N° 4641

CHAMBRE DES DEPUTES

Session ordinaire 1999-2000

PROJET DE LOI

relatif au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et le code d'instruction criminelle et transposant certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers et la directive 93/13/CEE concernant les clauses abusives dans les contrats conclus avec les consommateurs

* * *

(Dépôt: le 14.3.2000)

SOMMAIRE:

*

ARRETE GRAND-DUCAL DE DEPOT

Nous JEAN, par la grâce de Dieu, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre de l'Economie et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.– Notre Ministre de l'Economie est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi relatif au commerce électronique.

Palais de Luxembourg, le 7 mars 2000

Le Ministre de l'Economie,
Henri GRETHEN

Pour le Grand-Duc:
Son Lieutenant-Représentant
HENRI
Grand-Duc Héritier

SOMMAIRE

*

INTRODUCTION

Le projet de loi conserve l'esprit et un grand nombre de dispositions du projet de loi No 4554 déposé en avril 1999.

Le projet actuel contribue à doter le Grand-Duché de Luxembourg d'un cadre juridique global sur le commerce électronique.

Cependant, l'évolution des textes communautaires – directive relative à un cadre communautaire pour les signatures électroniques[1], accord politique en vue de la position commune relative à certains aspects du commerce électronique[2], proposition modifiée relative à la protection du consommateur en matière de services financiers négociés à distance[3] – a amené le gouvernement à déposer un nouveau projet de loi. Certes, il aurait été imaginable de déposer une longue liste d'amendements complexes mais cela aurait risqué de dénaturer la structure du projet de base, d'alourdir la compréhension d'un texte très technique.

Le projet de loi 4554 a un champ d'application restreint puisqu'il se limite à Internet, qui, malgré son développement rapide, reste un outil particulier des échanges à distance. Or, la directive „ventes à distance"[4] a un champ d'application plus large et porte sur des moyens de communications aussi divers que le téléphone ou le fax. Par ailleurs, cette directive contient des dispositions étrangères au commerce électronique stricto sensu, celles-ci doivent alors être transposées en droit national par une loi spécifique. Il en est de même pour la protection des données personnelles, en effet les directives[5] en ce domaine, s'appliquent au commerce électronique mais toutes les dispositions relatives au commerce électronique ne s'appliquent pas aux données personnelles[6].

---

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 13/12 du 19 janvier 2000.

2 Accord politique en vue de la position commune du Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, doc. interinstitutionnel N°14263/99, ECO 419 CONSOM 80 CODEC 826.

3 Amended proposal for a directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services and amending Directives 97/7/EC and 98/27/EC, 19 nov.1999, doc. No 2932/99, CONSOM 70, ECOFIN 238, CODEC 684.

4 Directive 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, JOCE L 144 du 4 juin 1997, p. 19.

5 Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, JOCE L 281 du 28 nov.1995, p. 31 et JOCE L 24 du 30 janv.1998, p. 1.

6 On ne peut pas invoquer l'obligation de transparence figurant dans notre projet de loi sur le commerce électronique pour empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet.

Le présent projet de loi, tout en ayant une portée générale, devra s'articuler avec les deux projets de loi spécifiques cités ci-dessus.

*

PARTIE A

EXPOSE DES MOTIFS

La fin du 20e siècle est marquée par l'avènement de la société de l'information. Le commerce électronique est désormais une donnée importante des activités économiques mondiales. En effet, le commerce électronique est un secteur d'avenir qui offre aux citoyens et aux entreprises européennes et luxembourgeoises des perspectives en termes de compétitivité, de croissance et d'emploi. Cependant, afin de garantir aux utilisateurs et aux consommateurs une protection efficace face au développement de ces nouvelles formes d'activité, il est nécessaire de mettre en place un cadre juridique sécurisant.

Chapitre 1 – *De la société de l'information au commerce électronique*

1) Le commerce sur internet

Les nouvelles technologies permettent de stocker et d'utiliser à un coût relativement faible des grandes quantités d'informations et créent ainsi les conditions nécessaires à l'ère de la société de l'information. Parallèlement, grâce aux fibres optiques, les technologies de communication se sont développées, depuis les années 80, au point d'en arriver à une multiplication phénoménale de leurs capacités de transmission.

Cependant, ce n'est qu'avec l'avènement d'un réseau digital global, Internet, qui a su combiner les potentiels des évolutions en matière de traitement de l'information et de techniques de communication, ou encore des autoroutes de l'information, qu'on peut parler d'une véritable révolution digitale.

La vitesse avec laquelle cette „révolution digitale" s'opère n'a pas d'équivalent dans l'histoire des technologies. Ainsi, en seulement quatre ans, 50 millions d'utilisateurs étaient sur Internet, alors que la barre de 50 millions d'utilisateurs a seulement été atteinte après 16 ans pour l'utilisation des microprocesseurs ou encore après 38 ans pour la radio.

Le premier moteur de la révolution technologique est certainement le secteur des techniques d'information et de communication puisque les réseaux électroniques nécessitent de plus en plus d'équipements avec un nombre croissant d'utilisateurs et des équipements de plus en plus performants nécessaires afin de suivre l'évolution technologique. Ces secteurs comptent désormais parmi les principaux moteurs de l'économie européenne. Ils créent des nouveaux emplois, renforcent la compétitivité et portent la croissance économique en Europe, tout en contribuant à maintenir l'inflation à des niveaux historiquement bas grâce au progrès technique[1] et à la libéralisation du secteur des télécommunications.

En effet, grâce au progrès technique le prix des microchips servant à stocker l'information dans les ordinateurs a quasiment été divisé par cent en moins de 7 ans[2]. Parallèlement, la pression concurrentielle entre entreprises, entre réseaux et entre technologies, pression concurrentielle accrue notamment grâce à la libéralisation du secteur des télécommunications, a aussi majoritairement contribué à une baisse des prix, tout en améliorant le choix et la qualité des biens et services[3].

Le secteur des techniques de l'information est également un moteur puissant pour l'emploi en Europe. En effet, on estime que la société de l'information génère un quart des nouveaux emplois nets crées en Europe entre 1995 et 1997 et enregistre des taux de croissance supérieurs à 8% par an pour le secteur des technologies de l'information (TI: comprenant p.ex. les secteurs ordinateurs et logiciels, équipements et services télécoms, équipement bureautique etc., voir graphique 1 ci-dessous).

