

## Technologies de l'Information et de la Communication

Une réalité qui s'inscrit chaque jour  
davantage dans notre quotidien...

*TIC, voilà bien une expression à la mode. Ce n'est pourtant qu'un début, car les Technologies de l'Information et de la Communication, désormais fiables et inscrites dans un cadre juridique clair et cohérent, devraient d'ici peu consacrer l'explosion de la communication électronique par Internet.*

*C'est d'évidence la voie que le gouvernement entend privilégier pour communiquer dans le futur avec les citoyens et les entreprises. Mais, si enthousiasmant que soit le projet, l'affranchissement de la tutelle du papier qui en résulte n'ira pas sans soulever des questions. Petit éclairage des enjeux et des perspectives.*

### **RANGEZ LES PAPIERS**

C'est une évidence : il est actuellement difficile de se faire une idée précise de la manière et du rythme auxquels les nouvelles technologies de l'information et de la communication vont bouleverser notre environnement professionnel, et sans doute également bien des aspects de notre vie privée. Mais une chose paraît d'ores et déjà certaine : l'accès haut débit, via les connexions ADSL, couplé à la croissance exponentielle de la puissance des ordinateurs, tant personnel que professionnel, sera le coup d'accélérateur qui finira de généraliser l'utilisation de

l'Internet dans les entreprises, en particulier les PME, et de populariser l'Internet pour les particuliers. Avec un effet différé que toutes les études confirment : les utilisateurs du haut débit dépassent nettement les autres internautes dans l'ensemble des usages. Il n'y a pas de quoi en être étonné : l'augmentation de la qualité de l'information transmise a toujours été directement liée à la capacité du canal de transmission à transporter une plus grande quantité d'informations par unité de temps, tout en s'affranchissant des interférences, des bruits et de l'atténuation liée à la distance.

Même s'il est vrai que la connexion permanente à Internet n'est pas encore entrée dans les mœurs et que les fabricants de téléphones n'ont pas toujours tenu leurs promesses, tout est (ou sera à court terme) en place pour que les technologies de l'information et de la communication offrent une réponse satisfaisante à des demandes de plus en plus diversifiées. Pas besoin d'être un grand clerc pour comprendre que des produits comme la carte proton, des services comme le home banking, la finance on-line, les communications par e-mail ou autres SMS, GPRS et bientôt l'EMS, ont manifestement de beaux jours devant eux. Ceux qui ont encore des doutes sur la popularité de l'e-mail méditeront sur les prévisions de l'Institut International Corporation : près de 10 milliards de messages électroniques ont transité sur Internet fin 2000,



de l'affaire. A quoi bon envoyer des documents électroniques, si le temps et la facilité gagnés par rapport à la version papier sont perdus en vérifications et conjectures diverses ? Poser la question, c'est y répondre : toute analyse perd son objectif si l'on ne garde pas à l'esprit que l'utilisation de documents électroniques ne se conçoit que s'ils offrent les mêmes garanties que la version papier. S'emballer au son des promesses magnifiques du secteur ne se justifie pas, si la valeur probante des documents, messages et autres traces informatiques demeure incertaine. Et là, comme l'observent justement Didier Gobert et Etienne Montero dans un remarquable article <sup>4</sup>, mieux vaut toujours deux précautions qu'une : *"Si les garanties offertes par le papier (intégrité, stabilité, durabilité, possibilité de porter une signature au bas du texte contenant l'engagement de manière à lier physiquement ces deux éléments sur le même support) ne souffrent pas de discussion, force est d'admettre que l'informatique est, à cet égard, nettement sujette à caution. Rien n'est plus facile de modifier, reproduire ou effacer un document informatique. En tous cas, l'intégrité d'un document, sa conservation dans la durée, la permanence de son lien avec le fichier contenant une signature, sont largement tributaires de la fiabilité des systèmes"*.

#### Les projets à court terme ?

L'utilisation d'Internet combinée à des signatures électroniques avancées certifiées par un organisme accrédité, pour l'envoi des déclarations TVA, IPP, I.Soc et la déclaration à la sécurité sociale...

S'il faut bien reconnaître que le contrôle de l'accès par des mots de passe n'est plus vraiment d'actualité, il convient d'éviter de tomber dans un pessimisme de mauvais aloi. A l'heure actuelle, il n'est plus guère contesté que les différentes techniques de signatures électroniques, fiables techniquement, apportent, selon leur degré de sécurisation et de fiabilité, une solution tout à fait acceptable, voire même beaucoup plus sûre. Le tout, il faut le souligner, dans un cadre juridique désormais clair et cohérent. Voici plus d'un an déjà, la loi du 20 octobre 2000 (MB du 22 décembre 2000), en modifiant notamment l'article 1322 du Code civil, avait reconnu l'utilisation des nouveaux moyens de communication, comme la télécopie, le

courrier électronique et le télégramme, dans la procédure judiciaire et extrajudiciaire. Technologiquement neutre, une seconde loi datée du 9 juillet 2001, et fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, est ensuite venue compléter le processus de transposition des exigences de la directive 1999/93/CEE du 13 décembre 1999 visant à établir un cadre communautaire pour les signatures électroniques. Publiée au Moniteur du 29 septembre 2001, cette loi définit, en effet, les différents types de signatures électroniques (manuscrite, digitalisée et numérique, ordinaire et avancée) <sup>5</sup> et leurs effets juridiques, et régit les activités des prestataires de services de certification. Résultat : depuis le 9 octobre 2001, un document signé électroniquement peut donc être considéré comme un acte sous seing privé sur lequel, en cas de contestation, le juge pourra se prononcer de façon discrétionnaire.

Avant d'entrer dans le vif du sujet, une précision d'ordre méthodologique s'impose. Dans une matière aussi complexe, la compréhension passe nécessairement par une approche rigoureuse des différentes composantes. Voici donc comment nous allons procéder. C'est donc par un bref exposé terminologique, en l'occurrence une petite dizaine de définitions pour en comprendre le jargon, que nous débuterons. Tout aussi indispensable pour saisir la problématique, nous consacrons ensuite quelques lignes à l'aspect technique. Histoire de comprendre comment la signature électronique, les certificats numériques et les autorités de certification s'articulent entre eux. Outre la première réalisation concrète, depuis le projet pilote que l'Institut avait développé via le réseau Isabel, nous mettrons ensuite à plat les projets en cours en matière de déclarations électroniques. A la lumière des enseignements d'un récent colloque qui lui était entièrement consacré, Ph. Wacquier, Conseiller au Service juridique de l'Institut, proposera enfin quelques premiers éléments de réflexion sur les implications des nouvelles technologies de communication et d'information sur le nécessaire respect de notre secret professionnel. A l'heure où les perquisitions virtuelles semblent vouloir entrer dans les mœurs, son application aux documents dématérialisés, qui ne vont plus tarder à envahir massivement nos ordinateurs, ne coule pas vraiment de source.

Il nous faut enfin rendre à César ce qui lui appartient : cet article a été rédigé sur la base des enseignements procurés par deux colloques récents. Bien intéressant, le premier <sup>6</sup>, sous l'égide de la faculté de droit de l'UCL, était consacré à la problématique du couple "signature électronique et certification". Le second fut organisé par l'Institut Professionnel des Comptables et des Fiscalistes agréés sur le thème de la simplification fiscale. <sup>7</sup>

<sup>4</sup> D. GOBERT et Etienne MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *Journal des Tribunaux*, 17 février 2001, pp. 114-128.

<sup>5</sup> Vous trouverez la définition de ces termes dans notre petit glossaire.

<sup>6</sup> "Signature électronique et certification", UCL, Département de Droit privé, Centre de droit des obligations, 25 septembre 2001.

<sup>7</sup> Il vous est loisible de télécharger le texte des interventions sur les sites Internet suivants : <http://www.ipcf.be> et <http://www.alainzenner.com>.

**PETIT GLOSSAIRE**

**ALGORITHME.** Formule mathématique utilisée dans les opérations de chiffrement et de déchiffrement pour convertir les données lisibles en un format codé et une clé.

**AUTHENTIFICATION.** Dans un réseau, processus par lequel le système valide les informations relatives à la connexion de l'utilisateur. Un nom d'utilisateur et un mot de passe sont comparés à une liste autorisée et, si le système détecte une correspondance, l'accès est accordé dans la limite des permissions de cet utilisateur (Dictionnaire encyclopédique bilingue de la micro-informatique, Microsoft, p. 34).

**AUTORITES DE CERTIFICATION** (Certification Authority). Personne physique ou morale accréditée qui délivre et gère des certificats ou fournit d'autres services liés aux déclarations électroniques (art. 2, al. 2, 10° Loi du 9 juillet 2001). Dans la mesure où les prestataires de service étrangers peuvent également développer ce type d'activité en Belgique, leur nombre devrait croître sensiblement au cours des prochaines années.

**CERTIFICATS.** Outils indispensables, ils permettent aux individus et aux organisations de sécuriser les transactions, professionnelles et personnelles, qui se font par les réseaux de communication : ils associent votre identité à une paire de clés qui peuvent être utilisées pour crypter et signer des informations numériques. Sans trop entrer dans les détails, disons qu'il en existe deux sortes, en fonction du type de signature que vous utilisez. Pour les signatures électroniques qualifiées, il faut, en effet, un certificat qualifié, - ce qui suppose qu'il répond aux conditions énumérées dans l'annexe 1 de la loi du 9 juillet 2001 (voyez infra) -, émis par un prestataire de services de certification qui, lui-même, doit satisfaire aux conditions énumérées dans l'annexe 2 de cette même loi. Ils peuvent également être présentés électroniquement pour attester de votre identité ou de vos droits d'accès à des informations ou à des services en ligne...

