à l'obligation de délivrance ou de communication le fait, pour la personne à laquelle la délivrance ou la communication incombent légalement, de ne pas se conformer aux requêtes et instructions d'une administration fiscale visées à l'alinéa précédent.

Chapitre 2.- De la signature électronique et des prestataires de service de certification

Section 1. Définitions et effets juridiques de la signature électronique

Art. 17. Définitions

«Signataire»: toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une personne physique ou morale qu'elle représente.

«Dispositif de création de signature»: un dispositif qui satisfait aux exigences définies au règlement grand-ducal relatif au certificat qualifié.

«Dispositif sécurisé de création de signature»: un dispositif de création de signature qui satisfait aux exigences fixées par règlement grand-ducal.

«Dispositif de vérification de signature»: un dispositif qui satisfait aux exigences définies au règlement grand-ducal relatif au certificat.

«Certificat qualifié»: un certificat qui satisfait aux exigences fixées sur base de l'article 25 de la présente loi.

«Prestataire de service de certification»: toute personne, physique ou morale, qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques.

«Titulaire de certificat»: toute personne, physique ou morale, à laquelle un prestataire de service de certification a délivré un certificat.

«Accréditation»: procédure par laquelle un organisme faisant autorité reconnaît formellement qu'un organisme ou un individu est compétent pour effectuer des tâches spécifiques.

«Système d'accréditation»: système ayant des propres règles de procédure et de gestion et destiné à procéder à l'accréditation.

«Accréditation volontaire»: toute autorisation indiquant les droits et obligations spécifiques à la fourniture de services de certification, accordée, sur demande du prestataire de service de certification concerné, par l'Autorité nationale d'accréditation et de surveillance chargée d'élaborer ces droits et obligations et d'en contrôler le respect, lorsque le prestataire de service de certification n'est pas habilité à exercer les droits découlant de l'autorisation aussi longtemps qu'il n'a pas obtenu la décision de l'organisme.

«L'Autorité Nationale d'Accréditation et de Surveillance»: est le ministre ayant dans ses attributions l'Economie:

- qui dirige et gère, par ses services, un système d'accréditation et qui se prononce sur l'accréditation;
- qui dirige et gère, par ses services, la surveillance des prestataires de service de certification de signatures électroniques, et plus particulièrement de ceux qui émettent des certificats qualifiés.

Art. 18. Des effets juridiques de la signature électronique

(1) Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique créée par un dispositif sécurisé de création de signature que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat qualifié, constitue une signature au sens de l'article 1322-1 du Code civil.

(2) Une signature électronique ne peut être rejetée par le juge au seul motif qu'elle se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

(3) Nul ne peut être contraint de signer électroniquement.

Section 2. Des prestataires de service de certification

Sous - Section 1. Dispositions communes

Art. 19. De l'obligation de secret professionnel

(1) Les administrateurs, les membres des organes directeurs et de surveillance, les dirigeants, les employés et les autres personnes qui sont au service d'un prestataire de service de certification, ainsi que tous ceux qui exercent eux-mêmes les fonctions de prestataire de service de certification, sont obligés de garder strictement secrets tous les renseignements confiés à eux dans le cadre de leur activité professionnelle, à l'exception de ceux dont le titulaire de certificat a accepté la publication ou la communication. La révélation de tels renseignements est punie des peines prévues à l'article 458 du Code pénal.

(2) L'obligation de secret cesse lorsque la révélation d'un renseignement est autorisée ou imposée par ou en vertu d'une disposition législative, même antérieure à la présente loi.

(3) L'obligation de secret n'existe pas à l'égard de l'Autorité Nationale d'Accréditation et de Surveillance agissant dans le cadre de ses compétences légales.

(4) Toute personne exerçant ou ayant exercé une activité pour l'Autorité Nationale d'Accréditation et de Surveillance, ainsi que les auditeurs mandatés par l'Autorité Nationale d'Accréditation et de Surveillance, sont tenus au secret professionnel et passibles des peines prévues à l'article 458 du Code pénal en cas de violation de ce secret.

(5) Sous réserve des règles applicables en matière pénale, les renseignements visés au §1, une fois révélés, ne peuvent être utilisés qu'à des fins pour lesquelles la loi a permis leur révélation.

(6) Quiconque est tenu à l'obligation de secret visée au §1 et a légalement révélé un renseignement couvert par cette obligation, ne peut encourir de ce seul fait une responsabilité pénale ou civile.

Art. 20. De la protection des données à caractère personnel

(1) L'Autorité Nationale d'Accréditation et de Surveillance et les prestataires de service de certification sont tenus au respect des dispositions légales régissant le traitement de données à caractère personnel.

(2) Le prestataire de service de certification qui délivre des certificats à l'intention du public ne peut recueillir des données à caractère personnel que directement auprès de la personne qui demande un certificat, ou avec le consentement explicite de celle-ci, auprès de tiers. Le prestataire ne collecte les données que dans la seule mesure où ces dernières sont nécessaires à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.

(3) Lorsqu'un pseudonyme est utilisé, l'identité véritable du titulaire ne peut être révélée par le prestataire de service de certification qu'avec le consentement du titulaire ou dans les cas prévus à l'article 19§2.

Art. 21. Des obligations du titulaire de certificat

(1) Dès le moment de la création des données afférentes à la création de signature, le titulaire du certificat est seul responsable de la confidentialité et de l'intégrité des données afférentes à la création de signature qu'il utilise. Toute

utilisation de ceux-ci est réputée, sauf preuve contraire, être son fait.

(2) Le titulaire du certificat est tenu, dans les meilleurs délais, de notifier au prestataire de service de certification toute modification des informations contenues dans celui-ci.

(3) En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de la conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer immédiatement le certificat conformément à l'article 26 de la présente loi.

(4) Lorsqu'un certificat est arrivé à échéance ou a été révoqué, son titulaire ne peut plus utiliser les données afférentes à la création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de service de certification.

Sous - Section 2. Des prestataires de service de certification émettant des certificats qualifiés

Art. 22. De l'obligation d'information

(1) Préalablement à toute relation contractuelle avec une personne demandant un certificat qualifié ou à la demande d'un tiers qui se prévaut d'un tel certificat, le prestataire de service de certification procure, sur un support durable et dans une langue aisément compréhensible, les informations nécessaires à l'utilisation correcte et sûre de ses services.

Ces informations se rapportent au moins:

a) à la procédure à suivre afin de créer et de vérifier une signature électronique;
b aux modalités et conditions précises d'utilisation des certificats, y compris les limites imposées à leur utilisation, à condition que ces limites soient discernables par des tiers;
c aux obligations qui pèsent, en vertu de la présente loi, sur le titulaire du certificat et le prestataire de service de certification;
d à l'existence d'un régime volontaire d'accréditation;
e aux conditions contractuelles de délivrance d'un certificat, y compris les limites éventuelles de responsabilité du prestataire de service de certification;
f aux procédures de réclamation et de règlement des litiges.

(2) Le prestataire de service de certification fournit un exemplaire du certificat au candidat titulaire.

Dès son acceptation par le candidat titulaire, le prestataire de service de certification inscrit le certificat dans l'annuaire électronique visé par règlement grand-ducal sous réserve que le titulaire du certificat ait donné son consentement à cette inscription.

Art. 23. De l'obligation de vérification

(1) Préalablement à la délivrance d'un certificat, le prestataire de service vérifie la complémentarité des données afférentes à la création et à la vérification de signature.

(2) Lorsqu'un certificat qualifié est délivré à une personne morale, le prestataire de service de certification vérifie préalablement l'identité et le pouvoir de représentation de la ou des personne(s) physique(s) qui se présente(nt) à lui.