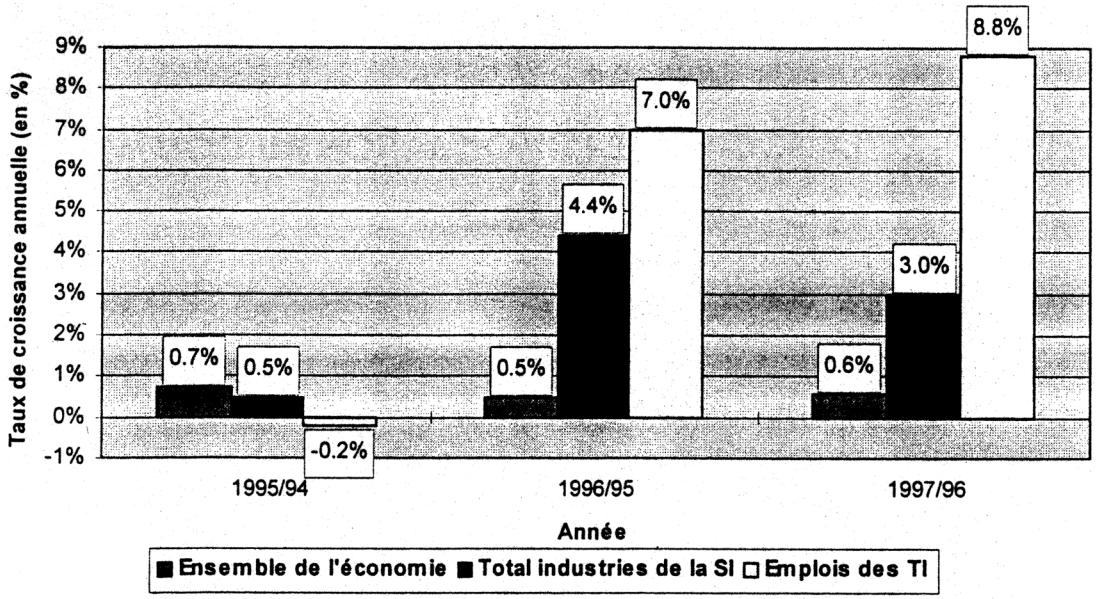
---

1 Les perspectives d'emploi dans la société de l'information: Exploiter le potentiel de la révolution de l'information, rapport de la Commission Européenne au Conseil Européen, 1998, COM(1998)590 final, http://europa.eu.int/comm/dg05/soc-dial/info_soc/jobopps/joboppfr.pdf.

2 Sources: Rapport „The Emerging Digital Economy" du US Department of Commerce, http://www.doc.gov/ecommerce/danc1.htm.

3 Sources: Rapport „The Emerging Digital Economy" du US Department of Commerce, http://www.doc.gov/ecommerce/danc1.htm.

Graphique 1: Croissance nette des nouveaux emplois dans la Société de l'Information



Source : éstimations de la Commission fondées sur des données Eurostat

Ceci porte le nombre total d'employés dans ces secteurs à plus de 4 millions de personnes. En Europe, comme aux Etats-Unis, on constate que les évolutions diverses dans l'emploi total, y compris les pertes d'emploi, des changements vers d'autres emplois et la création de nouveaux emplois se traduisent par une croissance nette de l'emploi[1].

Qui plus est, la demande de travail émanant des entreprises dépasse déjà largement l'offre. Selon des estimations[2], entre 500.000 et 600.000 emplois dans les secteurs reliés aux technologies de l'information (TII) ne peuvent être pourvus manque de candidats qualifiés. Ainsi cette croissance de la demande pour des emplois de spécialistes dans tous les domaines de la société de l'information devrait-elle, avec l'augmentation phénoménale prévue pour les prochaines années des activités commerciales sur Internet, entraîner un déficit croissant de main-d'oeuvre ayant les qualifications requises pour remplir les fonctions nécessaires. C'est d'ailleurs un défi majeur pour le système éducatif européen et national[3].

Cependant, la révolution digitale tirera ses ressources essentiellement à travers le commerce électronique et ses différentes composantes.

2) Le commerce électronique

Le commerce électronique et les potentiels de croissance économique qu'il représente se caractérisent le mieux en citant seulement ces quelques chiffres:

- en 1994 Internet comptait trois millions d'utilisateurs (principalement aux Etats-Unis d'Amérique), ce chiffre s'élevait à plus de 100 millions d'utilisateurs pour début 1998. En 2005 Internet comptera probablement un milliard d'utilisateurs[4]

---

1 Voir aussi OCDE, „Les incidences économiques et sociales du commerce électronique: Résultats préliminaires et programme de recherche – Exposé de synthèse", DSTI/ICCP(98)15/REV2.

2 Kolding M., McGovern S. et Rajah P., IDC „*Information Technology Skills Shortage: The Impending Impact on Business in Europe*", IDC, 1998, rapport spécial de IDC présenté pour le Sommet sur l'Emploi et la Formation dans la Société de l'Information à Bruxelles.

3 Voir aussi „Le marché des nouveaux médias au Luxembourg: état des lieux", une étude de l'observatoire des nouveaux médias du CRP Henri Tudor, où cet aspect est analysé plus en détail.

4 Sources: Rapport „*The Emerging Digital Economy*" du *US Department of Commerce*, **http://www.doc.gov/ecommerce/danintro.htm.** A en croire des prévisions plus optimistes la barre de 1 milliard d'utilisateurs Internet sera déjà passée en l'an 2000.

- entre fin 1998 et fin 1999 le nombre d'utilisateurs de Internet à travers le monde va augmenter de presque 30%, le portant à quasi 150 millions[1]
- on estime que 5000 à 7000 nouveaux noms de domaine sont enregistrés chaque jour sous un domaine générique (comme „com" par exemple)[2]
- selon UUNET, un des plus grands fournisseurs de „backbones", la colonne vertébrale du réseau Internet ou encore le réseau fédérateur, estime que le trafic sur Internet double tous les 100 jours
- en 1999, un ménage sur trois aux Etats-Unis sera on line, un ménage sur deux de ceux-ci achètera on line, c.-à-d. via le réseau Internet[3]
- le commerce entre entreprises réalisé à travers Internet est supposé atteindre un chiffre d'affaires supérieur à 400 milliards de dollars en 2002[4]
- en 1999 le volume du commerce électronique doublera et le chiffre d'affaires se situera autour de 68 milliards de dollars, ce qui équivaut au PIB d'un pays comme l'Irlande, ou encore la Pologne[5]
- l'économie „virtuelle" constituée par les utilisateurs d'Internet et le commerce qui s'y fait croît à un rythme trois fois supérieur à l'économie mondiale[6].