**CERTIFICAT PRINCIPAL (ROOT CERTIFICATE).** Certificat numérique de l'autorité de certification. Dans ce certificat, la clé publique est utilisée pour vérifier la signature de l'autorité de certification. L'autorité de certification signe, avec la clé privée correspondante, tous les certificats qui sont délivrés. Le "Root Certificate" permet de confirmer que la clé publique et l'autorité de certification sont associées.

**CERTIFICAT QUALIFIE.** Attestation électronique qui lie des données afférentes à la vérification de la signature avancée à une personne physique ou morale, confirme l'identité de cette personne et comporte les mentions suivantes : 1) certificat qualifié ; 2) identité du prestataire ainsi que son pays d'établissement ; 3) nom ou pseudonyme du signataire et, le cas échéant, l'indication d'une qualité spécifique ; 4) données afférentes à la vérification de la signature ; 5) période de validité du certificat et son code d'identité ; 6) signature électronique avancée du prestataire qui délivre le certificat ; 7) les limites à son

utilisation ; 8) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé.

**CLE.** Nombre unique combiné avec du texte pour produire un message chiffré ou une signature électronique

**CRYPTOGRAPHIE.** Art de transformer des informations lisibles (texte) en des informations que seules les personnes autorisées peuvent lire. Au cours de ce processus, l'information est codée (chiffrée) de façon à ce que seul le destinataire puisse lire ou altérer le message. Il peut être intercepté mais n'est intelligible que pour la personne qui est capable de le décoder (déchiffrer).

**EDIFACT** (Electronic Data Interchange for Administration, Commerce and Transport). Norme internationale qui standardise la structuration des données de la déclaration T.V.A. dans un message électronique et qui précise donc comment ces données doivent y être structurées.

**HASH.** Empreinte numérique condensée du message électronique.

**PKI.** Le Forum PKI est une alliance internationale, sans but lucratif, regroupant de nombreux acteurs du secteur, dont le but est d'accélérer l'adoption et l'utilisation de l'Infrastructure de Clé Publique (PKI) ainsi que les produits et services PKI. Le Forum PKI prône la coopération des industries et la conscientisation du marché pour permettre aux organisations de comprendre et de tirer profit de la valeur ajoutée que représente le PKI dans leurs activités commerciales et de e-business.

**SIGNATURE ELECTRONIQUE ORDINAIRE.** Donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification (art. 2, al. 2°, 1° Loi du 9 juillet 2001). En cas de contestation, ce type de signature peut être qualifié par le juge, au terme d'un débat contradictoire, d'acte sous seing privé valable (art. 1322 Code civil), mais également d'écrit ordinaire.

**SIGNATURE ELECTRONIQUE AVANCEE.** Signature électronique réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique (art. 4, § 4 Loi du 9 juillet 2001), ce qui suppose qu'elle répond à un certain nombre de critères de sécurité technique. Dans ce cas, le juge n'a plus aucune liberté d'appréciation quant à la validité. Le document est irréfragablement considéré comme un acte sous seing privé et la signature est reconnue équivalente à la signature manuscrite.

**X400.** Standard international pour l'envoi des messages électroniques auquel l'expéditeur (l'assujetti) se soumet afin de vérifier avec certitude (à 100 %) si son message est bien arrivé chez le destinataire (le Ministère des Finances), et qui permet à ce dernier de vérifier la date exacte à laquelle le message lui a été expédié. De son côté, le destinataire accepte cette norme comme outil de vérification, lorsque l'information lui est parvenue.

## UN PEU DE TECHNIQUE

Même si les perspectives qu'il offre assurent au ciel des nouvelles technologies de la communication et de l'information un bleu profond, il y a de nombreuses raisons de penser que les nuages s'amoncelleront rapidement, si d'aventure un certain nombre de précautions d'usage ne sont pas prises. Plus que la nature de l'information transmise ou la vitesse de transfert des données, chacun perçoit combien il est essentiel de mettre en place, dans un réseau ouvert comme Internet, un mécanisme de sécurisation des communications électroniques. Ce mécanisme doit garantir la confidentialité, l'authentification (c'est-à-dire qu'il doit permettre à chaque partie d'identifier avec certitude l'autre partie) et la non répudiation (c'est dire qu'il doit faire en sorte que les parties prenantes d'une opération ne puissent pas ultérieurement prétendre qu'elles n'ont pas participé). Il importe également, et c'est le minimum minimorum, que la version électronique d'un document présente les mêmes qualités fonctionnelles que son équivalent papier d'un même document : lisibilité, stabilité et inaltérabilité.

Comme c'est le cas de la protection des transactions traditionnelles par des tiers, l'Internet a besoin d'outils modernes pour la gestion des risques. La technologie joue ici un rôle essentiel : ces garanties sont, en effet, actuellement offertes par la signature électronique et la certification des signatures électroniques. Qui dit certificat dit forcément autorité de délivrance. Trois éléments, nécessairement complémentaires, qui composent donc l'alchimie de la signature électronique, et dont il convient de bien comprendre l'articulation. Comment une signature électronique est-elle liée à l'utilisation d'un tel certificat numérique et à une paire de clés ? Quel est le rôle des autorités de certification ? Comment puis-je obtenir un certificat numérique ? Voilà, entre autres, quelques-unes des questions auxquelles nous allons répondre brièvement.<sup>8</sup>

Pour créer une signature numérique, la technique la plus utilisée, lorsque l'on travaille en système ouvert, est la cryptographie asymétrique. Derrière ce vocable quelque peu ésotérique se cache une réalité somme toute assez simple : pour signer un envoi électronique, vous disposez de deux clés, liées entre elles par des relations mathématiques. L'une est privée et il importe d'en préserver absolument la confidentialité. Si la clé privée est, en effet, utilisée par une autre personne, la signature reste parfaitement valable. La responsabilité de la confidentialité de la clé privée et du code repose, en effet, sur son titulaire. L'autre est publique. Il vous est loisible de la distribuer, car elle permet de vérifier les signatures. A une clé privée correspond donc toujours une clé publique et réciproquement. Bien que les clés ne soient que des expressions mathématiques, il est matériellement impossible de retrouver la clé privée au départ de la clé publique. Ceci posé, voyons le principe. Les données cryptées avec la clé privée sont décryptées avec la clé publique par le destinataire du message. En revanche, toute communication cryptée avec une clé publique est décryptée avec une clé privée. Pour

gagner la confiance des utilisateurs, il faut alors leur garantir que la clé publique qu'ils possèdent est bien celle du signataire de l'envoi. C'est le rôle des autorités de certification. La clé publique est, en effet, liée à l'identité du signataire par un certificat qui permet de diffuser l'information de cette identité. Équivalent électronique des permis de conduire, des passeports et des cartes de membres, le certificat est donc une attestation électronique qui lie les données afférentes à la vérification d'une signature, à une personne physique ou morale. Les autorités de certification (tiers certificateurs) se bornent à vérifier l'identité des titulaires de clé publique et à créer et délivrer des certificats. C'est la raison pour laquelle le certificat contient nécessairement la clé publique de l'utilisateur, son nom, une date de validité, le nom de l'autorité de certification qui a délivré le certificat, un numéro de série et quelques autres informations, ainsi que la signature ajoutée par l'autorité de certification à l'aide de sa propre clé privée (Root certificat). Le niveau de certification dépend de la façon dont l'identité de la personne a été vérifiée au cours du processus de requête du certificat. Globalement, il existe trois niveaux de certification (Certificats de Classe 1 à 3). Le Certificat de Classe 3, qui assure le niveau le plus important de certification nécessaire à un individu, et que vous pouvez utiliser pour les transactions à haute valeur commerciale, comme les opérations bancaires électroniques et le commerce d'actions boursières, correspond à un coût annuel de 2.400 BEF.

Mais nous ne sommes pas encore au bout de nos peines. A ce stade, rien ne prouve, en effet, que le message n'a pas subi d'altération en cours de route. Parallèlement à ce processus à double clé, il a donc fallu trouver un système pour assurer la fonction d'intégrité de la version papier. C'est ici qu'entre en scène le Hash Code, obtenu en appliquant un premier algorithme de cryptage (SHA-1) à l'ensemble du texte. Ce Hash, en l'occurrence un extrait du message réduit au format 160 bits, est encrypté au moyen de la clé privée du signataire (avec application d'un second algorithme de type RSA Rivest, Shamir, Adleman) et constitue la signature électronique.

La vérification de la signature digitale est opérée en comparant deux résultats : le décryptage du Hash Code, à l'aide de la clé publique du destinataire (cryptée au moyen du RSA), et l'application de l'algorithme au texte.

- Si l'extrait de 160 bits créé au départ est bien identique à celui obtenu lors du contrôle à l'arrivée, deux choses sont certaines : d'une part, la signature électronique a été créée en utilisant la clé privée du signataire. C'est donc l'assurance que la clé publique correspond à la clé privée de l'expéditeur,

<sup>8</sup> Cette partie est largement inspirée par les textes des exposés présentés, lors du colloque UCL du 25 septembre 2001, par Isabelle Goes et Erik Luysterborg "Présentation de la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification" et Yves Timmermans "Signature électronique et certification : le notariat et les nouvelles technologies".

de sorte que personne ne se fait passer pour le signataire. D'autre part, le texte n'a pas été altéré depuis sa signature.