Art. 24. De l'acceptation des certificats

(1) Le contenu et la publication d'un certificat sont soumis au consentement de son titulaire.

(2) Le prestataire de service de certification conserve un annuaire électronique comprenant les certificats qu'il délivre et le moment de leur expiration. Dès son acceptation par le candidat titulaire, le prestataire de service de certification inscrit le certificat dans l'annuaire électronique visé par règlement grand-ducal sous réserve que le titulaire du certificat ait donné son consentement à cette inscription.

Art. 25. De l'émission et du contenu des certificats qualifiés

(1) Pour pouvoir émettre des certificats qualifiés, les prestataires de service de certification doivent disposer des moyens financiers et des ressources matérielles, techniques et humaines adéquates pour garantir la sécurité, la fiabilité et la pérennité des services de certification offerts. Ces exigences peuvent être précisées par voie de règlement grand-ducal.

(2) Tout certificat qualifié doit contenir les informations telles qu'arrêtées par règlement grand-ducal.

(3) A la demande du titulaire, le certificat peut contenir d'autres informations, non certifiées par le prestataire de service de certification, en précisant qu'elles n'ont pas été vérifiées par ce dernier.

(4) Un certificat qualifié peut être délivré tant par un prestataire de service de certification accrédité que par un prestataire de service de certification non accrédité pour autant que celui-ci remplit les conditions requises par la loi et les règlements grand-ducaux pris pour son application.

Art. 26. De la révocation des certificats

(1) A la demande de son titulaire, préalablement identifié, le prestataire de service de certification révoque immédiatement le certificat qualifié.

(2) Le prestataire de service de certification révoque également un certificat immédiatement lorsque:

a) après suspension, un examen plus approfondi démontre que le certificat a été constitué sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité, ou que la confidentialité des données afférentes à la création de signature a été violée ou que le certificat a été utilisé frauduleusement;
b lorsqu'elle est informée du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire.

(3) Le prestataire de service de certification informe le titulaire de la révocation du certificat dans les meilleurs délais et motive sa décision.

Elle prévient le titulaire de l'échéance du certificat au moins un mois à l'avance.

(4) La révocation d'un certificat qualifié est définitive.

(5) Immédiatement après la décision de révocation, le prestataire de service de certification inscrit la mention de la révocation du certificat dans l'annuaire électronique visé à l'article 23.

La révocation devient opposable aux tiers dès son inscription dans l'annuaire électronique.

Art. 27. De la responsabilité des prestataires de service de certificats qualifiés

(1) A moins qu'il ne prouve n'avoir commis aucune négligence, le prestataire de service de certification qui délivre à l'intention du public un certificat qualifié ou qui garantit publiquement un tel certificat est responsable du préjudice causé à toute personne qui se fie raisonnablement:

- à l'exactitude des informations contenues dans le certificat qualifié à dater de sa délivrance;
- à l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;
- à l'assurance que le dispositif de création de signature et le dispositif de vérification de signature fonctionnent ensemble de façon complémentaire, au cas où le prestataire a généré les deux dispositifs.

(2) A moins qu'il ne prouve n'avoir commis aucune négligence, le prestataire de service de certification qui délivre à l'intention du public un certificat qualifié ou qui garantit publiquement un tel certificat est responsable du préjudice causé à toute personne qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat.

(3) Le prestataire de service de certification n'est pas responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation ou la valeur limite des transactions pour lesquelles le certificat peut être utilisé, pour autant que ces limites soient inscrites dans le certificat et discernables par les tiers.

(4) Les dispositions des paragraphes 1 à 3 sont sans préjudice de la loi modifiée du 25 août 1983 relative à la protection juridique du consommateur.

Art. 28. De la reconnaissance des certificats de pays tiers

Les certificats, délivrés à titre de certificats qualifiés par un prestataire de service de certification établi dans un pays tiers à l'Union européenne, ont la même valeur juridique au Luxembourg que ceux délivrés par un prestataire de service de certification établi au Luxembourg:

a) si le prestataire de service de certification remplit les conditions visées par la présente loi et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi par un Etat membre de l'Union européenne; ou

b b) si un prestataire de service de certification établi dans un Etat membre de l'Union européenne garantit ces certificats; ou

c c) si le certificat ou le prestataire de service de certification est reconnu dans le cadre d'un accord bilatéral entre le Luxembourg et des pays tiers ou dans le cadre d'un accord multilatéral entre l'Union européenne et des pays tiers ou des organisations internationales.

Art. 29. La surveillance

(1) L'autorité nationale d'accréditation et de surveillance veille au respect par les prestataires de services émettant des certificats qualifiés des exigences contenues dans les articles 19 à 27 de la présente loi et dans les règlements grand-ducaux pris en application.

(2) Tout prestataire émettant des certificats qualifiés est tenu de notifier à l'autorité nationale la conformité de ses activités aux exigences de la présente loi et des règlements pris en son exécution.

(3) L'autorité nationale tient un registre des notifications, qui fait l'objet, à la fin de chaque année de calendrier, d'une publication au Mémorial, Recueil administratif et économique, sans préjudice de la possibilité, pour l'autorité nationale, de publier à tout moment, soit au Mémorial, soit dans un ou plusieurs journaux, nationaux ou étrangers, une radiation du registre, si une telle mesure de publicité est commandée par l'intérêt public.

(4) L'autorité nationale peut, soit d'office, soit à la demande de toute personne intéressée, vérifier ou faire vérifier la conformité des activités d'un prestataire de service de certification aux dispositions de la présente loi ou des règlements pris en son exécution.

L'autorité peut avoir recours à des auditeurs externes agréés pour de telles vérifications. Un règlement grand-ducal détermine la procédure d'agrément, à délivrer par le ministre ayant dans ses attributions l'Economie. Pourront faire l'objet d'un agrément les personnes qui justifient d'une qualification professionnelle adéquate ainsi que de connaissances et d'une expérience spécialisées dans le domaine des technologies des signatures électroniques, et qui présentent des garanties d'honorabilité professionnelle et d'indépendance par rapport aux prestataires de service de certification dont elles sont appelées à vérifier les activités.

(5) Dans l'accomplissement de leur mission de vérification, les agents de l'autorité nationale ainsi que les auditeurs externes agréés ont, sur justification de leurs qualités, le droit d'accéder à tout établissement et de se voir communiquer toutes informations et tous documents qu'ils estimeront utiles ou nécessaires à l'accomplissement de leur mission.

Tout refus de la part d'un prestataire de service de certification de collaborer activement est puni d'une amende de 10.001 à 800.000 francs. L'autorité peut, en pareil cas, également procéder à la radiation des prestataires du registre des notifications.

(6) Si, sur le rapport de ses agents ou de l'auditeur externe agréé, l'autorité nationale constate que les activités du prestataire de service de certification ne sont pas conformes aux dispositions de la présente loi ou des règlements pris en son exécution, elle invite le prestataire à se conformer, dans le délai qu'elle détermine, auxdites dispositions. Si, passé ce délai, le prestataire ne s'est pas conformé, l'autorité nationale procède à la radiation du prestataire du registre des notifications.

(7) En cas de constatation d'une violation grave par un prestataire de service de certification des dispositions de la présente loi ou des règlements pris en son exécution, l'autorité nationale peut en informer à telles fins que de droit notamment les autorités administratives compétentes en matière de droit d'établissement. Les rapports établis à l'attention de l'autorité nationale peuvent être communiqués à ces autorités, dans la mesure où le prestataire de service de certification en a reçu communication dans ses relations avec l'autorité nationale.