Ces chiffres, tout en donnant un aperçu des énormes capacités de croissance offertes par le réseau Internet, montrent que les Etats-Unis d'Amérique ont toujours un rôle clé sur Internet.

En effet, il convient de rappeler que Internet a été développé aux Etats-Unis, d'abord pour les services de la défense, ensuite pour la recherche universitaire, avant de devenir un réseau universel et commercial. Cependant, concernant cette hégémonie de l'Amérique, une inversion de tendance est prévue pour 1999 où pour la première fois les citoyens américains seront en minorité sur Internet[7].

Selon les estimations de la Commission Européenne[8], le fossé entre le degré de pénétration moyen d'Internet dans l'Union Européenne et celui enregistré aux Etats-Unis d'Amérique est entrain de se combler rapidement, de sorte que le nombre „absolu" d'internautes européens devrait rejoindre celui des internautes américains après 2001 (graphique 2).

---

1 „*IDC predictions '99: The „real" Internet emerges*", de Frank Gens, *International Data Corporation*, IDC, **http://www.idcresearch.com**.

2 Rapport du Conseil d'Etat français „ Internet et les réseaux numériques ", juillet 1998.

3 *International Data Corporation*, IDC, cf. note 8 ci-dessus.

4 „*IDC's Internet Commerce Market Model(®)Predicts Buyers on the Web Will Increase nearly tenfold by 2002*", Carol Glasheen, IDC, **http://www.idcresearch.com.**

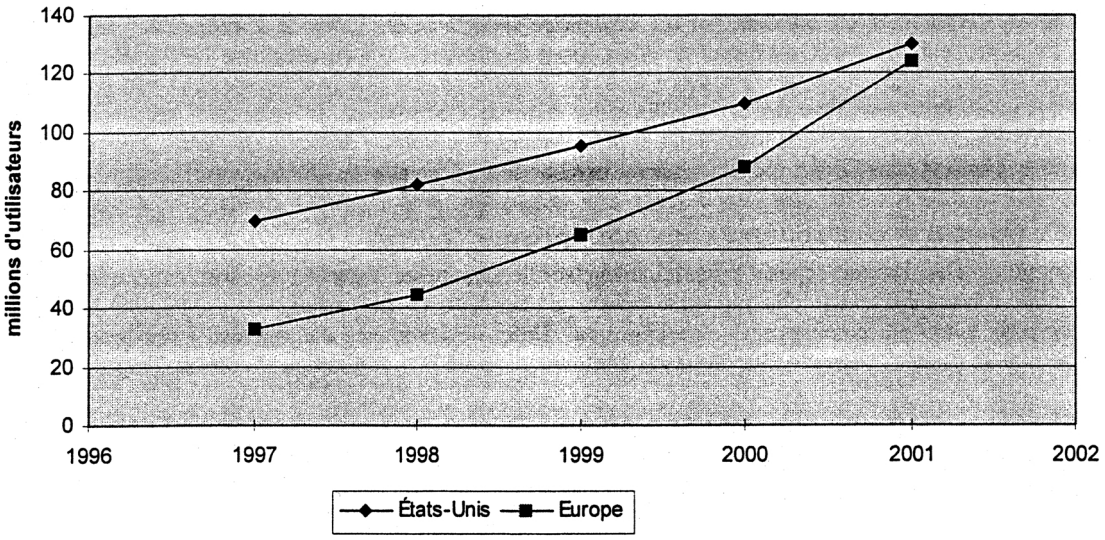
5 *International Data Corporation*, IDC, cf. note 8 ci-dessus.

6 *Sources*: Rapport „*The Emerging Digital Economy*" du *US Department of Commerce*, **http://www.doc.gov/ecommerce/danintro.htm**, NUA Internet Research, **http://www.nua.ie/surveys**, IDC Research, **http://www.idcresearch.com.**

7 *International Data Corporation*, IDC, cf. note 8 ci-dessus.

8 Dans „Les perspectives d'emploi dans la société de l'information: Exploiter le potentiel de la révolution de l'information, rapport de la Commission Européenne au Conseil Européen", 1998, COM(1998)590 final, **http://europa.eu.int/ comm/dg05/soc-dial/info_soc/jobopps/joboppfr.pdf**.

Graphique 2: Augmentation prévue des utilisateurs d'Internet (1997-2001)



Source : éstimations de la Commission basées sur les données fournies par les professionels du secteur

Ainsi, en prenant en compte le fait que Internet soit un phénomène global et que l'Europe semble être en voie de rattraper le retard qu'on y enregistre, on peut raisonnablement transposer la plupart des estimations des Etats-Unis d'Amérique afin de disposer d'une bonne indication sur la situation en Europe, tout en prenant en compte un léger décalage temporel. Cette hypothèse se confirme d'ailleurs par les résultats des récentes analyses à ce sujet:

- En 1998 le commerce électronique en Europe s'élevait seulement à quelque 110 milliards de Francs luxembourgeois (ou encore 2,72 milliards d'euros ou 2,8 milliards de dollars), ce chiffre devrait s'élever à plus de 550 milliards de Francs Luxembourgeois (ou encore 13,6 milliards d'euros presque 16 milliards de dollars) en l'an 2000[1]
- Selon une récente étude de marché, le chiffre d'affaires du commerce électronique en Allemagne avoisinait les 80 millions de dollars en 1998 alors qu'en 2002 ce commerce équivaudra déjà à 1,85 milliard de dollars[2].

Plus précisément la situation au Luxembourg semble pleinement s'inscrire dans les tendances précitées. En effet:

- Au Luxembourg on estime qu'en 1997 seulement 11% des ménages avaient accès à Internet[3] alors que 39% avaient accès à un ordinateur[4]. En comparant le taux d'équipement en micro-ordinateurs du Luxembourg par rapport aux autres pays européens, on constate donc que le Luxembourg se situe en deuxième position après le Danemark et largement au-dessus de la moyenne, créant ainsi une prédisposition favorable à la croissance du commerce électronique au Luxembourg[5].