- Si le résultat n'est pas identique, le message a été modifié entre l'envoi et la réception et il doit être rejeté.

Tout cela vous paraît bien compliqué ? Ne vous tracassez pas, ces opérations s'effectuent de manière totalement transparente. C'est l'ordinateur qui effectue le travail.

### Un petit exemple

Imaginons que A souhaite envoyer un message électronique sécurisé à B. Sa rédaction terminée, il le crypte – en d'autres mots, il le rend illisible – au moyen de sa clé privée. Le fichier obtenu constitue sa signature numérique. A sa réception, B peut le déchiffrer au moyen de la clé publique de A qu'il a pu télécharger auparavant. Dans ce cadre, l'autorité de certification compare les données fournies par A durant la procédure de requête de certificat en ligne et celles contenues dans sa base de données clients, identifie les intervenants et, grâce au certificat de clé publique, permet à B d'accéder à la clé publique de A, en garantissant qu'il s'agit bien de la sienne. Si l'opération réussit, B aura la certitude qu'il s'agit bien d'un message de A. S'il s'avère, par contre, que A n'a pas signé, le message sera rendu inutilisable et détruit.

Retournons à présent le sens de l'opération. Le message que B expédie devra nécessairement être chiffré avec la clé publique de A. De son côté, étant le (ou la) seul(e) à posséder la clé privée correspondante, A est également le seul qui puisse le déchiffrer.

Résumons. La clé privée est utilisée pour chiffrer le message et seule l'autre clé de la paire, liée à l'identité du titulaire par un certificat numérique, permet de le déchiffrer. Toute communication dont la signature est vérifiée positivement à l'aide d'une clé publique certifiée émane donc du titulaire du certificat. Toute communication cryptée à l'aide d'une clé publique ne pourra être décryptée que par le titulaire du certificat. Combinés avec le chiffrement, les certificats numériques fournissent donc une solution de sécurité complète assurant l'identité de toutes les parties impliquées dans une transaction. Si l'on ajoute que les plus courants (le type X 509) peuvent s'intégrer sans difficultés dans les principaux navigateurs ou logiciels de courrier électronique, voire même dans les versions les plus récentes des programmes de traitement de texte ou d'édition de documents mixtes, comme Acrobat, de sorte que la signature et le cryptage de documents électroniques n'impliquent plus le recours à des logiciels spécifiques, il y a fort à parier que nous aurons trouvé les arguments pour vous convaincre. Si tel n'est pas le cas, - 2 400 BEF pour introduire une déclaration, c'est effectivement beaucoup plus onéreux que la poste – sachez enfin qu'il ne s'agira pas du seul usage de votre certificat. Outre l'envoi sécurisé de vos courriers électro-

niques, l'identification sur les sites web, l'accès aux données privées et professionnelles protégées, comme des intranets ou d'autres réseaux de communication numériques, les transactions de faible valeur commerciale, les achats en ligne,... exigent de plus en plus de l'opérateur qu'il possède un certificat ...

Intéressé ? Pour obtenir votre certificat personnel, c'est très simple. Il suffit de prendre contact et d'examiner l'offre des opérateurs actuellement actifs sur le marché belge : Global Sign, Isabel, Belgacom ... Tout en ne perdant pas de vue que leur nombre devrait croître assez rapidement dans les prochaines années.

## UNE PREMIÈRE RÉALISATION CONCRÈTE : EDIVAT

Le Ministère des Finances a fait ses comptes : 2,8 millions, ni plus ni moins, de déclarations doivent être encodées manuellement chaque année. Une montagne de formulaires que deux projets, autant que faire se peut, devraient à court terme mettre à plat :

- Le scanning qui, dans un premier temps, visera la déclaration TVA, le relevé intracommunautaire, le listing client, mais également la déclaration au précompte professionnel, les matrices cadastrales.
- Le système EDIFACT (messages électroniques structurés), en l'occurrence la possibilité d'envoyer dans la mailbox de l'Administration, sous la forme d'un attachement à un e-mail, un maximum de 999 déclarations TVA (mensuelles ou trimestrielles), le tout au format EDIFACT et nécessairement via un réseau sécurisé de type X 400. Réserve dans les faits aux seuls professionnels comme les experts-comptables et les conseils fiscaux, ce mode d'envoi, qui offre une alternative crédible aux techniques de la signature électronique, implique la conclusion préalable d'un protocole d'accord avec l'Administration fiscale. Comme nous l'avons déjà signalé, l'envoi électronique des déclarations ne se conçoit évidemment que s'il présente les mêmes garanties de lisibilité, d'inaltérabilité, de durabilité et d'identification de la déclaration manuscrite. De son côté, l'Administration doit également pouvoir rendre à César ce qui lui appartient, en d'autres mots, identifier sans erreur l'expéditeur et l'identité de la déclaration parvenue. C'est la raison de l'existence de ce Protocole d'accord, au demeurant téléchargeable sur le site du Ministère des Finances.

Faisons le point. Au moment de terminer ces lignes, le scanning est toujours à l'état de projet. Planifié de janvier à fin septembre 2002, l'objectif est de mettre en place deux centres de scannage, l'un à Gand et l'autre à Namur, afin de remplacer l'encodage manuel de différents documents papier par une saisie électronique à l'aide de procédures automatisées. Basé à Bruxelles, un troisième centre

servira ensuite de back-up, tout en étant utilisé pour le scannage des matrices cadastrales. Mais, pour l'heure, le système profitera essentiellement à l'Administration, dans la mesure où les annexes à la déclaration devront toujours être envoyées sur support papier au bureau de TVA compétent. Par contre, on ne peut que se réjouir que l'archivage électronique possède déjà un cadre législatif. En vertu des dispositions de la loi du 5 septembre 2001, entrée en vigueur le jour de sa date de publication au Moniteur, le 13 octobre 2001, les données des déclarations (déclarations périodiques, listing annuel, relevé trimestriel des opérations intracommunautaires) et les renseignements qui sont enregistrés, conservés ou reproduits par l'Administration de la TVA selon un procédé photographique, optique, électronique ou par une autre technique de l'informatique ou de la télématique, ainsi que leur représentation sur un support lisible, ont force probante pour l'application de la TVA. Traduisez : les copies ou les reproductions obtenues au moyen des procédés visés par la loi ont la même force probante que les documents originaux, qu'ils soient en papier ou électronique.<sup>9</sup>

Développé en étroite collaboration avec l'Institut, le second projet, au demeurant fort proche dans son esprit des initiatives que nous avons prises en collaboration avec la société Isabel, nous intéresse davantage. Il mérite d'autant plus l'attention qu'il est opérationnel depuis plusieurs mois, les modifications nécessaires ayant été apportées à la législation.<sup>10</sup> Le site du Ministère des Finances vous en proposant un commentaire fort complet (<http://minfin.fgov.be/portail1/fr/cddeclarfr.html>), c'est donc par une présentation schématique des aspects techniques que nous débiterons.

Concrètement, la déclaration TVA électronique est envoyée à une adresse électronique (la mailbox) répertoriée sur un réseau sécurisé de type X 400, dont plusieurs (Belgacom, Isabel, GEIS, IBM) sont opérationnels en Belgique. Le choix est libre, dans la mesure où ce sont les opérateurs de ces réseaux qui doivent veiller à ce que les messages arrivent à destination, même si l'expéditeur et le destinataire d'un message se trouvent sur des réseaux différents. L'envoi se fait nécessairement au format EDIFACT.

Trois messages différents sont, en l'occurrence, utilisés au cours du processus d'envoi de la déclaration électronique.

- D'abord, la déclaration (message RDRMES) envoyée par l'assujetti concerné ou par le bureau comptable mandaté arrive dans la mailbox de l'Administration de la TVA. Les grilles qui ne sont pas remplies sur la déclaration papier ne seront pas enregistrées dans le message EDIFACT.
- L'Administration vérifie ensuite si le message est rédigé dans un format valable. Le résultat de ce contrôle formel se retrouve dans l'accusé de réception (CONTRL).
- Un contrôle du contenu complémentaire est enfin effectué, afin de vérifier si la déclaration peut être traitée par l'Administration. Si tel est le cas, le ré-

sultat de ce contrôle est confirmé par le deuxième volet de l'accusé de réception.

Lorsque ces différents contrôles sont positifs, c'est la mention "OK" qui figurera sur l'accusé de réception. L'expéditeur a aussi la certitude qu'une déclaration déterminée est reçue par l'Administration et qu'elle sera traitée. Si l'accusé de réception mentionne "Statut non OK", la déclaration sera réputée non introduite. Si le message contient plusieurs déclarations – rappelons qu'il est possible d'en introduire 999 au maximum par envoi –, le constat vaudra pour chacune d'entre elles. S'il y a des problèmes au niveau de l'expéditeur, du lay-out du message, ou lorsqu'il y a des fautes de contenu dans le message, l'expéditeur saura alors, sur base de codes, pour quelle raison la déclaration n'a pas été acceptée, et peut dans ce cas envoyer un nouveau message (correct).