Sous-section 3. Des prestataires de service de certification accrédités

Art. 30. De l'accréditation

(1) Les prestataires de service de certification sont libres de demander ou non une accréditation.

(2) L'accréditation couvre la délivrance de certificats relatifs à l'identité, éventuellement à la profession ou tout autre attribut durable du titulaire du certificat, ainsi qu'à toute autre mention pouvant être certifiée.

(3) Le prestataire de service de certification peut demander l'accréditation pour un ou plusieurs de ces éléments et pour une ou plusieurs catégories de titulaires.

Art. 31. Des conditions d'obtention de l'accréditation

(1) Les conditions d'obtention et de conservation de l'accréditation sont fixées par un règlement grand-ducal.

(2) Un règlement grand-ducal détermine:

a) la procédure de délivrance, d'extension, de suspension et de retrait des accréditations;
b les frais d'examen et de suivi des dossiers;
c les délais d'examen des demandes;
d le montant et les modalités de la garantie financière;
e les conditions visant à assurer l'interopérabilité des systèmes de certification et l'interconnexion des registres de certificats;
f les règles relatives à l'information que le prestataire de service de certification est tenu de conserver concernant ses services et les certificats délivrés par lui;

g les garanties d'indépendance que les prestataires de service de certification doivent offrir aux utilisateurs du service;

h la durée de conservation des données.

(3) Des conditions complémentaires peuvent être fixées par règlement grand-ducal pour qu'un prestataire de service de certification soit habilité à délivrer des certificats à des personnes qui souhaitent utiliser une signature électronique dans leurs échanges avec les autorités publiques.

(4) La décision sur la suspension ou le retrait de l'accréditation peut être déférée, dans le délai d'un mois, sous peine de forclusion, au tribunal administratif, qui statue comme juge de fond.

Art. 32. De l'arrêt et du transfert des activités

(1) Le prestataire de service de certification accrédité informe dans un délai raisonnable l'Autorité Nationale d'Accréditation et de Surveillance de son intention de mettre fin à ses activités ou, le cas échéant, de son incapacité de poursuivre ses activités. Il s'assure de la reprise de celles-ci par un autre prestataire de service de certification accrédité, dans les conditions décrites au §2 du présent article, ou, à défaut, prend les mesures requises au §3 du présent article.

(2) Le prestataire de service de certification accrédité peut transférer à un autre prestataire tout ou partie de ses activités. Le transfert des certificats est opéré aux conditions suivantes:

a) le prestataire de service de certification avertit chaque titulaire de certificat encore en vigueur qu'il envisage de transférer les certificats à un autre prestataire de service de certification au moins un mois avant le transfert envisagé;

b il précise l'identité du prestataire de service de certification auquel le transfert de ces certificats est envisagé;

c il indique à chaque titulaire de certificat leur faculté de refuser le transfert envisagé, ainsi que les délais et modalités dans lesquelles il peut le refuser. A défaut d'acceptation expresse du titulaire au terme de ce délai, le certificat est révoqué.

(3) Tout prestataire de service de certification accrédité qui cesse ses activités sans que celles-ci ne soient reprises par un autre prestataire de service de certification accrédité, révoque les certificats un mois après en avoir averti les titulaires et prend les mesures nécessaires pour assurer la conservation des données conformément à l'article 25.

(4) Le décès, l'incapacité, la faillite, la dissolution volontaire et la liquidation, ou tout autre motif involontaire d'arrêt des activités sont assimilés à une cessation d'activité au sens de la présente loi.

Art. 33. Du contrôle

(1) Lorsque l'Autorité Nationale d'Accréditation constate qu'un prestataire de service de certification accrédité ne se conforme pas aux prescriptions de la présente loi et des règlements, elle fixe un délai pour régulariser la situation et éventuellement, suspend l'accréditation.

(2) Si, après l'écoulement de ce délai, le prestataire de service de certification accrédité n'a pas régularisé sa situation, la même autorité procède au retrait de l'accréditation.

(3) Le prestataire de service de certification est tenu de mentionner immédiatement dans son annuaire électronique le retrait de l'accréditation et d'en informer sans délai les titulaires de certificat.

Sous-section 4. Du recommandé électronique

Art. 34. Le message signé électroniquement sur base d'un certificat qualifié dont l'heure, la date, l'envoi et le cas échéant la réception, sont certifiés par le prestataire conformément aux conditions fixées par règlement grand-ducal constitue un envoi recommandé.

TITRE III. DISPOSITIONS PENALES

Art. 35. L'article 196 du Code pénal est modifié comme suit: «Seront punies de réclusion de cinq à dix ans les autres personnes qui auront commis un faux en écritures authentiques et publiques, et toutes personnes qui auront commis un faux en écritures de commerce, de banque ou en écritures privées, en ce compris les actes sous seing privé électronique,

Soit par fausses signatures,

Soit par contrefaçon ou altération d'écritures ou de signatures,

Soit par fabrication de conventions, dispositions, obligations ou décharges, ou par leur insertion après coup dans les actes,

Soit par addition ou altération de clauses, de déclarations ou de faits que ces actes avaient pour objet de recevoir et de constater.»

Art. 36. L'article 197 du Code pénal est modifié comme suit: «Dans tous les cas exprimés dans la présente section, celui qui aura fait usage du faux sera puni comme s'il était l'auteur du faux.»

Art. 37. L'article 487 du Code pénal est modifié comme suit: «Sont qualifiées fausses clefs: Tous crochets, rossignols, passe-partout, clefs imitées, contrefaites ou altérées, y compris électroniques;

Les clefs qui n'ont pas été destinées par le propriétaire, locataire, aubergiste ou logeur, aux serrures, cadenas ou aux fermetures quelconques auxquelles le coupable les aura employées;

Les clefs perdues, égarées ou soustraites, y compris électroniques, qui auront servi à commettre le vol.

Toutefois, l'emploi de fausses clefs ne constituera une circonstance aggravante que s'il a eu lieu pour ouvrir des objets dont l'effraction eût entraîné une aggravation de peine.»

Art. 38. L'article 488 du Code pénal est modifié comme suit: «Quiconque aura frauduleusement contrefait ou altéré des clefs, y compris électroniques sera condamné à un emprisonnement de trois mois à deux ans et à une amende de 10.001 francs à 80.000 francs.»

Art. 39. L'article 498 du Code pénal est modifié comme suit: «Sera puni d'un emprisonnement d'un mois à un an et d'une amende de 20.000 francs à 400.000 francs, ou d'une de ces peines seulement, celui qui aura trompé l'acheteur:

Sur l'identité du bien vendu, en livrant frauduleusement un bien autre que l'objet déterminé sur lequel a porté la transaction;

Sur la nature ou l'origine du bien vendu, en vendant ou en livrant un bien semblable en apparence à celui qu'il a acheté ou qu'il a cru acheter.

Les dispositions qui précèdent s'appliquent aux biens mobiliers y compris incorporels et immobiliers.»

Art. 40. L'article 505 du Code pénal est modifié comme suit: «Ceux qui auront recelé, en tout ou en partie, les choses ou les biens incorporels enlevés, détournés ou obtenus à l'aide d'un crime ou d'un délit, seront punis d'un emprisonnement de quinze jours à cinq ans et d'une amende de 10.001 francs à 200.000 francs.

Ils pourront, de plus, être condamnés à l'interdiction, conformément à l'article 24.

Constitue également un recel le fait de sciemment bénéficier du produit d'un crime ou d'un délit.»

Art. 41. L'article 509-1 du Code pénal est modifié comme suit: «Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 20.000 francs à 1.000.000 francs ou de l'une de ces deux peines.