---

1 Rapport du Conseil d'Etat français „Internet et les réseaux numériques", juillet 1998.

2 Studie: E-Commerce boomt in Deutschland, GNN, Golem Network News, **http://www.gnn.de**.

3 Commission Européenne DG X, EUROBAROMETRE, Rapport Numéro 47, parution octobre 1997, **http://europa.eu.int/en/comm/dg10/infcom/epo/eb.html**.

4 Cependant une étude récente (de septembre 1998), intitulée „Informatique et téléphonie", de l'ILReS, semble confirmer les chiffres enregistrés en 1997 par la DGX pour son eurobaromètre. En effet, dans cette étude on estime que 34% des ménages sont équipés d'un ordinateur et que 11% de la population a accès à Internet tous lieux de connexion confondus. Source: „Le marché des nouveaux médias au Luxembourg: état des lieux", une étude de l'observatoire des nouveaux médias du CRP Henri Tudor.

5 *Source*: „Le marché des nouveaux médias au Luxembourg: état des lieux", une étude de l'observatoire des nouveaux médias du CRP Henri Tudor.

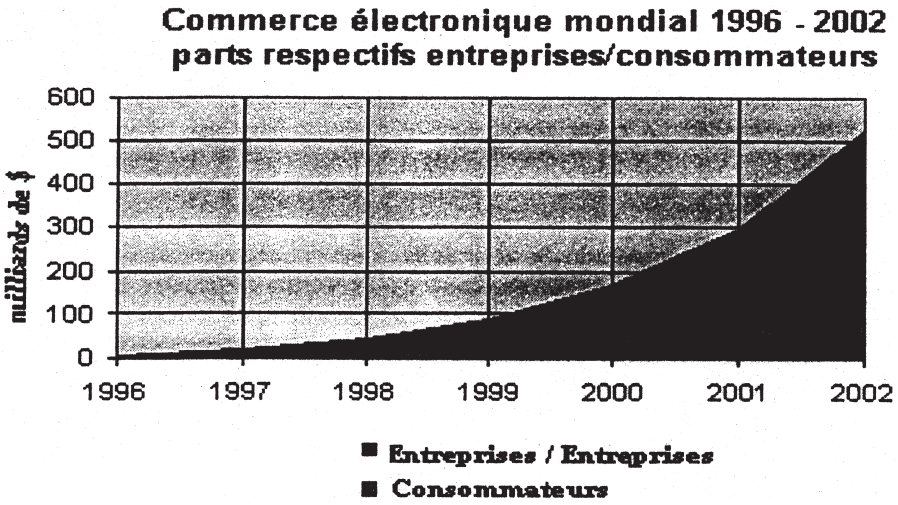
- Cependant comme dans tous les autres pays, il s'agit d'un domaine où on enregistre des croissances très importantes. Ainsi, les principaux fournisseurs Internet ont vu le nombre de souscriptions Internet doubler durant les derniers six mois de 1998, il est prévu que durant les trois premiers mois de 1999 il y aura encore un doublement[1].
- L'année 1998 a aussi été marquée par une croissance importante des noms de domaine „.lu": entre fin 1997 et fin 1998, leur nombre a quasiment doublé passant de presque 1.700 en décembre 1997 à plus de 3.200 fin 1998[2].

Concernant les trois composantes essentielles du commerce électronique, le commerce entre entreprises, le commerce de services et de biens intangibles et le commerce électronique de biens physiques, les situations bien que toutes orientées dans le sens d'une croissance certaine se présentent assez diversement.

2.1) *Le commerce électronique entre entreprises*

Le commerce électronique repose essentiellement sur le commerce entre entreprises, cette composante de l'économie d'Internet étant la plus répandue (tant aux Etats-Unis qu'en Europe), elle compterait en effet pour plus de trois quarts du commerce électronique total. Enfin, le commerce électronique entre entreprises croît également à un rythme beaucoup plus élevé que le commerce avec les consommateurs finaux (graphique 3).

Graphique 3[3]: Commerce Electronique Mondial (1996-2002)



Pour les entreprises le commerce électronique avec leurs partenaires commerciaux comporte de nombreux avantages par rapport aux formes traditionnelles de relations entre entreprises. La production de biens et services appuyée sur Internet peut en effet engendrer des coûts de fournitures moins élevés, des besoins de stockage réduits, des cycles de design et de production moins longs et une nette réduction des coûts frictionnels[4].

Du côté des ventes aux entreprises (voire même aux consommateurs finaux), le commerce électronique permet également une baisse considérable des coûts. Ainsi les coûts de vente et de marketing sont-ils moins élevés pour le commerce sur Internet que pour les formes traditionnelles de commerce. Internet permet aussi d'offrir un service plus efficace et efficient aux consommateurs. Finalement, Inter-

---

1 Enquête Ministère de l'Economie, janvier 1999.

2 *Source* RESTENA, Réseau Téléinformatique de l'Education Nationale et de la Recherche (responsable des noms de domaine du deuxième niveau „.lu").

3 *Source: International Data Corporation,* IDC, **http://www.idcresearch.com.**

4 Le rapport „*The Emerging Digital Economy*" du *US Department of Commerce*, **http://www.doc.gov/ecommerce** fournit une description plus détaillée de ces aspects en fournissant également des chiffres concernant certaines grandes compagnies américaines.

net permet l'ouverture à des marchés inaccessibles (surtout pour des PME) via les formes de commerce traditionnel. En effet, sur Internet le commerce peut se faire à travers le monde entier et à toute heure.

Au Luxembourg, une récente étude[1] réalisée par ILRES à la demande du Ministère de l'Economie montre que 20% des ménages utilisent internet (15% à domicile et 32% au travail ou à l'école). Le nombre des utilisateurs a augmenté rapidement par rapport à décembre 1999 où 14% des ménages avaient indiqué avoir un accès à internet.[2]

2.2) *Le commerce électronique des services et biens intangibles*

A côté du commerce entre entreprises le secteur le plus prometteur en terme de croissance sur Internet est celui des biens et services qui permettent une livraison digitale: essentiellement des services et des biens intangibles qui permettent une livraison via le réseau Internet.

Ainsi les journaux, les banques, les assurances et les compagnies aériennes offrent déjà leurs services online. De même la musique et les livres seront dans un proche avenir accessibles directement sur Internet avec une livraison digitale à la clé.