Comme on l'imagine, ce mode d'envoi offre la possibilité d'introduire des déclarations en BEF ou en EUR, mais l'unité monétaire choisie, qui devra être indiquée sur l'enveloppe électronique, devra être uniforme par envoi. En d'autres mots, une déclaration en BEF dans une enveloppe EUR entraînera le rejet de tout l'envoi. Les montants utilisés ne contiennent pas de signe mais sont toujours positifs. Les montants en euros sont imprimés en eurocents et reproduits dans le message sans notation décimale.

Tel que nous venons de le décrire, ce système présente les avantages propres à toute communication sous forme électronique (les dates et heures certaines, la possibilité d'expédier les documents en dehors des heures d'ouverture de bureau à une seule adresse et la suppression des frais d'impression et d'expédition

liés au support papier), mais également des contraintes spécifiques. Dès lors qu'il permet de se passer du recours à la signature électronique, la première d'entre elles est certainement que les assujettis qui souhaitent l'utiliser doivent préalablement conclure un protocole d'accord avec l'Administration. Par sa signature, les parties s'enga-

#### EDIVAT en résumé

- Réseau X 400
- Format EDIFACT
- 999 déclarations max. par envoi
- Protocole d'accord
- Phase de test obligatoire d'une durée de trois mois maximum
- EUR OU BEF
- Même délai d'introduction que les déclarations manuscrites : au plus tard le 20 du mois suivant le mois ou le trimestre auquel la déclaration se rapporte.

<sup>9</sup> Vous trouverez un excellent résumé de l'état de la question dans les documents parlementaires (Doc. Parl., Chambre, 2000-2001, n° 1286/001 à 003).

<sup>10</sup> Un arrêté royal assez technique, daté du 5 septembre, modifiant les AR n° 1, 2, 3, 23 et 50 relatifs à la TVA et publié au Moniteur du 18 septembre 2001, a arrondi les angles. L'indication du lieu où les déclarations des assujettis doivent être envoyées a été modifiée. Dorénavant, il sera demandé aux assujettis d'envoyer leurs différentes déclarations ainsi que leur relevé intracommunautaire au "service indiqué par le Ministre des Finances". Les termes de la législation actuelle ("à l'office de contrôle de la TVA dont l'assujetti relève") ne permettaient pas cette possibilité. Il a donc fallu les modifier.

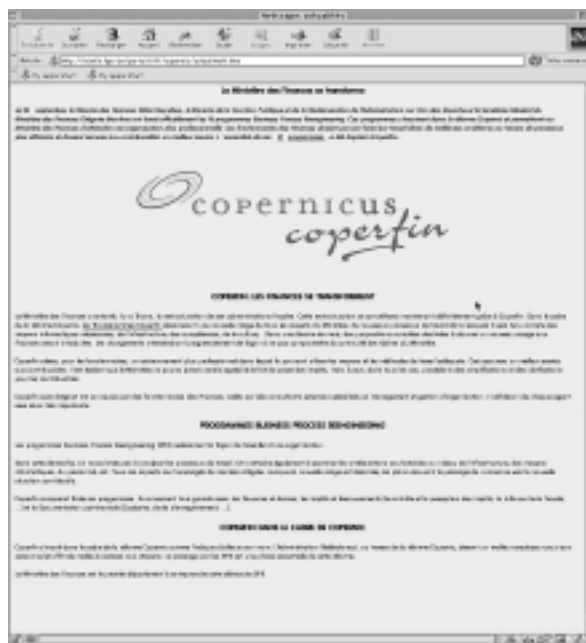
gent à reconnaître le fait de l'introduction et de l'identification, de l'intégrité, de l'authenticité et de la non réputation des données de déclarations introduites. L'Administration vérifiera pour chaque message reçu si tel contrat formel existe. Lors du contrôle du mandat, l'identifiant et l'adresse X 400 du mandataire ainsi que l'identifiant de la fiduciaire, seront vérifiés. Regrettons également qu'il n'est pas possible, à l'heure où nous terminons ces lignes (18/11/2001), d'expédier par la même voie le relevé trimestriel des livraisons intra-communautaires ainsi que le listing annuel des clients. Intéressé ? Introduisez une demande écrite à l'adresse e-mail suivante : [info.edivat@minfin.fed.be](mailto:info.edivat@minfin.fed.be) en mentionnant dans l'objet "CANDIDAT EDIVAT". L'Administration prendra rapidement contact et vous communiquera votre adresse X 400. Vous pourrez alors envoyer vos premières déclarations sur base desquelles l'Administration exécutera les tests nécessaires pour vérifier si le format du message correspond aux spécifications techniques et s'il n'y a pas de fautes de contenu dans le message. Pendant la phase de test, les déclarations papier doivent continuer à être introduites. La version électronique (mailbox) pourra ainsi être comparée avec la déclaration papier encodée dans les bureaux TVA concernés. Tout au long de la procédure de test, notez également qu'il vous sera loisible de prendre contact avec un responsable, sans qu'il soit question pour l'Administration d'assurer le help-desk pour chaque candidat de la phase de test. Si vous n'arrivez pas à envoyer des déclarations TVA valables pendant la période de test, la période de test sera alors considérée comme non réussie, et vous n'aurez pas accès à la phase opérationnelle. Parce qu'il permet l'envoi simultané de centaines de déclarations en un seul e-mail, ce système, par ailleurs intégré dans la plupart des logiciels comptables sous la forme d'une option gratuite, répond à un besoin spécifique des bureaux comptables et fiscaux d'une certaine dimension. Ce faisant, il n'entre pas vraiment en concurrence avec les autres projets pilotes que l'Administration

entend développer à court terme, comme la possibilité offerte, dès février 2002, aux assujettis d'introduire individuellement leurs déclarations par Internet. Même s'ils participent de la même logique, la technologie utilisée est différente, de même que les besoins rencontrés. Les projets de déclarations électroniques que nous présentons dans les lignes qui suivent impliquent, tous sans exception, l'utilisation de la signature électronique.

## LES PROJETS

### Trois axes d'actions complémentaires

1. Assurer une meilleure sécurité juridique, en améliorant la clarté et la cohérence des réglementations.
2. Réorganiser les modalités d'administration de l'impôt, en réorganisant les administrations fiscales dans une optique " client ", en rattrapant leur retard sur le plan informatique, et en changeant la mentalité des fonctionnaires des finances.
3. Alléger la paperasserie, en liaison étroite avec les organisations professionnelles intéressées.



<http://minfin.fgov.be/portail1/fr/copernic/cdbcopernicfr.html>

Après avoir mis en exergue ce qui est déjà du domaine du concret, ouvrons le tiroir à projets. On sait l'importance qu'accordent tout à la fois Didier Reynders et Alain Zenner <sup>11</sup> à la mise en place d'une administration efficace pourvue d'une nouvelle culture d'entreprise. Passant par une révision profonde de la conception de la mission du fisc et de ses valeurs, et la redéfinition des méthodes de travail sur le terrain, en un mot, le plan Copernic <sup>12</sup> (<http://minfin.fgov.be/portail1/fr/copernic/cdbcopernicfr.html>) n'aura rien d'une sinécure. Mais les projets sont

<sup>11</sup> Un simple clic sur leurs sites respectifs (<http://min.fin.f.gov.be> et <http://www.alainzenner.com>) démontre toute l'étendue et la diversité des projets en cours. Le catalogue des mesures envisagées que vous y découvrez vaut assurément le détour.

<sup>12</sup> Le plan Copernic s'appuie plus précisément sur 16 programmes "Business Process Reengineering", dits BPR, destinés à redessiner les tâches et processus de décision. Il poursuit un double objectif : 1. Créer un environnement plus professionnel susceptible d'offrir aux fonctionnaires des moyens adéquats. Le Ministre des Finances, Didier Reynders, précise à ce propos que ledit projet tient enfin compte des besoins de l'Administration fiscale en outillage informatique et personnel qualifié ; 2. Rendre aux contribuables un service performant et épuré de toute lourdeur administrative.

Le 8 octobre 2001, le planning de différents groupes de travail (particuliers, petites et moyennes entreprises, grandes entreprises et lutte contre la fraude) a été approuvé par un comité de pilotage. Des propositions, en principe finalisées en 2002, sont actuellement en cours de discussions autour de cinq axes stratégiques : proactivité de l'Administration ; transparence et égalité ; accessibilité de l'Administration et de l'information ; rapidité des services et simplification des interactions avec l'Administration, et concentration sur les activités à valeur ajoutée. Ce plan coûtera environ 400 millions de BEF au Trésor. Sa mise en oeuvre s'étalera sur une dizaine de mois, mais, globalement, ses effets à l'égard des citoyens se feront ressentir plus tardivement.

Le principe de la nouvelle culture fiscale <sup>13</sup> : la mission du fisc n'est pas de taxer à tout prix, mais de prélever le juste impôt

1. Contrôles à la fois plus efficaces et moins conflictuels, plus réalistes et moins tracassiers pour les contribuables.
2. Priorité accordée à la lutte contre la grande fraude, plus difficile il est vrai que le harcèlement des contribuables sur des questions de détail.
3. Rupture avec la pratique fiscale de toujours appliquer la loi fiscale de manière aussi restrictive que possible, indépendamment de son esprit.
4. Mise au placard par les agents taxateurs de leurs préjugés et a priori.
5. Retour aux principes, en gommant par exemple de l'esprit des fonctionnaires l'idée que "dans le doute, on taxe".
6. Application de la loi de manière raisonnable et uniforme dans l'ensemble du pays.

là, tout autant que la volonté politique et le travail d'arrache-pied pour les voir aboutir.