Lorsqu'il en sera résulté soit la suppression soit la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 50.000 francs à 1.000.000 francs.»

Art. 42. L'article 509-2 du Code pénal est modifié comme suit: «Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 50.000 francs à 500.000 francs ou de l'une de ces deux peines.»

Art. 43. L'article 509-3 du Code pénal est modifié comme suit: «Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé de données ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 50.000 francs à 500.000 francs ou de l'une de ces deux peines.»

Art. 44. L'article 509-4 du Code pénal est abrogé.

Art. 45. L'article 509-5 du Code pénal est abrogé.

TITRE IV. DES COMMUNICATIONS COMMERCIALES

Art. 46. Définition

«Communication commerciale»: toutes les formes de communication destinées à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une entreprise, d'une organisation, ou d'une personne ayant une activité commerciale, industrielle, artisanale ou de profession libérale.

Ne constituent pas en tant que tel des communications commerciales:

- les coordonnées permettant l'accès direct à l'activité de cette entreprise, organisation ou personne notamment un nom de domaine ou une adresse de courrier électronique;
- les communications relatives aux biens, services ou à l'image de cette entreprise, organisation ou personne élaborées d'une manière indépendante de celle-ci, en particulier lorsqu'elles sont fournies sans contrepartie financière.

Art. 47. Obligation de transparence

La communication commerciale doit respecter les conditions suivantes:

a) la communication commerciale doit être clairement identifiable en tant que telle;
b la personne physique ou morale pour le compte de laquelle la communication commerciale est faite doit être clairement identifiable;
c les concours ou jeux promotionnels doivent être clairement identifiables comme tels et leurs conditions de participation doivent être aisément accessibles et présentées de manière précise et non équivoque.

Art. 48. Des communications commerciales non sollicitées

(1) La communication commerciale non sollicitée par courrier électronique doit être identifiée en tant que telle, d'une manière claire et non équivoque, dès sa réception par le destinataire.

(2) L'envoi de communications commerciales par courrier électronique par un prestataire de service de la société de l'information à un destinataire n'est possible qu'en cas d'absence d'opposition manifeste de sa part.

(3) Les prestataires qui envoient par courrier électronique des communications commerciales non sollicitées doivent consulter régulièrement les registres «opt out» désignés par règlement grand-ducal où les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces personnes.

L'inscription des personnes physiques sur un ou plusieurs registres d'opt out se fait sans frais pour ces personnes.

Est puni d'une amende de dix mille un à deux cent mille francs, tout prestataire n'ayant pas respecté le souhait des personnes inscrites sur un ou plusieurs registres d'opt out.

TITRE V. DES CONTRATS CONCLUS PAR VOIE ELECTRONIQUE

Chapitre 1er. - Dispositions communes

Art. 49. Définitions

«Support durable»: tout instrument qui permet au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées.

«Service financier»: tout service fourni par un établissement de crédit, un autre professionnel du secteur financier ou une entreprise d'assurance et de réassurance.

Art. 50. Champ d'application

(1) Le présent titre s'applique aux contrats conclus par voie électronique entre professionnels, et entre professionnels et consommateurs, à l'exception des contrats suivants:

- les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location;
- les contrats pour lesquels la loi requiert l'intervention des tribunaux, d'autorités publiques ou de professions exerçant une autorité publique;

- les contrats de sûretés et les garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale;
- les contrats relevant du droit de la famille ou du droit des successions.

(2) Les dispositions des articles 53 à 59 s'appliquent uniquement entre professionnels et consommateurs.

Art. 51. Informations «techniques» générales à fournir

(1) Sans préjudice de l'obligation générale d'information de l'article 5 de la présente loi et, sauf si les parties sont des professionnels et en ont convenu autrement, les modalités de formation d'un contrat par voie électronique doivent être transmises par le prestataire de manière claire et non équivoque et préalablement à la conclusion du contrat. Les informations à fournir doivent porter notamment sur:

a) les différentes étapes techniques à suivre pour conclure le contrat;
b l'archivage ou non du contrat par le prestataire une fois celui-ci conclu et son accessibilité;
c les moyens techniques pour identifier et corriger les erreurs commises dans la saisie des données avant que le contrat ne soit conclu;
d les langues proposées pour la conclusion du contrat.

(2) Les clauses contractuelles et les conditions générales doivent être fournies au destinataire du service de manière à lui permettre de les conserver et de les reproduire.

(3) Les deux premiers paragraphes du présent article ne s'appliquent pas aux contrats entre personnes n'agissant pas dans le cadre de leurs activités commerciales ou professionnelles conclus exclusivement par échange de courrier électronique ou par des communications individuelles équivalentes.

Art. 52. Du moment de la conclusion du contrat

(1) Sauf si les parties qui sont des professionnels en ont convenu autrement, dans les cas où il est demandé à un destinataire du service d'exprimer son consentement en utilisant des moyens technologiques, pour accepter l'offre du prestataire, le contrat est conclu quand le destinataire du service a reçu, par voie électronique, de la part du prestataire l'accusé de réception de l'acceptation du destinataire du service.

a) L'accusé de réception de l'acceptation est considéré comme étant reçu lorsque le destinataire du service peut y avoir accès;
b le prestataire est tenu d'envoyer immédiatement l'accusé de réception de l'acceptation.

(2) Les dispositions du premier paragraphe du présent article ne sont pas applicables aux contrats entre personnes n'agissant pas dans le cadre de leurs activités commerciales ou professionnelles conclus exclusivement au moyen d'un échange de messages électroniques ou au moyen de communications individuelles équivalentes.

Chapitre 2.- Des contrats conclus avec les consommateurs

Art. 53. Informations préalables à fournir au consommateur

(1) Sans préjudice de l'obligation générale d'information de l'article 5 de la présente loi et des obligations d'information spécifiques aux services financiers, en temps utile avant la conclusion du contrat, le prestataire a l'obligation de fournir au consommateur, de manière claire et compréhensible les informations suivantes:

- les coordonnées du prestataire de service de certification le cas échéant accrédité auprès duquel ce dernier a obtenu un certificat;
- les caractéristiques essentielles du produit ou du service proposé;
- la monnaie de facturation;
- la durée de validité de l'offre et du prix;
- les modalités et modes de paiement, les conséquences d'une mauvaise exécution ou d'une inexécution des engagements du prestataire;
- le cas échéant, les conditions de crédit proposées;
- l'existence ou l'absence d'un droit de rétractation;
- le mode de remboursement des sommes versées le cas échéant par le consommateur en cas de rétractation de sa part;
- le coût de l'utilisation du service de la société de l'information lorsqu'il est calculé sur une autre base que le tarif de base;
- les conditions des garanties commerciales et du service après-vente existants;
- l'absence d'une confirmation des informations, le cas échéant;
- pour les contrats portant sur la fourniture durable ou périodique d'un produit ou d'un service, la durée minimale du contrat.

(2) Ces informations doivent être fournies par tout moyen adapté au service de la société de l'information utilisé, et accessibles à tout stade de la transaction.

Lorsqu'il est en mesure de le faire, le prestataire doit mettre en place un service de la société de l'information permettant au consommateur de dialoguer directement avec lui.

(3) Pour les produits et services qui ne sont pas soumis à un droit de rétractation conformément à l'article 55§4, les informations additionnelles suivantes doivent être fournies au consommateur:

- les caractéristiques du système d'exploitation ou de l'équipement nécessaire pour utiliser de manière efficace le produit ou le service commandé;
- le temps approximatif et le coût du téléchargement éventuel d'un produit ou d'un service, et le cas échéant les modalités et conditions du contrat de licence.