Presque tous les grands journaux ont aujourd'hui des services online, cette tendance étant appuyée d'une part par une demande des consommateurs et d'autre part par un basculement des sources de revenus de la publicité. Les sites Internet des journaux luxembourgeois comptent d'ailleurs aussi parmi les plus visités au Luxembourg[3].

Cependant, actuellement les services online des journaux ne sont toujours pas bénéficiaires ni pour les grands journaux internationaux ni pour les journaux locaux. Ainsi actuellement la présence sur Internet semble-t-elle plutôt une activité nécessaire mais accessoire pour les éditeurs de journaux, activité qui débouche d'ailleurs parfois sur des nouveaux créneaux commerciaux comme l'offre de portes d'accès pour d'autres firmes, voire la création de sites pour le compte d'autrui[4].

Bon nombre de compagnies aériennes, essentiellement aux Etats-Unis d'Amérique, offrent déjà la possibilité d'acquérir électroniquement des billets d'avion, réduisant ainsi considérablement leurs coûts en évitant de passer par des agents professionnels et augmentant en même temps considérablement leurs taux d'occupation des avions. En effet, grâce à Internet ils peuvent offrir en dernière minute et à un large public des prix spéciaux sur des vols peu remplis et ainsi diminuer leurs coûts fixes. Les possibilités offertes par la vente électronique de tickets tant pour les compagnies aériennes que pour les clients ont d'ailleurs assez rapidement été identifiés en Europe et les procédés de vente en ligne, souvent sous forme de vente aux enchères, abondent aussi de ce côté de l'atlantique. Ainsi, la compagnie luxembourgeoise d'aviation, Luxair, offre depuis fin janvier 1999 des vols dernière minute sur Internet.

Un autre secteur très prometteur pour le développement du commerce sur Internet est certainement celui des banques. On estime, qu'en 1997, plus de 4,5 millions de ménages aux Etats-Unis utilisaient déjà les facilités du „online banking" pour effectuer leurs transactions courantes, ce nombre sera probablement multiplié par quatre avant la fin de l'année 2000[5]. Les transactions bancaires courantes effectuées via Internet apportent pour les banques et leurs clients un gain substantiel de coûts et de temps. Selon une étude américaine le coût du traitement „traditionnel" (au guichet) d'une transaction bancaire courante (comme un chèque ou un virement) coûte environ cent fois plus à la banque que le même type de transaction effectuée par Internet. En effet, le coût d'une opération courante au guichet est estimé par une étude américaine à 1,07 dollar contre un penny pour la même opération effectuée via Internet[6]. De plus, en utilisant Internet, les banques pourront offrir à leurs clients des nouveaux services, voire adopter plus facilement leurs services aux profils individuels de leurs clients.

---

1 Données du 1er semestre 1999.

2 *Source*: „Measuring information society", Eurbaromètre, 16 mars 1999.

3 Dans DELOITTE & TOUCHE CONSULTING Group., CENTRE DE RECHERCHE PUBLIC-CENTRE UNIVERSITAIRE, LABORATOIRE DE DROIT ECONOMIQUE, 1998, „ABBL Mission Electronic Commerce Synthèse des travaux Mai 1998", en référence à une enquête de Luxweb.

4 Voir aussi le rapport sur „Le marché des nouveaux médias au Luxembourg: état des lieux", une étude de l'observatoire des nouveaux médias du CRP HENRI TUDOR. Les auteurs de ce rapport analysent plus précisément le secteur de l'édition de livres et de journaux et les comportements face à Internet des acteurs luxembourgeois dans ce secteur.

5 „*The Emerging Digital Economy*", du *US Department of Commerce*, chapitre 4: la livraison digitale de biens et services, **http://www.doc.gov/ecommerce/danc4.htm**

6 *Source*: „*The Emerging Digital Economy*", du *US Department of Commerce*, chapitre 4, en référence à une étude de Booz-Allen & Hamilton, Inc.: „*Internet Banking: A Survey of Current and Future Development*", février 1996.

Sur les cent banques les plus importantes en Amérique, un quart est déjà classé dans la catégorie banque Internet „pure“, permettant à leurs clients d'effectuer toutes les opérations via Internet. Plusieurs banques au Luxembourg offrent déjà des facilités pour effectuer des transactions bancaires via Internet[1] et malgré le succès assez considérable rencontré par ces offres[2], il semblerait qu'actuellement le nombre peu élevé de ménages connectés à Internet constitue encore un frein inhérent au développement de cette clientèle. Cependant, en confirmation de la forte progression du nombre des raccordements enregistrés par les fournisseurs d'accès à Internet, ce handicap serait en train de diminuer amenant des taux de croissance encore plus considérables pour la clientèle „Internet Banking“ résidente au Luxembourg.

Le secteur des assurances bien que très présent sur Internet avec des informations et des publicités semble prendre un départ plus modéré concernant la conclusion de contrats online, une tendance qui a fortiori est aussi observée en Europe et au Luxembourg. Néanmoins, selon les prévisions faites pour les Etats-Unis d'Amérique on enregistrera des importants taux de croissance concernant le commerce électronique dans ce secteur. Ainsi, on estime qu'en moins de deux ans, en 2001, les compagnies d'assurances concluront des contrats via Internet pour 1,1 milliard de dollars[3]. La croissance du volet assurance online sera, elle aussi, poussée par une demande croissante des consommateurs, combinée avec un gain de coûts pour les compagnies d'assurance et un regain de concurrence sur le marché.

Hormis les services traditionnels offerts en ligne, on imagine que dans un proche avenir bon nombre de biens relevant notamment du domaine de la propriété intellectuelle pourront être commercialisés et livrés via Internet.

En effet, Internet est un réseau idéal pour distribuer à des coûts peu élevés des logiciels, de la musique, des livres[4] ou encore des vidéos digitalement c.-à-d. avec une livraison digitale à la clé. Cependant, les chances de croissance „électronique“ à long terme de ce secteur dépendent essentiellement de l'évolution des techniques permettant de protéger les droits d'auteur et d'endiguer la contrefaçon[5].