S'il est d'évidence trop tôt pour tirer un premier bilan, rien n'empêche toutefois de brosser un état de la situation, histoire de juger des avancées obtenues et des projets à concrétiser. Ils sont légion. La simplification des procédures fiscales, l'optimisation de la sécurité juridique, concrétisées notamment par la récente obligation de motiver tout accroissement d'impôt ou l'édition désormais régulière de brochures d'information sur les droits et les devoirs des contribuables/assujettis, notamment lors des contrôles fiscaux, compte ainsi parmi les éléments plus novateurs. S'y ajoute, au rang des projets, la suppression des timbres fiscaux, la réduction du nombre des registres dans le secteur de l'automobile, la mise à disposition d'une base de documentation fiscale, consultable gratuitement par tous les contribuables sur le site du Ministère des Finances, le téléchargement de formulaires fiscaux, sociaux, comptables... Toujours en concertation avec les organisations professionnelles, le plan d'action prévoit aussi, dans ce domaine, l'harmoni-

sation de la facturation, la dispense de certification dans les marchés publics, la suppression de l'obligation de facturer pour les opérations exemptées, l'amélioration <sup>14</sup> de la lisibilité des formulaires fiscaux... Last but not least, les "correspondants professionnels" du Ministère, comme les notaires (qui doivent informer le fisc préalablement à la vente d'immeubles) ou les huissiers (en cas de saisie) verront ces échanges d'information réglés de manière électronique.

Quoiqu'elle connaîtra encore quelques rebondissements, la simplification administrative et, ce qui est aujourd'hui au centre de nos préoccupations, les déclarations électroniques, valent d'évidence que l'on s'y intéresse de très près. Au risque de tailler dans des habitudes bien ancrées, c'est en effet In-

ternet, combiné à des signatures électroniques avancées certifiées par un organisme accrédité, qui servira de rampe de lancement à la plupart des communications avec l'Administration fiscale. Même si le système présentera un caractère facultatif, l'éventualité à plus long terme que certaines déclarations (T.V.A. et I.Soc.) ne puissent plus valablement être introduites que par la voie électronique, ne saurait toutefois être écartée d'un revers de la main. Chez nos voisins français, la loi oblige, en effet, désormais les entreprises réalisant plus de 100 millions de francs de chiffre d'affaires annuel à déclarer et à régler leur TVA en ligne, étant entendu que toutes les entreprises dont le chiffre d'affaires n'atteint pas le montant indiqué peuvent bien entendu bénéficier du système, bien qu'elles n'y soient pas contraintes.

#### a) Déclarations électroniques via Internet

Même si l'on n'en est pas encore là, quatre projets sont actuellement développés au sein du groupe de travail "e-government" aux réunions duquel l'Institut prend une part active.

#### Déclarations TVA - février 2002

L'objectif de ce projet est d'offrir à tous les déclarants TVA un moyen d'introduction de leurs déclarations TVA accessible via Internet. L'envoi des déclarations individuelles par Internet requiert la signature numérique et l'utilisation d'un certificat de classe 3, dont le coût annuel est actuellement de 2.400 BEF. Cette formule devrait également utiliser un formulaire intelligent détectant les erreurs de cohérence.

Voici comment les choses devraient se dérouler :

- 1) connexion du PC utilisateur sur le site du Ministère des Finances;
- 2) apparition du sigle de la nouvelle déclaration TVA;
- 3) vérification du certificat;
- 4) encodage manuel <sup>15</sup> des données sur la déclaration à l'écran;

<sup>13</sup> Extraits du discours d'Alain Zenner en clôture du colloque IPCF du 30 octobre 2001.

<sup>14</sup> L'amélioration de la lisibilité des formulaires fiscaux requiert notamment de réduire le contenu de ceux-ci aux seules données réellement indispensables au contrôle administratif et de les adapter, dans toute la mesure du possible, malgré la difficulté du vocabulaire technique, en fonction des destinataires. Des groupes de travail pluridisciplinaires seront institués au sein des administrations en vue de simplifier et d'améliorer la lisibilité des formulaires fiscaux. L'objectif est de faire porter prioritairement l'effort sur les documents qui concernent le plus de monde, à savoir l'avertissement-extrait de rôle (pour lequel une modification fondamentale de la présentation a été formulée le 1er octobre 2001) et les trois principaux avis de l'Administration (avis aux employeurs, avis versements anticipés et avis débiteurs de commissions, honoraires, etc.) dont les présentations sur le site Internet seront rendues "user friendly".

<sup>15</sup> Dans l'état actuel du projet, la déclaration ne pourra pas encore être envoyée au départ direct du logiciel comptable, mais des solutions techniques pourraient voir le jour vers 2003.

- 5) contrôles de cohérence on-line;
- 6) si les contrôles sont OK, la déclaration peut être envoyée et le contribuable reçoit un accusé de réception;
- 7) le contrôle du certificat n'interviendra qu'à chaque ouverture de session, de sorte qu'il sera possible d'envoyer, par exemple, 10 déclarations à la suite l'une de l'autre sans devoir repasser par toute la procédure à chaque envoi.

#### *Déclarations IPP – exercice d'imposition 2002*

Pour l'exercice d'imposition 2002, un formulaire électronique intelligent pourra être téléchargé par le citoyen depuis le site Internet du Ministère. Ce formulaire pourra être complété, imprimé, signé manuellement et renvoyé, sous forme d'une annexe à la déclaration papier officielle, à l'Administration par voie postale ou déposé auprès du service adéquat. Les modifications à apporter aux procédures légales sont par ailleurs à l'examen. Un lien direct avec l'outil de calcul de l'impôt des personnes physiques accessible via Internet sera disponible.

A plus long terme, cette formule pourrait également être couplée à un préremplissage de la déclaration. Envisagé pour les salariés et les pensions, ce préremplissage s'appuiera sur l'ensemble des données en possession de l'Administration, comme celles communiquées par les employeurs.

#### *Déclarations I.Soc – exercice d'imposition 2002*

L'objectif de ce projet est d'offrir aux entreprises un moyen d'introduction de leur déclaration d'impôt des sociétés (I.Soc) accessible via Internet.

Dès l'exercice d'imposition 2002, la déclaration ainsi que les diverses annexes administratives à fournir seront disponibles sous forme de formulaires électroniques intelligents et pourront être téléchargées par l'entreprise depuis le site Internet du Ministère. Ces formulaires seront complétés, imprimés, signés manuellement et renvoyés à l'Administration par voie postale ou déposés auprès du service adéquat.

Les modifications à apporter aux procédures légales sont par ailleurs à l'examen.

#### *Déclarations au précompte professionnel – premier trimestre 2002*

Dès le début du deuxième trimestre 2002, un formulaire électronique intelligent pourra être téléchargé depuis le site Internet du Ministère et complété par l'employeur. Dans un premier temps, ce formulaire sera imprimé, signé manuellement et renvoyé à l'Administration par voie postale ou déposé auprès du service adéquat. A l'instar des déclarations TVA, la déclaration électronique PRP proprement dite sera développée selon deux modalités différentes. Premièrement, les déclarations actuellement envoyées par disquette dans le cadre du projet BETAX pourront être envoyées par voie électronique dans leur format actuel. Deuxièmement, les données issues du for-

mulaire intelligent mentionné ci-dessus pourront être envoyées par voie électronique moyennant l'utilisation d'une signature électronique qualifiée. Ces développements sont prévus dans le courant de l'année 2002. Depuis début septembre, un groupe de travail regroupant des représentants des secrétariats sociaux et des personnes agissant en tant que mandataires au nom des employeurs et des fonctionnaires des administrations fiscales, planche sur la question.

#### **b) Formulaires électroniques – premier et second semestre 2002**

Quelque 500 formulaires papier seront progressivement mis à la disposition des citoyens et des entreprises sous une forme électronique. Dans une seconde phase prévue pour le second semestre 2002, environ 250 formulaires supplémentaires seront concernés par ce projet. Une priorité sera donnée aux formulaires des différentes déclarations fiscales. Dans un premier temps, ces formulaires pourront être complétés à l'écran, mais ils devront être imprimés avant d'être renvoyés par voie postale à l'Administration. Il est toutefois prévu, en tout cas pour certains d'entre eux, de pouvoir ultérieurement les compléter en ligne et de les renvoyer électroniquement.

#### **c) Base de données fiscales sur le site Internet des Finances – premier et second semestre 2002**

L'objectif est de mettre à disposition du grand public une base de données fiscales bilingue, accessible via Internet, reprenant la législation fiscale et les arrêtés d'exécution, la jurisprudence récente, quelle que soit son orientation, les questions parlementaires, le commentaire de l'Administration, les conventions internationales, ainsi que divers autres documents pouvant présenter une valeur informative. Le mémento fiscal déjà disponible sur le site sera conservé. Dotée d'un moteur de recherche performant, une première version de cette base de données fiscales ne reprenant pas la jurisprudence sera disponible sur le site fin janvier, la version complète devant elle voir le jour au début du second trimestre 2002. A ce moment, une version CD-ROM de la base de données fiscales sera également mise à disposition du personnel du Ministère des Finances.

#### **d) Messagerie départementale (e-mail) – début 2002**

L'idée est de doter tous les agents et services du Ministère des Finances d'une adresse e-mail leur permettant de communiquer tant intra qu'extra-muros.