Art. 54. De la confirmation et de l'enregistrement des informations

(1) Le consommateur doit recevoir, au plus tard lors de la livraison du produit ou de l'exécution de la prestation de service, sur un support durable à sa disposition et auquel il ait accès, la confirmation des informations mentionnées à l'article 53 et, quand il y a lieu, les conditions d'exercice du droit de rétractation.

(2) Le §1 ne s'applique pas aux services dont l'exécution elle-même est réalisée au moyen d'un service de la société de l'information, dès lors que ces services sont fournis en une seule fois et qu'ils sont facturés par le prestataire.

(3) Le prestataire doit permettre au consommateur d'obtenir, dans les meilleurs délais après la conclusion du contrat, sur support durable le contenu de la transaction précisant notamment la date et l'heure de la conclusion du contrat.

Art. 55. Du droit de rétractation du consommateur

(1) Pour tout contrat conclu par voie électronique, le consommateur dispose d'un délai de sept jours pour se rétracter, sans indication de motif et sans pénalités.

Toutefois, si le consommateur n'a pas reçu la confirmation prévue à l'article 54, le délai de rétractation est de 3 mois.

Le délai de rétractation est porté à 30 jours pour les contrats relatifs aux polices d'assurance sauf les polices visées au §4 g) du présent article, et aux opérations de pension.

Ces délais courent:

- pour les services, à compter du jour de la conclusion du contrat;

- pour les produits, à compter de la réception du produit.

(2) Si cette confirmation intervient pendant le délai de trois mois visé au §1, le délai de sept jours recommence à courir à compter du jour de la réception des informations par le consommateur.

(3) Le consommateur exerce son droit de rétractation sur tout support durable.

En outre, le consommateur doit être remboursé dans les 30 jours des sommes qu'il a, le cas échéant, versées en paiement.

(4) Sauf convention contraire, le consommateur ne peut exercer le droit de rétractation prévu au §1 pour les contrats:

a) de fourniture de services dont l'exécution a commencé, avec l'accord du consommateur, avant la fin du délai de rétractation de sept jours prévu au §1;
b de fournitures de produits confectionnés selon les spécifications du consommateur ou nettement personnalisés ou qui, du fait de leur nature, ne peuvent pas être réexpédiés ou sont susceptibles de se détériorer ou de se périmer rapidement;
c de fourniture d'enregistrements audio ou vidéo ou de logiciels informatiques descellés ou téléchargés par le consommateur;
d de fourniture de journaux, périodiques et de magazines;
e de services de paris et de loteries;
f de services financiers dont le prix dépend des fluctuations du marché financier en dehors du contrôle du prestataire, qui peuvent survenir durant la période de rétractation, tels que les services relatifs:
   - aux opérations de change;
   - aux instruments du marché monétaire;
   - aux valeurs mobilières et autres titres négociables;
   - aux OPCVM et autres systèmes de placement collectif;
   - aux contrats à terme (futures) et options;
   - aux contrats à terme sur taux d'intérêt (FRA);
   - aux contrats d'échange (swaps) sur taux d'intérêt, sur devises ou aux contrats d'échange sur des flux liés à des actions ou à des indices d'actions (equity swaps);
   - aux options visant à acheter ou à vendre tout instrument relevant de la présente liste, y compris les contrats à terme et options;
g les polices d'assurance de moins d'un mois.

(5) Lorsque le prix d'un service est entièrement ou partiellement couvert par un crédit accordé au consommateur par le prestataire ou par un tiers, sur la base d'un accord conclu entre ce dernier et le prestataire, l'exercice par le consommateur de son droit de rétractation entraîne la résiliation, sans pénalité, du contrat de crédit.

Art. 56. Du paiement du service financier fourni avant la rétractation

(1) Quand le consommateur exerce son droit de rétractation conformément à l'article 55, il ne peut être tenu qu'au paiement de la partie du prix proportionnellement au service financier effectivement fourni par le prestataire.

(2) Le prestataire ne peut exiger du consommateur un paiement sur la base du §1 s'il n'a pas rempli son obligation d'information prévue à l'article 53, ni s'il a commencé à exécuter le contrat avant la fin du délai de rétractation sans que le consommateur ait expressément donné son consentement à cette exécution.

(3) Le prestataire renvoie, dans les meilleurs délais et au plus tard dans les 30 jours, au consommateur toutes sommes qu'il a perçues de ce dernier en accord avec le contrat conclu, excepté le montant à payer au §1 du présent article. Ce délai court du jour où le prestataire a reçu la notification de la rétractation par le consommateur.

(4) Le consommateur renvoie au prestataire toute somme ou propriété qu'il a reçue du prestataire, dans les meilleurs délais et au plus tard dans les trente jours. Ce délai court du jour de l'envoi de la notification de la rétractation par le consommateur.

Art. 57. De la fourniture non demandée

(1) Sans préjudice des règles applicables en matière de reconduction tacite des contrats, la fourniture d'un produit ou d'un service non demandée à un consommateur est interdite, lorsqu'elle est assortie d'une demande de paiement.

(2) Le consommateur n'est tenu à aucun engagement relatif aux fournitures de biens ou de services qu'il n'a pas expressément demandées, l'absence de réponse ne valant pas consentement.

Art. 58. De la charge de la preuve

La preuve de l'existence d'une information préalable, d'une confirmation des informations, du respect des délais et du consentement du consommateur incombe au prestataire. Toute clause contraire est considérée comme abusive au sens de l'article 1er de la loi modifiée du 25 août 1983 relative à la protection juridique du consommateur.

Art. 59. Exemptions

Les articles 53, 54 et 55 ne s'appliquent pas:

- aux contrats de fourniture de denrées alimentaires, de boissons ou d'autres biens ménagers de consommation courante fournis au domicile d'un consommateur, à sa résidence ou à son lieu de travail;
- aux contrats de fourniture de services d'hébergement, de transports, de restauration, de loisirs, lorsque le prestataire s'engage, lors de la conclusion du contrat, à fournir ces prestations à une date déterminée ou à une période spécifiée.

TITRE VI. DE LA RESPONSABILITE DES PRESTATAIRES INTERMEDIAIRES

Art. 60. Simple transport

(1) Le prestataire de service de la société de l'information qui transmet sur un réseau de communication, des informations fournies par un destinataire du service ou qui fournit un accès au réseau de communications ne peut voir sa responsabilité engagée pour les informations transmises à condition:

a) qu'il ne soit pas à l'origine de la transmission;
b qu'il ne sélectionne pas le destinataire de la transmission; et c) qu'il ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

(2) Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises à condition que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communications et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

Art. 61. Forme de stockage dite caching

Le prestataire qui fournit un service de la société de l'information consistant dans la transmission sur un réseau de communications des informations fournies par un destinataire du service ne peut pas voir sa responsabilité engagée pour le stockage automatique, intermédiaire et temporaire de cette information fait avec le seul objectif de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service à condition:

a) qu'il ne modifie pas l'information;
b qu'il se conforme aux conditions d'accès de l'information;
c qu'il se conforme aux règles concernant la mise à jour de l'information, indiquée d'une manière largement reconnue et utilisée par l'industrie;
d qu'il n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information, et
e qu'il agisse promptement pour retirer l'information qu'il a stockée ou pour rendre l'accès à celle-ci impossible, dès qu'il a effectivement connaissance du fait que l'information a été retirée là où elle se trouvait initialement sur le réseau, ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'une autorité judiciaire ou administrative a ordonné le retrait de l'information ou interdit son accès.