A ce stade il convient de parler également de „l'administration électronique“. En effet, l'Etat en tant que client et distributeur de services, est confronté aux mêmes risques mais principalement confronté aux mêmes espoirs de gain que les entreprises privées, la mise en oeuvre des principes de commerce électronique évoluant en symbiose avec l'essor des services publics livrés en ligne[6]. A partir de janvier 1999, les Assurances Sociales allemandes peuvent utiliser des signatures électroniques conformes à la loi allemande sur la signature électronique pour signer certains décomptes internes. Selon des estimations du Ministère du Travail allemand, cette mesure permettrait d'épargner un milliard de DM par an.

2.3) *Le commerce électronique des biens „physiques“*

Finalement, le commerce électronique de biens physiques, commandés en ligne sur le réseau Internet et délivrés ensuite physiquement, affiche aussi des fortes possibilités de croissance. Depuis 1997 les

---

1 BIL et Fortis-Bank. A noter que le service S-Line offert par la BCEE n'est pas réellement du Internet banking mais plutôt du PC banking. En fait, ce type de gestion des affaires bancaires partage dans une large mesure les avantages de la gestion bancaire via Internet, mais quelques différences tant au niveau de l'universalité pour le client qu'au niveau coût par transaction pour l'établissement bancaire subsistent.

2 D'après une enquête du Ministère de l'Economie (janvier 1999), le succès remporté par les offres „Internet Banking“ des banques opérant sur la place luxembourgeoise est tel que le taux de pénétration global (c.-à-d. comprenant et les clients résidents et les clients étrangers) avoisine les taux de pénétration du Internet Banking enregistrés aux Etats-Unis. Cependant, il faut prendre en compte qu'aux Etats-Unis, il s'agit quasi uniquement de clientèle résidente.

3 *Source*: rapport „*The Emerging Digital Economy*“, du *US Department of Commerce*, chapitre 4, **http://www.doc.gov/ecommerce/danc4.htm.**

4 La société XeroX est en train de développer une imprimante qui permettra à partir d'une livraison digitale via Internet d'imprimer un livre sous sa forme traditionnelle.

5 Actuellement, texte consolidé du 30 septembre 1999 de la proposition modifiée de directive du Parlement européen et du Conseil sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Cette directive vise à mettre en place un cadre pour adapter les législations en matière de droit d'auteur dans l'UE à la société de l'information. Un projet de loi qui transpose déjà la majorité des dispositions contenues dans cette proposition de directive a d'ailleurs été déposé au Luxembourg (projet de loi sur les droits d'auteur, les droits voisins et les bases de données, projet N°4431, déposé le 24.4.1998) et va être amendé.

6 Réf.: „Markt- oder Staatsmacht. Streit um digitale Signaturen“, Christiane Schulzki-Haddouti, (c)Verlag Heinz Heise, **http://www.heise.de/ct/99/01/058/**

études de marché américaines montrent que les consommateurs sur Internet se replient sur le commerce en ligne de biens traditionnels (textile, jouets, livres et fleurs), alors qu'auparavant ils achetaient surtout de l'équipement informatique. Pour 1999 on prévoit que plus de 50% des ménages américains qui seront online vont commander via Internet.

Paradoxalement la situation au Luxembourg se présente de façon inverse puisque les sites concernant les produits qui se vendent le mieux sur Internet ailleurs dans le monde, c.-à-d. matériel et logiciels informatiques ainsi que CD de musique, n'y existent pas.

De façon générale le commerce électronique au Grand-Duché est très peu développé ceci s'expliquant essentiellement par des freins techniques quant au paiement électronique via carte bancaire, un manque de prise de conscience des acteurs quant aux potentiels offerts par Internet ainsi que par une certaine immaturité des clients méfiants et préférant le contact local[1]. La seule exception étant probablement le commerce des livres via Internet (voir ci-dessous).

L'exemple le plus parlant du succès que Internet rencontre comme nouveau moyen de distribution est certainement celui de la distribution des livres. En effet, on estime que désormais un tiers de tous les livres vendus aux Etats-Unis sont achetés sur Internet. Amazon, la première librairie virtuelle sur Internet a rencontré un tel succès que les grandes chaînes de librairies traditionnelles (comme Barnes and Noble par exemple) se sont vu forcées de suivre l'exemple de Amazon, s'ils ne voulaient pas risquer de disparaître du marché des livres. Cependant, à l'instar des journaux, les librairies virtuelles n'arrivent pas encore à l'heure actuelle à dégager un bénéfice suffisant leur permettant la survie économique indépendante. Selon les estimations le seuil de rentabilité devrait cependant être atteint dans un ou deux ans.

En Europe les librairies virtuelles enregistrent également un succès grandissant se traduisant par une demande électronique en forte croissance. Ainsi la FNAC et son site comptent-ils parmi les sites les plus visités et le nombre de ventes qui y sont enregistrés a déjà dépassé celui des ventes par minitel et téléphone. Au Luxembourg bon nombre de librairies offrent également une sélection de librairie virtuelle sur Internet (souvent avec une liaison vers leurs partenaires internationaux avec leur catalogue plus extensif), notamment les Messageries du livre qui ont l'avantage de pouvoir faire profiter leurs clients de leur propre service de livraison, garantissant ainsi une livraison rapide et peu coûteuse[2].

Les avantages tant pour les consommateurs (en terme de choix et en terme de disponibilité) que pour les distributeurs (en terme de réduction des stocks et des coûts de loyer) sont particulièrement évidents pour le commerce de biens physiques via Internet: ce commerce multiplie en fait tous les avantages de la vente par correspondance en ajoutant des attraits supplémentaires en terme de disponibilité mondiale et horaire.

Cependant, l'énorme potentiel de croissance réelle que le commerce électronique représente pour le secteur de la distribution aux consommateurs (tant avec livraison digitale qu'avec livraison physique) se caractérise surtout en pensant que les deux tiers des utilisateurs d'Internet en 2002 n'y sont pas encore en 1999. En effet, alors que le pourcentage des ménages qui ont accès à Internet et qui commandent via Internet ne croît que très lentement, c'est essentiellement l'énorme croissance des „abonnés" à Internet qui sera le moteur de la consommation via Internet.

Ainsi, tous ces chiffres donnent une idée de la forte croissance de la „population" Internet ainsi que des capacités de croissance offertes par le développement du commerce électronique mais ils peuvent aussi renseigner sur les besoins qui s'adressent aux autorités publiques en matière de législation.

En effet, le fait que le pourcentage des ménages ayant accès à Internet et utilisant le réseau pour passer des commandes n'augmente que lentement témoigne du fait que bon nombre de consommateurs éprouvent encore des réticences à utiliser le commerce virtuel pour leurs achats, ceci s'expliquant essentiellement par un manque de confiance quant à la sécurité des transactions effectuées via Internet.