D'ici le début de l'année 2002, la concrétisation du plan informatique quinquennal 2001-2005 devrait se traduire par l'acquisition de plus de 12.000 PC et 10.000 imprimantes. L'infrastructure serveur devrait être disponible en avril 2002 et l'installation des postes clients s'étalera sur l'année 2002. Selon les prévisions, la majorité des adresses e-mail devrait déjà être opérationnelle dès juin 2002.

## L'EXPERT-COMPTABLE, LE CONSEIL FISCAL, LE SECRET PROFESSIONNEL ET LES TIC

Dans le cadre de cet article concernant les nouvelles technologies de l'information, les experts-comptables et les conseils fiscaux, il nous a semblé important de faire le point sur le secret professionnel, d'autant qu'un colloque sur le sujet se déroulait les 8 et 9 novembre à Namur.

Si les professions d'expert-comptable et de conseil fiscal n'ont pas été abordées, la réflexion sur ce thème, principalement dans des professions traditionnellement en pointe en ce domaine (médecins, avocats...), s'est retrouvée vivifiée par des interventions d'une haute qualité scientifique et intellectuelle.

La matière du secret professionnel et la punition de sa divulgation trouve son siège à l'article 458 du code pénal, lequel punit les personnes dépositaires des secrets qu'on leur confie, par état ou dans le cadre de leur profession, et qui, hormis les cas prévus par la loi, auront révélés ces secrets, d'une peine de 8 jours à 6 mois de prison et d'une amende de 100 à 500 francs (soit avec les décimes actuels, maximum cent mille francs).

Au regard d'autres délits sur l'atteinte à la personne et à la réputation, les sanctions pénales semblent peu importantes. Cependant, il apparaît que la sanction de la violation du secret professionnel a trouvé à s'appliquer dans d'autres domaines de punition. Ainsi, la plupart du temps, la violation du secret professionnel est-elle sanctionnée au sein des ordres déontologiques et des juridictions disciplinaires. Des condamnations civiles en dommages et intérêts peuvent venir sanctionner l'atteinte à la confidentialité et la violation du secret professionnel. De plus, des poursuites pénales peuvent être déclarées nulles, si ces poursuites sont entamées sur base de faits révélés à l'occasion d'une violation du secret professionnel.

Nous n'entrons pas ici dans les fondements du principe du secret professionnel (assurer la confiance, protéger les intérêts de la société et des individus...), mais rappelons que l'article 58 de la loi du 22 avril 1999 relative aux professions comptables et fiscales (qui a créé l'Institut des experts-comptables et des conseils fiscaux) dispose clairement que l'article 458 du Code pénal est applicable aux experts-comptables et aux conseils fiscaux externes.

L'objet de cet article n'est pas de faire le tour de la matière, deux journées de colloques n'y ont pas suffi. Cependant, il fallait rappeler certains principes avant d'examiner l'évolution possible ou probable du secret professionnel à l'heure des technologies de l'information et de la communication (les TIC).

Nous allons tenter, dans la suite de ce texte, de synthétiser l'intervention du Doyen de la Faculté de Droit de Namur, Monsieur Yves Poulet, qui avait pour thème : *"Le secret professionnel face au développement des nouvelles technologies"*.

Deux questions furent posées en prémisses à cette intervention :

- Le secret professionnel, constitue-t-il une institution d'une autre époque ?
- Le secret professionnel à l'épreuve des législations TIC ?

Pour y répondre, le Professeur Poulet présente 4 thèses en "concurrence" :

1° Le droit des nouvelles technologies de l'information (ex. : la loi sur la protection de la vie privée) crée, dans le chef du détenteur du secret, une obligation de sécurité (l'article 16 de la loi sur la vie privée prévoit la mise en place de conseillers en sécurité).

2° Au gré des réseaux que la loi parfois elle-même instaure, le secret partagé peut se "diluer" (ex. dossier médical informatisé, flux d'informations administratives...). De la dilution du secret renaît l'intérêt pour la confidentialité d'un certain nombre de données.

3° La loi protégeant la vie privée pourrait sembler être un substitut à la règle du secret professionnel, ces nouveaux textes punissant plus gravement les atteintes à la vie privée que la violation du secret professionnel. Cependant, si la loi sur la vie privée consacre une réappropriation par l'individu de ses données, le secret professionnel vise à protéger non pas une personne, mais une relation du type de celle entre une personne et son (ou ses) confident(s) (médecin, avocat, expert-comptable, ...).

4° Les évolutions des méthodes d'investigation policière et le code d'instruction criminelle, au-delà de la saisie de documents ou disques durs, permettent la perquisition on-line des serveurs auxquels a accès la personne éventuellement mise en cause. Qu'en est-il dès lors du secret professionnel et du droit au silence des dépositaires du secret ?

Dans ses conclusions, le professeur Poulet rappelle quelques principes que les professions détentrices de tels secrets se doivent de défendre et d'appliquer :

- L'obligation pour les détenteurs de secret d'utiliser les technologies de protection, et particulièrement le devoir d'information et de conscientisation des organes déontologiques.
- L'obligation pour les autorités publiques de ménager un équilibre entre confidentialité des données et liberté d'exercice de l'art professionnel d'une part, et intérêt public d'autre part.
- Une synergie entre la protection de la vie privée et le secret professionnel, et non l'affaiblissement du secret par la consécration de la vie privée.
- Le maintien absolu du droit de se taire pour les détenteurs du secret.

A plusieurs reprises au cours de ces journées, la réaffirmation des principes fondateurs du secret professionnel, dans le climat actuel d'après les attentats du 11 septembre, a semblé une nécessité, à une époque où tout dépositaire d'un secret semble être devenu suspect. En effet, le secret professionnel fait partie des principes qui fondent nos démocraties, en permettant à chacun de pouvoir discuter librement et sans crainte avec ses conseillers privilégiés que peuvent être le médecin, l'avocat, le prêtre, l'expert-comptable, le conseil fiscal et d'autres professions qui participent à l'équilibre des relations interpersonnelles au sein de notre société.

**Ph. Wacquier**  
Conseiller Service juridique  
p.wacquier@iec-iab.be

## DISONS-LE TOUT "NET" ...

Nous voici au terme de notre premier voyage dans le monde des nouvelles technologies de l'information et de la communication. Trois conclusions<sup>16</sup> s'imposent. La première se veut une réponse indubitable, la seconde s'apparente à une recommandation et la dernière prend la forme du bilan. Nous y présentons, en effet, schématiquement les actions de l'Institut en la matière et dressons l'état des pistes de réflexion et des projets en cours.

**1. D'abord, la question et sa réponse.** L'avènement des "TIC", une révolution au même titre que l'arrivée de la machine à vapeur, le moteur à combustion ou l'électricité ? Dans son rapport 2001 sur le commerce électronique et le développement,<sup>17</sup> la CNUCED y croit manifestement. Et prédit, sans aucune ambiguïté, que "*La chute spectaculaire du prix de la puissance de calcul et le développement de l'interconnexion ont, ou auront, des effets radicaux sur les activités, tels les services financiers, l'éducation, ... , le conseil, ... et la comptabilité*".

Ce constat, qui vaut son pesant de réflexions, plusieurs raisons nous incitent à le partager.

Même si la route est encore longue vers la connexion universelle et permanente par ondes radio, l'eldorado des communications (SCOOP!) , les "outils" sont là et bien là. L'évolution récente en est le parfait révélateur. Prenons, par exemple, votre téléphone portable. Jusqu'il y a peu, il ne vous servait qu'à échanger des coups de fil, voire l'un ou l'autre message SMS. S'il est récent, c'est désormais un redoutable organisateur de rendez-vous (la plupart du temps, directement connectable sur votre PC via le port infrarouge ou la fonction bluetooth), une redoutable machine d'échange de fax ou de données par Internet, voire un outil de navigation sur le Web, via sa fonction wap. Ce n'est pourtant qu'un début. Dotée de la technologie GPRS, la nouvelle génération de portables - parions qu'ils garniront à coup sûr beaucoup de sapins de Noël - permettent d'écouter de la musique avec un rendu de qualité, réceptionnent les e-mails<sup>18</sup> trois fois plus vite, mais surtout, notamment parce qu'ils offrent désormais une facturation au volume des données échangées, garantissent du temps pour consulter les pages Web et autres sites wap. Le rapport qualité-prix, c'est également l'angle d'attaque idéal pour aborder l'autre "révolution" : l'ordinateur. Qu'il soit portable (dans une moindre mesure, mais la tendance s'inverse), de bureau, voire familial, quasi tous les modèles de PC se retrouvent actuellement dans une spirale de baisse des prix, alors même que leurs performances explo-

sent. A prix égal par rapport à l'an passé, les processeurs ont doublé de fréquence, la mémoire vive a été multipliée par deux, voire par quatre, tout comme la capacité des disques durs. Avec toujours plus de puissance sous le capot, les PC modernes sont des machines fiables, rapides, offrant une réponse satisfaisante à de multiples besoins et demandes. Souvent équipés de lecteur DVD et même de graveur CD, ils se révèlent être d'excellentes chaînes musicales susceptibles de lire en dolby digital d'innombrables morceaux musicaux préalablement téléchargés et d'incomparables machines de traitement des images numériques. Mais surtout, grâce à leur carte modem et leur connexion Internet rapide, revigorée par les récentes chutes des paliers tarifaires, ils vous connectent sur le monde. De plus en plus rapidement et pour de moins en moins cher. En la matière, la Belgique fait la course en tête. S'il fallait des chiffres pour vous en convaincre, les voici, issus d'une étude récente d'Inside consulting publiée dans l'Echo du 28 novembre : "*Un Belge sur trois est un utilisateur régulier (au moins une fois par mois) du réseau à large bande et 9 % de la population adulte (750.000 utilisateurs) possède désormais ce type de connexion (ADSL ou câble). Soit le même pourcentage qu'aux Etats-Unis et 3 % de plus que la moyenne européenne*". Qu'un PC puisse ainsi constituer un excellent outil de travail, c'est une réalité dont vous pouvez apprécier chaque jour le caractère tangible : recherche d'informations, - désormais orchestrée de main de maître par les nouveaux moteurs de recherche -, archivage et communications électroniques sont, en effet, autant d'atouts qui plaident en leur faveur.