Art. 62. Hébergement

(1) Sans préjudice des dispositions de l'article 63§2, le prestataire qui fournit un service de la société de l'information consistant dans le stockage des informations fournies par un destinataire du service, ne peut pas voir sa responsabilité engagée pour les informations stockées à la demande d'un destinataire du service à condition que:

a) le prestataire n'ait pas effectivement connaissance que l'activité ou l'information est illicite et, en ce qui concerne une action en dommages, qu'il n'ait pas connaissance de faits ou de circonstances selon lesquels le caractère illicite de l'activité ou de l'information est apparent; ou
b le prestataire, dès le moment où il en a une telle connaissance, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

(2) Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.

Art. 63. Obligation en matière de surveillance

(1) Pour la fourniture des services visés aux articles 60 à 62, les prestataires ne sont pas tenus d'une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni d'une obligation générale de rechercher des faits ou circonstances indiquant des activités illicites.

(2) Pour la fourniture des services visés à l'article 62, les prestataires sont toutefois tenus à une obligation de contrôle spécifique afin de détecter de possibles infractions aux articles 383, alinéa 2 et 457-1 du Code pénal.

(3) Les paragraphes 1 et 2 du présent article sont sans préjudice de toute activité de surveillance, ciblée ou temporaire, demandée par les autorités judiciaires luxembourgeoises lorsque cela est nécessaire pour sauvegarder la sûreté, la défense, la sécurité publique et pour la prévention, la recherche, la détection et la poursuite d'infractions pénales.

TITRE VII. DES PAIEMENTS ELECTRONIQUES

Art. 64. Définitions

Pour l'application du présent titre, il faut entendre par:

(1) «instrument de paiement électronique»: tout système permettant d'effectuer par voie entièrement ou partiellement électronique, les opérations suivantes:

a) des transferts de fonds;

b) des retraits et dépôts d'argent liquide;

c) l'accès à distance à un compte;

d) le chargement et le déchargement d'un instrument de paiement électronique rechargeable.

(2) «instrument de paiement électronique rechargeable»: tout instrument de paiement électronique sur lequel des unités de valeur sont stockées électroniquement.

Art. 65. Champ d'application

(1) Les dispositions de la présente loi ne s'appliquent pas:

a) aux transferts électroniques de fonds réalisés par chèque et aux fonctions de garantie des transferts de fonds réalisés par chèque;
b aux transferts électroniques de fonds réalisés au moyen d'instruments rechargeables sans accès direct à un compte pour le chargement et le déchargement, et qui ne sont utilisables qu'auprès d'un seul vendeur de produits ou de services.

Art. 66. La preuve des paiements effectués

L'émetteur doit conserver un relevé interne des opérations effectuées à l'aide d'un instrument de paiement électronique, pendant une période de trois ans à compter de l'exécution des opérations.

Art. 67. La charge de la preuve

L'émetteur doit, en cas de contestation d'une opération effectuée à l'aide d'un instrument de paiement électronique, apporter la preuve que l'opération a été correctement enregistrée et comptabilisée, et n'a pas été affectée par un incident technique ou une autre défaillance.

Art. 68. Des risques liés à l'utilisation d'un instrument de paiement électronique

(1) Le titulaire d'un instrument de paiement électronique a l'obligation de notifier à l'émetteur – ou à l'entité désignée par lui – dès qu'il en a connaissance, la perte ou le vol de cet instrument ou des moyens qui en permettent l'utilisation, ainsi que toute utilisation frauduleuse; ainsi que la perte ou le vol de l'instrument de paiement électronique rechargeable.

L'émetteur d'un instrument de paiement électronique doit mettre à la disposition du titulaire les moyens appropriés pour effectuer cette notification et pour rapporter la preuve qu'il l'a effectuée.

(2) Sauf dans les cas où il s'est rendu coupable d'une fraude ou de négligence grave, le titulaire d'un instrument de paiement électronique visé à l'article 64§1 a), b) et c):

- assume jusqu'à la notification prévue au paragraphe précédent les conséquences liées à la perte, au vol ou à son utilisation frauduleuse par un tiers, à concurrence d'un montant fixé par règlement grand-ducal. Ce montant ne peut dépasser 150 euros.

Par dérogation à l'alinéa 1 du paragraphe 2 du présent article, l'émetteur n'est pas responsable de la perte de la valeur stockée sur l'instrument de paiement électronique rechargeable, lorsque celle-ci est la conséquence de l'utilisation de celui-ci par un tiers non autorisé, même après la notification prévue dans le présent article.

- est dégagé de toute responsabilité de l'utilisation de l'instrument de paiement électronique visé à l'article 64§1 a), b) et c) après la notification.

(3) En toute hypothèse, l'utilisation d'un instrument de paiement électronique sans présentation physique de celui-ci ou identification électronique, n'engage pas la responsabilité de son titulaire.

Art. 69. Irrévocabilité des instructions de paiement

Le titulaire ne peut révoquer une instruction qu'il a donnée au moyen de son instrument de paiement électronique, à l'exception de celle dont le montant n'est pas connu au moment où l'instruction est donnée.

TITRE VIII. DISPOSITIONS FINALES

Art. 70. Le Ministre de l'Economie est autorisé à procéder à l'engagement pour les besoins de l'Autorité d'Accréditation et de Surveillance de trois agents de la carrière supérieure de l'Etat, à occuper à titre permanent et à tâche complète. Les engagements définitifs de personnel au service de l'Etat se feront par dépassement de l'effectif total du personnel et en dehors du nombre d'engagements de renforcement déterminé dans la loi du 24 décembre 1999 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2000.

Art. 71. (1) Par règlement grand-ducal il peut être créé un comité «commerce électronique» regroupant des utilisateurs tant du secteur public que du secteur privé. Un règlement grand-ducal fixe la composition de ce comité.

(2) Ce comité aura pour objectif d'accompagner l'application de la présente loi, de diffuser des informations sur le commerce électronique et de produire des avis pour le ministère compétent.

Art. 72. Dans toute disposition légale ou réglementaire future, la référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes de «loi du 14 août 2000 relative au commerce électronique».

Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité commerce électronique

Art. 1er. Au sens du présent règlement, on entend par:

1° *Données afférentes à la création de signature:* des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique.

2° *Dispositif de création de signature:* un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature.

3° *Dispositif sécurisé de création de signature:* dispositif de création de signature qui satisfait aux exigences prévues à l'article 4 du présent règlement grand-ducal.

4° *Données afférentes à la vérification de signature:* des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisés pour vérifier la signature électronique.

5° *Dispositif de vérification de signature:* un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature.

6° *Certificat:* une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne.

7° *Certificat qualifié:* un certificat qui satisfait aux exigences visées à l'article 2 du présent règlement et qui est fourni par un prestataire de service certification satisfaisant aux exigences de l'article 3 du présent règlement.

8° *Produit de signature électronique:* tout produit matériel ou logiciel, ou élément spécifique de ce produit destiné à être utilisé par un prestataire de service de certification pour la fourniture de services de signature électronique ou destiné à être utilisé pour la création ou la vérification de signatures électroniques.

9° Signature électronique du prestataire de service de certification délivrant des certificats qualifiés, une signature électronique qui satisfait aux exigences suivantes:

- être liée uniquement au signataire;
- permettre d'identifier le signataire;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et
- être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

CHAPITRE I - EXIGENCES RELATIVES AU CERTIFICAT QUALIFIE

Art. 2. (1) Tout certificat qualifié doit contenir les informations suivantes:

1° une mention spécifiant que le certificat est délivré à titre de certificat qualifié;

2° l'identification du prestataire de service de certification, ainsi que le pays dans lequel il est établi;

3° le nom du signataire ou un pseudonyme qui est identifié comme tel;

4° les données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;

5° l'indication du début et de la fin de la période de validité du certificat, qui ne peut dépasser 3 ans;

6° le code d'identité du certificat;

7° la signature électronique du prestataire de service de certification délivrant des certificats qualifiés tel que prévu à l'Art.1. point 9°.