Le commerce électronique ne connaîtra son véritable essor auprès des particuliers que si le cadre juridique des transactions électroniques est clarifié et adapté, afin de renforcer la confiance des consommateurs.

---

1 Voir le rapport sur „Le marché des nouveaux médias au Luxembourg: état des lieux" du CRP HENRI TUDOR qui présente une analyse plus approfondie.

2 Le rapport „Le marché des nouveaux médias au Luxembourg: état des lieux", une étude de l'observatoire des nouveaux médias du CRP HENRI TUDOR, présente une analyse plus approfondie de ce secteur.

Chapitre 2 – *Un cadre légal et réglementaire global mais évolutif*

„Internet et les réseaux numériques, c'est avant tout un nouvel espace, un espace international qui transcende les frontières, un espace décentralisé qu'aucun opérateur ni aucun Etat ne maîtrise entièrement, un espace hétérogène où chacun peut agir, s'exprimer et travailler avec une grande liberté."

Cette description du réseau Internet présentée par le Conseil d'Etat (France) dans son rapport de juillet 1998 sur le commerce électronique résume en quelque sorte le fait que la majorité des évolutions sur Internet enregistrées jusqu'à cette date se sont faites en l'absence d'un suivi législatif. Selon certains ceci aurait même favorisé l'essor initial du réseau. Ce rapport a été suivi du document d'orientation élaboré dans le but d'adapter le cadre législatif et réglementaire de la société de l'information afin d'établir une société de l'information pour tous[1].

Cependant, à ce stade de l'évolution du commerce en ligne, on peut aisément imaginer le regain de vigueur que pourrait apporter au commerce électronique une législation axée sur la promotion des possibilités offertes par le commerce électronique, tout en garantissant aux consommateurs et aux professionnels une sécurité juridique égale à celle couvrant les transactions commerciales traditionnelles. Cependant, la notion d'une législation Internet appelle quelques remarques fondamentales:

- Premièrement, Internet n'est pas naturellement un espace du droit, puisque celui-ci, d'application territoriale, s'appuie sur des comportements, des catégories homogènes et stables, tous éléments qui font défaut dans le cas d'Internet. Cet antagonisme avec le droit aurait même, selon certains, favorisé l'essor initial du réseau, libre de toutes contraintes. Cependant, le succès et la généralisation progressive d'Internet, qui comme il ressort des quelques chiffres présentés ci-dessus est désormais une „place de marché mondial" conduit à la nécessité de la fixation des règles de cet espace.
- Deuxièmement, concernant la problématique du droit sur Internet, il convient de rappeler que l'ensemble de la législation existante s'applique aux acteurs opérant sur Internet. Ainsi, il ne s'agit en aucun cas de créer un droit spécifique de l'Internet. En effet, les réseaux sont des espaces dans lesquels tout type d'activité peut être pratiqué et toutes les règles régissant un domaine particulier ont vocation à s'appliquer. Cependant, le législateur doit garantir une égalité de traitement législatif entre commerce électronique et commerce traditionnel et introduire dans la législation les nouveaux concepts nécessaires à l'exécution du commerce par voie électronique.
- Finalement, le caractère transfrontalier des réseaux numériques induit une modification substantielle des modes de régulation habituels des pouvoirs publics, d'une part, compte tenu des limites inhérentes à toute initiative purement nationale, la coopération internationale des Etats est nécessaire pour faire respecter l'intérêt public dans un espace largement dominé par l'initiative privée, d'autre part la réglementation d'origine étatique doit désormais se combiner avec l'autorégulation des acteurs, c'est-à-dire l'intervention de ceux-ci pour décliner les principes de la règle de droit dans des environnements non prévus par celle-ci, et pour agir de façon préventive contre la commission d'infractions. En d'autres termes, Internet et les réseaux introduisent une double interdépendance, entre Etats et entre acteurs publics et privés.

Il est donc important que le projet prenne en compte des résultats des diverses négociations internationales concernant Internet et les réseaux numériques, à savoir:

- Le „Rapport Sacher sur le Commerce Electronique"[2] et les Conclusions de la Conférence Ministérielle de Ottawa[3] de l'Organisation pour la Coopération et le Développement Economique (OCDE), et l'adoption le 10 décembre des lignes directrices pour la protection des consommateurs en matière de commerce électronique[4],
- les travaux de la Commission des Nations Unies pour le Droit Commercial International (CNUDCI) qui a élaboré une loi modèle sur le commerce électronique et s'efforce actuellement à dégager un corps de règles uniformes relatives aux signatures numériques[5],

---

1 Dossier de presse soumis à consultation publique de novembre-décembre 1999, Ministère de l'Economie, des finances et de l'industrie.

2 „Rapport sur le Commerce Electronique" Groupe ad hoc d'experts de haut niveau du secteur privé sous la présidence de John Sacher, contribution indépendante à l'OCDE.

3 *„Conference Conclusions of the OECD Ministerial Conference „A Borderless World: Realising the Potential of Global Electronic Commerce" "*, OECD SG/EC(98)14/REV6, Octobre 1998, OECD, Paris.

4 Voir http://www.oecd.org/news_and_events/release/nw99-121a.htm.

5 *Draft Uniform Rules on electronic signatures*, UNCITRAL, A/CN, 9 WG.IV/WP, 82 du 29/6/99.

- l'Organisation Mondiale du Commerce (OMC),[1]
- l'Organisation Mondiale de la Propriété Intellectuelle (OMPI)[2]. L'OMPI a rédigé le rapport final relatif aux processus de l'OMPI sur les noms de domaine de l'Internet[3], le 30 avril 1999 avec notamment l'adoption très probable d'une procédure administrative de règlements des litiges qui se déroulerait dans une grande mesure en ligne,
- le Conseil de l'Europe[4], qui a mis au point un projet de Lignes Directrices sur la protection des données dans les inforoutes,
- la communication de la Commission européenne „A European initiative in electronic commerce", COM (97) 157,
- les textes communautaires: d'une part, la directive relative à un cadre communautaire pour les signatures électroniques du 13 décembre 1999 et l'accord politique en vue de la position commune relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur, le 7 décembre[5].