**SCOOP!** Des expériences concrètes ont cependant déjà lieu et les résultats sont impressionnants. Armé d'un PC équipé d'une carte wireless, la technologie WI-FI vous permet, en effet, de surfer à volonté sur internet dans un rayon de 50 à 100 mètres autour d'une antenne émettrice de signaux radio qui sert de récepteur.

Mais, nous direz-vous, pour crier que puisse être ainsi leur intérêt, rien ne prouve que les nouvelles technologiques seront nécessairement inductrices de changements ? Confondre technologie et services est une erreur. Une autre, et beaucoup plus importante, serait pourtant de sous-estimer leur impact. Au terme d'une première réflexion, des changements sont prévisibles sur trois axes : les relations cabinet-clients, les contacts cabinet-pouvoirs publics et les formes de collaboration entre confrères et de communication au sein des cabinets. Avec, à la clé, l'émergence d'un nouvel espace de travail et d'échange. Passons les brièvement en revue.

- a) La possibilité d'offrir des produits et des services sur le net induit nécessairement que l'offre devient accessible en dehors de toute considération territoriale et sans délimitation aucune quant à la clientèle potentielle. Si le développement exponentiel d'Internet offre des possibilités nouvelles sur le marché de l'e-business, on s'accorde souvent à dire qu'elles ne sont pas toujours faciles à saisir et que, pour clairement répondre et ciblées qu'elles soient par la Commission

<sup>16</sup> Disponible sur notre site. (<http://www.accountancy.be>), la version électronique de cet article présente une sélection d'articles et d'ouvrages directement téléchargeables.

<sup>17</sup> Voyez note n° 3.

<sup>18</sup> On estime que les 14 milliards d'e-mails qui sont échangés chaque jour vont doubler dans les quatre prochaines années.

européenne,<sup>19</sup> les interrogations que suscite ce développement ne trouvent pas toujours des réponses satisfaisantes. Parmi les questions régulièrement posées par les entrepreneurs du secteur, figurent en bonne place : les modalités d'imposition (qualification des revenus, localisation de la prestation, ...), les modalités de paiement et les règles contractuelles, tant relatives à la validité du contrat lui-même (à partir de quand et où le contrat est-il conclu, quel est le tribunal compétent pour connaître d'un litige et quelle loi s'applique) ... qu'au niveau de la preuve (quelle est la valeur à accorder à une signature électronique ?).

Bien entendu, le choix d'une solution de commerce électronique dépend avant tout de la nature exacte du projet. Si les projets développés par des grandes entreprises opérant, par exemple, dans le secteur de la distribution, prennent, en termes de coûts et d'investissement, des allures imposantes, les PME, de plus en plus incitées<sup>20</sup> à se lancer dans l'e-business, peuvent envisager de se tourner vers des offres de service plus ... abordables. C'est, dans un premier temps, à ce niveau et dans ce genre de situation que se concrétisent d'ores et déjà les premières opportunités. Mais ce n'est pas la seule. Des soutiens logistiques, notamment sous la forme de certification des sites Web ou des documents électroniques (factures, comptabilité...) pourront également être envisagés. Même si cette idée peut paraître audacieuse à certains, cette nouvelle opportunité de service ne saurait être négligée : en Angleterre, les "Chartered Accountants" représentent 30 % des professionnels qui mettent en place, paramètrent, forment et aident les entreprises à s'organiser autour de leurs outils informatiques.

Une autre grave méprise serait de croire que les nouvelles technologies ne véhiculeront des changements que dans les seules entreprises actives sur le marché du e-business. Parions, sans trop de risque, que le vent des nouvelles technologies souffle(ra) sur toutes les entreprises et que la plupart verront leur organisation et leur culture transformée. Dopées par une information qui

circule mieux et plus vite, les relations avec les fournisseurs, partenaires et clients<sup>21</sup>, la politique de communication, le marketing, et même la gestion du personnel, verront leurs cadres d'action et leurs priorités sensiblement modifiées. Dans un marché où les PME seront donc de plus en plus interconnectées, les outils et méthodes de travail vont résolument prendre une orientation on-line. Une perception sans cesse plus affinée permettra le prédiagnostic des pistes à suivre et garantira, en étroite vue d'esprit avec les dirigeants, des réponses rapides et proactives aux questions soulevées. La fourniture en temps réel d'informations<sup>22</sup> est désormais possible, quel que soit l'endroit où vous vous trouvez, la journée, le week-end et même durant la nuit... Mais les changements se glissent également parfois où on les attend le moins. A l'instar de cet autre monument ancien qu'est notre carte d'identité, dont la nouvelle version électronique parviendra à quelque 330.000 citoyens de onze communes pilotes dès mi-2002, notre carte de visite se verra, à plus ou moins court terme, remplacée par un modèle virtuel et multimédia. Moyen durable de nouer des cyber-relations avec la clientèle, mais également prolongement naturel du portail du cabinet, cette carte de visite<sup>23</sup> pourrait être dotée d'un seul numéro que différents services utilisant Internet traduiront en autant d'informations dont l'énoncé, soyons clair, devra être déterminé avec le plus grand soin.

- b) De la politique de communication électronique dont il a fait son credo, le Gouvernement espère d'évidence engranger des dividendes immédiats : un travail matériel réduit et des communications plus conviviales et interactives, notamment générées par la mise à la disposition prochaine de chaque agent des Finances d'une adresse de courrier électronique, l'édition des formulaires intelligents, la base de données fiscales... Avec l'envoi, dans deux ans, des déclarations électroniques IPP, c'est toutefois à un bouleversement fondamental des rôles traditionnels que l'on assistera : "Aujourd'hui - comme Alain Zenner se plaît à le souligner -, c'est le fisc qui contrôle la déclaration et le contribuable qui l'établit. Demain, le fisc établira la déclaration et ce sera le contribuable qui vérifiera, du moins dans 80 % des cas, les cas dans lesquels le fisc connaît les revenus des contribuables". Au-delà du trait d'humour, si l'idée de simplification administrative et du guichet Internet unique qui se profile à l'horizon est plus que séduisante - toutes les administrations y seront reliées, de sorte que les citoyens ne devront plus communiquer qu'une seule fois une information ou une documentation déterminée -, c'est déjà une évidence de dire qu'elle a également ses contraintes et ses points controversés et ses détracteurs. La mise en place de ces téléprocédures nécessitant une identification certaine de l'émetteur et une vérification de l'authenticité des documents, certains s'interrogeront sur ce qu'il advient de données personnelles ainsi transmises... Peu d'informations circulent également sur le mode de règlement des conflits potentiels entre, par exemple, une déclaration transmise électronique-

<sup>19</sup> Directive européenne 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur. [http://www.ispo.cec.be/Ecommerce/legal/documents/2000\\_31ec/2000\\_31ec\\_fr.pdf](http://www.ispo.cec.be/Ecommerce/legal/documents/2000_31ec/2000_31ec_fr.pdf).

<sup>20</sup> Voyez, par exemple, le site <http://europa.eu.int/yourvoice> récemment développé par la Commission européenne en collaboration avec les Euro-info centres.

<sup>21</sup> La combinaison PC-portable qui permet d'établir un contact permanent avec les forces commerciales peut également être couplée avec la technologie de la reconnaissance vocale...

<sup>22</sup> Depuis le 19 novembre 2001, les comptes annuels déposés en 2001 et pendant les trois années précédentes peuvent être consultés et téléchargés sur le site de la BNB. La disponibilité des comptes annuels des entreprises est donc fortement accélérée. Deux types de consultations sont possibles a) un forfait annuel de 500 EUR avec libre consultation, b) un montant de base annuel de 100 EUR et une facturation mensuelle de 2 EUR par consultation (Source : Banque nationale de Belgique.).

<sup>23</sup> Les trois grands logiciels de messagerie que sont Outlook Express, Microsoft Outlook et Netscape Messenger vous permettent déjà de joindre à tous vos mails une carte de visite au format vcf, reprenant vos coordonnées directement intégrables dans le carnet d'adresses de votre correspondant.

ment et un document rectificatif papier expédié ultérieurement. Plus fondamentalement, les téléprocédures posent enfin en filigrane la question des modalités du maintien des professions comptables et fiscales au sein des flux déclaratifs des clients.