(2) Le certificat qualifié contient également, selon les cas, les informations suivantes:

1° une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné;

2° l'accréditation du prestataire de service de certification;

3° les limites à l'utilisation du certificat, ainsi que les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé.

(3) Le Ministre ayant la normalisation dans ses compétences publie au Mémorial les références des normes ou réglementations techniques généralement admises y compris nationales, relatives au certificat qualifié, avec renvoi au présent règlement.

CHAPITRE II - EXIGENCES RELATIVES AUX PRESTATAIRES DE SERVICE DE CERTIFICATION DELIVRANT DES CERTIFICATS QUALIFIES

Art. 3. (1) Un prestataire de service de certification doit:

1° faire la preuve qu'il est suffisamment fiable pour fournir des services de certification;

2° assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat;

3° veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;

4° vérifier, sur présentation d'un document officiel d'identité, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;

5° avoir recours à du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, plus particulièrement, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;

6° utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument;

7° prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données;

8° disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la loi et les règlements grand-ducaux, en particulier pour endosser la responsabilité de dommages;

9° enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant un délai d'au moins dix ans, à dater de sa délivrance, en particulier, pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;

10° ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés;

11° utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de telle sorte que:

- seules les personnes autorisées puissent introduire et modifier des données,
- l'information puisse être contrôlée quant à son authenticité,
- les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et
- toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

(2) Le Ministre ayant la normalisation dans ses compétences publie au Mémorial les références des normes ou réglementations techniques généralement admises y compris nationales, relatives au prestataire de service de certification délivrant des certificats qualifiés, avec renvoi au présent règlement.

Ne sont pas publiées au Mémorial, les normes relatives aux produits de signature électronique, dont les numéros de référence ont été publiés au Journal officiel des Communautés européennes.

CHAPITRE III - EXIGENCES RELATIVES AUX DISPOSITIFS SECURISES DE CREATION DE SIGNATURE ELECTRONIQUE

Art. 4. (1) Les dispositifs sécurisés de création de signature doivent garantir, par les moyens techniques et les procédures appropriés, que:

1° les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée;

2° l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles;

3° les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par des tiers.

(2) Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

(3) Le Ministre ayant la normalisation dans ses compétences publie au Mémorial les références des normes ou réglementations techniques généralement admises y compris nationales relatives aux produits de signature électronique, avec renvoi au présent règlement, à l'exception des normes relatives aux produits de signature électronique, dont les numéros de référence ont été publiés au Journal officiel des Communautés européennes.

Sont également publiés au Mémorial avec renvoi au présent règlement la référence aux dispositifs sécurisés de création de signature électronique qui ont été certifiés conformes aux exigences définies au présent article par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

CHAPITRE IV – PAIEMENT ELECTRONIQUE

Art. 5. Sauf dans les cas où il s'est rendu coupable d'une fraude ou d'une négligence grave, le titulaire d'un instrument de paiement électronique assume jusqu'à la notification prévue à l'article 68 §1 de la loi du 14 août 2000 relative au commerce électronique les conséquences liées à la perte, au vol ou à son utilisation frauduleuse par un tiers, à concurrence d'un montant de 150 euros.

CHAPITRE V - CREATION DU COMITE « COMMERCE ELECTRONIQUE »

Art. 6. Il est institué auprès du Ministère de l'Economie un organisme consultatif appelé Comité commerce électronique, ci-après dénommé le Comité.

Art. 7. Le Comité a pour missions:

1° d'assurer que toutes les parties intéressées soient associées aux activités dans ce domaine;

2° de contribuer à la clarification des exigences concernant les certificats qualifiés;

3° de contribuer à la clarification des exigences concernant les prestataires délivrant les certificats qualifiés;

4° de contribuer à la clarification des exigences concernant les dispositifs sécurisés de création de signature électronique;

5° de faire des recommandations pour la vérification sécurisée de la signature;

6° de diffuser les informations sur le commerce électronique;

Art. 8. Le Comité comprend les membres suivants:

1° cinq nommés sur proposition des Ministres ayant dans leurs attributions l'État, l'Economie, la Justice, les Classes Moyennes et les Finances;

2° un membre nommé sur proposition de l'Office Luxembourgeois d'Accréditation et de Surveillance (OLAS);

3° un membre nommé sur proposition de l'Organisme luxembourgeois de normalisation;

4° trois membres nommés sur proposition des chambres professionnelles patronales;

5° deux membres choisis pour leur compétence particulière dans la matière;

6° un membre représentant les consommateurs.

Les membres sont nommés par le Ministre ayant dans ses attributions l'Economie.

Le Ministre ayant dans ses attributions l'Economie nomme un président et un vice-président parmi les membres du Comité.

Le mandat est accordé pour une durée de trois ans. Il est renouvelable.

Art. 9. Il est adjoint au Comité un secrétariat dont la gestion est assurée par un agent désigné par le Ministre ayant dans ses attributions l'Economie.

Art. 10. Le Comité se réunit sur convocation de son président.

Le président doit convoquer le Comité sur demande d'au moins trois de ses membres.

Art. 11. Des experts peuvent être appelés à assister aux réunions.

Art. 12. A défaut d'avis spécifique, le procès-verbal de la réunion fait figure d'avis du Comité. Il indique le point de vue de la majorité simple des membres du Comité. Les membres qui sont d'un avis différent ont le droit d'y faire insérer leur point de vue. Le procès-verbal est soumis pour approbation aux membres du Comité pour être transmis au Ministre ayant dans ses attributions l'Economie.

Art. 13. Le Comité peut constituer des groupes de travail chargés de préparer une étude ou un avis à soumettre au Comité dans des matières spécifiques.

Art. 14. Un jeton de présence, à fixer par arrêté motivé du Gouvernement en Conseil, est alloué par séance aux membres présents du Comité, aux groupes de travail, aux experts présents ainsi qu'à l'agent assurant la gestion du secrétariat du Comité.

EXTRAITS DU CODE CIVIL relatifs à la preuve

Chapitre VI: De la preuve des obligations et de celle du paiement

Art. 1315. Celui qui réclame l'exécution d'une obligation doit la prouver.

Réciproquement, celui qui se prétend libéré, doit justifier le paiement ou le fait qui a produit l'extinction de son obligation.

Art. 1316. Les règles qui concernent la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment, sont expliquées dans les sections suivantes.

Section I - De la preuve littérale

Paragraphe Ier: - Du titre authentique

Article 1317. L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.

Art. 1318 L'acte qui n'est point authentique par l'incompétence ou l'incapacité de l'officier, ou par un défaut de forme, vaut comme écriture privée, s'il a été signé des parties.

Art. 1319. L'acte authentique fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers ou ayants cause.

Néanmoins, en cas de plaintes en faux principal, l'exécution de l'acte argué de faux sera suspendue par la mise en accusation; et, en cas d'inscription de faux faite incidemment, les tribunaux pourront, suivant les circonstances, suspendre provisoirement l'exécution de l'acte.

Art. 1320. L'acte, soit authentique, soit sous seing privé, fait foi entre les parties, même de ce qui n'y est exprimé qu'en termes énonciatifs, pourvu que l'énonciation ait un rapport direct à la disposition. Les énonciations étrangères à la disposition ne peuvent servir que d'un commencement de preuve.

[Art. 1321.]

Paragraphe II. - De l'acte sous seing privé

Art. 1322. L'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique.