- c) C'est un lieu commun de dire que la toile nous rapproche. Et que parmi la gamme des formes de relations confraternelles, l'utilisation des réseaux constituera certainement une note majeure des prochaines années. Mais, bien davantage qu'une simple invitation à la coopération entre confrères, les nouvelles techniques induiront certainement des modifications dans le mode de fonctionnement des cabinets. Partage d'information - le Web est avant tout un extraordinaire espace d'échange d'idées -, recrutement par sites Web ou e-mails, meilleure gestion du temps grâce aux logiciels de gestion de cabinet, augmentation de la productivité et de l'efficacité des collaborateurs par une politique de télétravail bien comprise, réseaux sans fil de type LAN ouvrant aux collaborateurs l'accès aux données et autres facilités de l'entreprise, via les cartes ethernet, où et quand ils le veulent, délocalisation des activités d'encodage et autres tâches manuelles..., voici, pour vous en convaincre, quelques exemples pratiques de cette évolution...\*

**2. S'il convient de toute évidence de ne pas sous-estimer le véritable enjeu de ce défi qui s'offre à notre profession, il faut également en respecter le contexte et les contraintes. Comme il vaut mieux prévenir que guérir, voici deux données que nous vous recommandons de garder à l'esprit. L'une a trait au cadre juridique, l'autre concerne les aspects techniques.**

- a) Chacun, c'est l'évidence, souhaite pouvoir signer un document électronique en toute confiance. Dès lors qu'ils ne peuvent plus être signés à la main, les signatures électroniques s'avèrent indispensables pour authentifier à la fois le signataire et le contenu, alors que d'autres techniques de sécurité (encryptage et Hasch Code) contribuent à assurer la confidentialité des documents lors de leur transmission sur Internet.

\* Dans ce cadre, vous lirez avec intérêt l'article de G. DELVAUX, "Le Commerce sur le net et sa relation avec les cabinets d'experts-comptables", *Revue belge de la comptabilité*, n° 3/2001, pp. 33 à 52.

<sup>24</sup> La Directive européenne sur les signatures électroniques (Directive 1999/93/C du Parlement européen et du Conseil du 13 décembre 1999 relative à la politique communautaire en matière de signatures électroniques) exige que tous les Etats membres de l'Union européenne adaptent, dans leur législation nationale, le principe selon lequel certaines techniques sophistiquées de signature numérique répondent aux exigences légales relatives aux données électroniques.

<sup>25</sup> Proposé par de nombreux acteurs sur le Web, le certificat numérique n'est qu'une composante de l'édifice qui constitue une offre juridiquement acceptable pour les utilisateurs.

<sup>26</sup> Changer les mots de passe des autres utilisateurs, accéder à des lecteurs partagés et en ouvrir sur le réseau, modifier les composantes de son choix, n'est pas une opération compliquée en soi pour tout hacker averti.

Parallèlement, le recours grandissant aux nouvelles technologies en matière de communication électronique, de reproduction et de conservation des documents a contraint les administrations fiscales à intégrer ces nouvelles technologies de traitement. Commune à la plupart des pays européens<sup>24</sup>, la technique utilisée en Belgique repose sur l'utilisation de deux clés, l'une privée et confidentielle et l'autre publique, qu'il vous est loisible de distribuer, le tout dans un schéma de cryptage asymétrique en combinaison avec un certificat X 509V3 qualifié. Des mesures législatives ont également été prises pour accorder aux informations enregistrées, conservées ou reproduites au moyen des nouvelles technologies la même force probante que celle octroyée aux documents papier. Combinés aux deux lois relatives aux signatures électroniques et à leur certification, les documents signés électroniquement engagent légalement leur signataire. Dans ce contexte, bien faire la différence entre une signature électronique sécurisée, qui emporte des conséquences juridiques, et un simple certificat numérique<sup>25</sup>, qui, au mieux, est une présomption d'identification, est plus qu'une nécessité. Il est tout aussi important de rappeler que seule la signature électronique avancée (donc la signature électronique réali-sée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique) est assimilée de manière irréfutable à un acte manuscrit. S'il s'agit, par défaut, d'une signature électronique ordinaire, le juge peut, au terme d'un débat contradictoire, considérer un document signé comme un acte sous seing privé ou comme un écrit ordinaire.

Au-delà de ce problème formel de preuve, ne perdons enfin pas de vue, au risque de scander un refrain à la mode, mais pourtant tellement vrai, que le monde des réseaux est ainsi fait qu'il existe des millions de failles et sans doute encore davantage de manières de les exploiter. Il faut donc raison garder : qui dit connexion permanente, dit également explosion des problèmes de sécurité.<sup>26</sup> Pour palier aux risques, il faut commencer par la mesure la plus évidente : garder absolument confidentielle la clé privée.

- b) Pour profiter pleinement des nouvelles technologies, il faut également s'équiper, en d'autres mots acquérir un modem ADSL et un ordinateur dernier cri. Souvent entendu, ce constat doit être nuancé. Pour deux raisons. Même s'il s'agit des plus répandues et qu'elles font encore l'objet d'offres promotionnelles régulières, le câble et les lignes ADSL ne sont pas les seules solutions d'Internet rapide. Même si le confort et l'efficacité escomptée au final valent certainement la chandelle, le haut débit n'impose absolument pas de posséder un ordinateur de course, le Pentium 2, avec 64 Mo de mémoire constituant toutefois un minimum pour un surf agréable et performant... Des informations à retenir à l'heure où le climat n'incite guère aux dépenses importantes...

**3. Reste alors à dresser le bilan.** L'histoire se nourrissant volontiers de symboles, elle retiendra certainement ceux de l'ère numérique qui se presse à nos portes. Nous n'allons plus travailler de la même façon, ni même penser pareil.

Manquer le virage de la dématérialisation des informations est difficilement envisageable, dès lors que nous sommes en première ligne. C'est la raison pour laquelle nous vous avons proposé -sans vous agonir de schémas complexes et abscons-, au terme d'une présentation technique, une première mise à plat de certains problèmes et des solutions envisageables, avec leurs limites et leurs perspectives. A l'heure où les choses se précipitent - l'accès permanent que les connexions à large bande offriront d'ici peu décupleront les potentialités, mais également les risques -, les utilisateurs potentiels que nous sommes doivent opter pour des solutions garantissant une sécurité optimale.

Pour fondamental qu'il soit, ce n'est pas le seul aspect de la question. Personne ne songerait à nier que la question de la compatibilité des pouvoirs d'investigation du fisc et du respect de la vie privée<sup>27</sup> prend une tournure particulière avec le développement des TIC. Et que l'éthique, valeur essentielle de notre profession, mérite une attention tout aussi particulière. C'est la raison pour laquelle nous prenons une part active dans les travaux des deux groupes "Ethique et fiscalité" et "Fiscalité et vie privée", respectivement dirigés par M. Jean Bastin et le Professeur Pouillet. En notre qualité de membre de la FEE (<http://www.fee.be>), nous participons également aux réunions du groupe de travail "Indirect tax working party", lequel a publié, dans le cadre de la table ronde "VAT Can it survive in the 21st century?" organisée à Bruxelles le 24 avril 2001, une importante réflexion sur l'e-business. Nous prenons également une part active dans les travaux de l'"European Consortium for Web assistance and Trust" tendant à mettre en place une procédure de certification des sites Web électroniques. On ne saurait enfin passer sous silence notre apport significatif dans les projets EDIVAT et INTERVAT, que nous avons décrits en long et en large dans le cadre de cet article, pp. 39 à 43.

<sup>27</sup> Simultanément à l'entrée en vigueur de la loi du 11 décembre 1998 sur la protection des données personnelles, la Commission de protection de la vie privée présente, depuis le 1er septembre 2001, un nouveau site : <http://privacy.fgov.be>. Disponible en français et en néerlandais, il propose un relevé des dispositions légales applicables en matière de vie privée ainsi qu'un moteur de recherche de ses avis. Un modèle de déclaration est également accessible.

A l'évidence, ces participations viendront à point nommé pour nourrir le débat global que l'on ne saurait éviter sur les tenants et aboutissants de l'influence certaine des nouvelles technologiques sur notre mode d'exercice professionnel, de même que sur l'environnement professionnel dans lequel il s'exerce.

Les nouveaux besoins appellent de nouvelles réponses... Au nombre des pistes envisageables, l'idée de mettre en place une sorte de réseau national immatériel des professionnels des chiffres ne saurait être écartée d'office. Partant de même du constat, journalièrement vérifiable, que l'expert-comptable et le conseiller fiscal connaissent leurs clients, la question du rôle certificateur de l'identité, voire, pour autant qu'un certain nombre de conditions soient remplies, du contenu d'un acte émanant de ce même client, mérite certainement que l'on s'y intéresse. Des initiatives de même nature (avocats certifiés et avocats certificateurs) sont à l'étude auprès de l'Ordre français des avocats du Barreau de Bruxelles. Tout aussi intéressant est l'examen des mesures d'ores et déjà bien concrètes prises par les pays voisins en la matière. Parmi celles-ci, les réalisations cadrées dans le projet "Chaînon



<http://www.fee.be>

manquant" (<http://chainon.manquant.net>) en France, ne sont pas les moins innovantes. Jugez-en. Pour 115 euros HT, les membres du réseau "Experts-comptables et commissaires aux comptes de France" reçoivent un lot de 150 cartes multimédias personnalisées à leurs noms et coordonnées professionnelles, un site Web administrable à distance sans connaissance infographique particulière (<http://cabinet.experts-comptables.ws>), un dispositif cryptographique de signature électronique (certificat numérique, lecteur de carte, carte à puce cryptographique, logiciel de signature Sing and Cryptet) et des offres privilégiées exclusives des partenaires du réseau...

Même si la règle "chacun son métier" reste d'actualité, l'avenir semble plus que jamais aux partenariats bien pensés... Rendez-vous dans les prochains numéros...