Art. 1322-1. (L. 14 août 2000) La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.

Elle peut être manuscrite ou électronique.

La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article.

Art. 1322-2. L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive.

Art. 1323. Celui auquel on oppose un acte sous seing privé, est obligé d'avouer ou de désavouer formellement son écriture ou sa signature.

Ses héritiers ou ayants-cause peuvent se contenter de déclarer qu'ils ne connaissent point l'écriture ou la signature de leur auteur.

Art. 1324. Dans le cas où la partie désavoue son écriture ou sa signature, et dans le cas où ses héritiers ou ayants-cause déclarent ne les point connaître, la vérification en est ordonnée en justice.

Art. 1325. Les actes sous seing privé qui contiennent des conventions synallagmatiques, ne sont valables qu'autant qu'ils ont été faits en autant d'originaux qu'il y a de parties ayant un intérêt distinct.

Il suffit d'un original pour toutes les personnes ayant le même intérêt.

Chaque original doit contenir la mention du nombre des originaux qui en ont été faits. Néanmoins le défaut de mention que les originaux ont été faits doubles, triples, etc., ne peut être opposé par celui qui a exécuté de sa part la convention portée dans l'acte.

(L. 14 août 2000) Le présent article ne s'applique pas aux actes sour seing privé revêtus d'une signature électronique.

Art. 1326. (L. 14 août 2000) L'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention de la somme ou de la quantité en toutes lettres. Cette mention doit être écrite de sa main ou être revêtue spécifiquement d'une signature électronique, si elle est indiquée également en chiffres, en cas de différence, l'acte sous seing privé vaut pour la somme écrite en toutes lettres, à moins qu'il ne soit prouvé de quel côté est l'erreur.

Art. 1327. Abrogé (L. 22 décembre 1986)

Art. 1328. Les actes sous seing privé n'ont de date contre les tiers que du jour où ils ont été enregistrés, du jour de la mort de celui ou de l'un de ceux qui les ont souscrits, ou du jour où leur substance est constatée dans les actes dressés par des officiers publics, tels que procès-verbaux de scellé ou d'inventaire.

[Art. 1328. à 1332.]

Art. 1333. (L. 14 août 2000) Les copies, lorsque le titre original ou un acte faisant foi d'original au sens de l'article 1322-2 subsiste, ne font foi que de ce qui est contenu au titre ou à l'acte, dont la représentation peut toujours être exigée.

Art. 1334. Lorsque le titre original ou l'acte faisant foi d'original au sens de l'article 1322-2 n'existe plus, les copies effectuées à partir de celui-ci, sous la responsabilité de la personne qui en a la garde, ont la même valeur probante que les écrits sous seing privé dont elles sont présumées, sauf preuve contraire, être un copie fidèle lorsqu'elles ont été réalisées dan le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal.

Paragraphe IV. - Des copies des titres

[Art. 1335 à **1340]**

Section II - De la preuve testimoniale

Art. 1341. (L. 22 décembre 1986) Il doit être passé acte devant notaires ou sous signatures privées de tous actes juridiques portant sur une somme ou valeur excédant celle qui est fixée par règlement grand-ducal, même pour dépôts volontaires, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre.

Art. 1342. Abrogé (L. 22 décembre 1986)

Art. 1343. (L. 22 décembre 1986) Celui qui a formé une demande excédant la somme prévue à l'article 1341, ne peut plus être admis à la preuve testimoniale, même en restreignant sa demande primitive.

Art. 1344. (L. 22 décembre 1986) La preuve testimoniale, sur la demande d'une somme même inférieure à celle qui est prévue à l'article 1341, ne peut être admise lorsque cette somme est déclarée être le restant ou faire partie d'une créance plus forte qui n'est point prouvée par écrit.

Art. 1345 et **1346.** abrogés (L. 22 décembre 1986)

Art. 1347. Les règles ci-dessus reçoivent exception lorsqu'il existe un commencement de preuve par écrit.

On appelle ainsi tout acte par écrit qui est émané de celui contre lequel la demande est formée, ou de celui qu'il représente, et qui rend vraisemblable le fait allégué.

(L. 22 décembre 1986) Peuvent être considérés par le juge comme équivalant à un commencement de preuve par écrit les déclarations faites par une partie lors de sa comparution personnelle, son refus de répondre ou son absence à la comparution.

Art. 1348. (L. 22 décembre 1986) Les règles ci-dessus reçoivent encore exception lorsque l'obligation résulte d'un des faits réglés par les articles 1371 à 1381 du Code civil ou lorsque l'une des parties, soit n'a pas eu la possibilité matérielle ou morale de se procurer une preuve littérale de l'acte, soit a perdu le titre qui lui servait de preuve littérale, par suite d'un cas fortuit ou d'une force majeure.

Alinéa 2 abrogé (L. 14 août 2000).

Règlement grand-ducal du 22 décembre 1986 pris en exécution des articles 1348 du code civil et 11 du code de commerce

Art. 1er. Les reproductions et enregistrements visés à l'article 1348 du code civil et à l'article 11 du code de commerce doivent satisfaire aux conditions suivantes:

a) être la reproduction ou l'enregistrement fidèle et durable du document original ou de l'information à l'origine de l'enregistrement;
est réputée durable toute reproduction indélébile de l'original et tout enregistrement qui entraîne une modification irréversible du support;

b être effectués de façon systématique et sans lacunes;

c être effectués selon des instructions de travail conservées aussi longtemps que les reproductions ou enregistrements;

d être conservés avec soin, dans un ordre systématique, et protégés contre toute altération.

Art. 2. Les règles suivantes doivent être observées pour la reproduction d'un document par micrographie, lorsque l'original est détruit:

1° les travaux doivent être surveillés par le dépositaire du document ou par une personne désignée comme responsable de l'opération;

2° la reproduction doit permettre de déterminer l'ordre de prise de vue;

3° les diverses phases de la reproduction doivent s'opérer strictement selon le schéma arrêté aux instructions de travail;

4° les principes d'indexage et de repérage des images doivent permettre à un tiers compétent d'accéder à l´image d'un document dans un temps raisonnable;

5° l'enregistrement doit faire l'objet d'un procès-verbal contenant les indications suivantes:

- nature et sujet des documents microfilmés;
- date de l'opération;
- nom de l'opérateur responsable;
- déclaration que les documents saisis ont été microfilmés de façon complète, régulière et sans altération.

Cette déclaration est à signer par l'opérateur responsable et doit être conservée, à moins qu´elle ne fasse l'objet d'un enregistrement à la suite des documents microfilmés.

6° la reproduction doit être parfaitement lisible et techniquement satisfaisante; la fidélité de la reproduction doit être vérifiée avant la destruction de l'original;

7° la reproduction doit être toujours disponible pour consultation par les personnes ayant droit de regard.

Art. 3.

1. Les règles suivantes s'appliquent aux programmes d'enregistrement informatiques:

a) la documentation de programme, les descriptions de fichiers et les instructions de programme doivent être directement lisibles et tenues soigneusement à jour sous la responsabilité de la personne en ayant la garde.
b les documents définis à l'alinéa a) ci-dessus doivent être conservés sous une forme communicable aussi longtemps que les enregistrements auxquels ils se réfèrent.

2. Si, pour une raison quelconque, les données enregistrées sont transférées d'un support informatique à un autre, la personne en ayant la garde doit démontrer leur concordance.

3. Les règles suivantes s'appliquent aux systèmes informatiques dans leur ensemble:

a) les systèmes doivent comporter les sécurités nécessaires pour éviter une altération des enregistrements;
b les systèmes doivent permettre de restituer à tout Instant les informations enregistrées sous une forme directement lisible.