Au niveau national, le groupe de travail interministériel présidé par le Ministère de l'Economie a pu bénéficier des conseils et des avis de DELOITTE & TOUCHE, du professeur A. BERENBOOM et de maître E. JOORIS (ULB) ainsi que du rapport du Laboratoire de Droit Economique du CRP Centre Universitaire à Luxembourg, dirigé par le Professeur A. PRUM, de la collaboration précieuse du professeur POULLET (CRID, Namur) et de S. MUNOZ, consultant (docteur en droit). De manière générale, le projet de loi luxembourgeois se propose de prendre en compte tous les résultats atteints par les diverses négociations au niveau international et d'inclure les avancées des projets de directive au niveau européen tout en établissant le cadre juridique nécessaire pour renforcer la confiance des utilisateurs de sorte que le commerce électronique puisse prendre son plein essor.

Chapitre 3 – *Les transactions électroniques*

Le réseau Internet permet aujourd'hui d'acheter et de vendre. Les entreprises commerciales sont de plus en plus nombreuses à s'afficher sur ce réseau et à offrir aux consommateurs leurs produits et services. Le potentiel de ce nouveau moyen de commerce électronique résulte de la possibilité qu'il offre aux parties de négocier et faire des affaires sans jamais se rencontrer physiquement, en dématérialisant complètement leurs échanges, qui peuvent en outre être concrétisés de façon très rapide.

Le réseau Internet est cependant un réseau ouvert, par opposition aux réseaux fermés, à l'instar par exemple du réseau informatique interne d'une entreprise, seulement accessible par son personnel, ou encore le réseau de distributeurs automatiques de billets de banques. La directive relative à un cadre communautaire pour les signatures électroniques définit les réseaux fermés comme des systèmes résultant d'accords volontaires de droit privé entre un nombre défini de participants. A ce titre cette directive ne s'applique qu'aux réseaux ouverts car en réseau fermé il est nécessaire que la liberté des parties leur permette de convenir entre elles des modalités et conditions dans lesquelles elles acceptent les données signées électroniquement[6].

Le problème qui se pose donc aux parties qui opèrent des transactions par l'intermédiaire du réseau Internet consiste d'abord à s'identifier sans erreur. Cette fonction d'identification est en étroite relation avec la nécessité d'authentification des échanges et engagements des parties. Les partenaires peuvent enfin souhaiter assurer la confidentialité de leurs transactions, à raison par exemple du secret des affaires ou du secret bancaire.

---

1 Cf. „Le commerce électronique et le rôle de l'OMC", deuxième publication, dans la série „Dossiers spéciaux" Août 1998, OMC, Genève.

2 Réf „WIPO RFC-3, *Interim Report of the WIPO Internet Domain Name Process*", December 1998, WIPO/OMPI, Genève, cf. **http://wipo2.wipo.int/process/eng/processhome.html**

3 Accessible sur http://wipo2.wipo.int.

4 Projet de Lignes Directrices du Conseil d'Europe sur la protection des données dans les inforoutes, **http://www.coe.fr/dataprotection**

5 Directive 99/93/CE op.cit; sur la position commune sur le commerce électronique, Conseil des ministres du Marché intérieur, op.cit.

6 Considérant 16 de la directive du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

L'identité des parties et l'authenticité de leurs actes en ligne est assurée par leurs signatures électroniques respectives, qui jouent ainsi le même rôle que la signature manuscrite dans les affaires traditionnelles.

Finalement, la reconnaissance de la valeur juridique des outils d'une transaction dans le monde virtuel d'Internet revêt une importance capitale. La signature et le message électroniques doivent, s'ils assurent avec certitude l'identification des signataires et l'authentification du message, pouvoir, au même titre que l'écrit ou la signature manuscrite, constituer la preuve d'une transaction en cas de contestation.

Le concept de signature électronique ne se réfère pas à un mécanisme de signature unique mais à des technologies variées (code secret, techniques basées sur la cryptographie symétrique ou asymétrique, signature biométrique, …) qui méritent l'appellation de signature électronique dans la mesure où elles permettent la réalisation, par voie électronique, des fonctions de la signature classique, à savoir, l'identification du signataire et l'expression de sa volonté d'adhérer au contenu du message signé.[1]

Cependant, parmi toutes ces techniques, la signature numérique ou digitale offre aujourd'hui des garanties de fiabilité et de sécurité inégalées par les autres types de signatures. Pour faciliter la compréhension des dispositions du projet de loi, une description succincte de son mode de fonctionnement est utile.

1) La cryptographie

Dans l'état actuel des techniques, la signature électronique est générée par l'utilisation de la cryptographie (ou chiffrement). De manière générale, la cryptographie recouvre les processus informatiques par lesquels un message intelligible est rendu inintelligible (cryptage), sauf pour les personnes habilitées à disposer des moyens permettant le décodage (décryptage). Ainsi comprise, la cryptographie rejoint son acception courante: rendre un message secret. Mais ce sont les mêmes techniques qui sont utilisées pour la signature électronique.

La cryptographie repose sur des algorithmes mathématiques complexes qui permettent, par diverses opérations de calculs, de coder et décoder des données. L'utilisateur peut faire facilement usage de la cryptographie par l'utilisation de logiciels informatiques qui mettent en œuvre les algorithmes adéquats. Leur fonctionnement repose sur l'attribution à l'utilisateur d'une ou plusieurs clefs de cryptage.

Une solution très simple et bien connue pour rendre un message incompréhensible est de décaler, par exemple de deux positions vers la droite dans l'alphabet, chaque lettre des mots du message. Dans ce système élémentaire, le mot BONJOUR devient DQPLQWT. Le destinataire procédera évidemment à l'inverse pour retrouver le message original. Dans cet exemple, „l'algorithme" de cryptage correspond à „décaler les lettres vers la droite" et la „clef de cryptage" est „de deux positions".

Il existe à l'heure actuelle deux grandes familles de systèmes de cryptographie: la cryptographie symétrique et la cryptographie asymétrique.

1.1) *La cryptographie symétrique*

Dans le cas de la cryptographie symétrique, la clef de cryptage est unique et secrète. Son propriétaire, expéditeur du message codé, doit nécessairement transmettre sa clé secrète à son correspondant, qui l'utilisera pour décoder le message. C'est l'inconvénient principal du mécanisme, car il suppose que la clef (secrète) puisse être transmise de manière sécurisée. Sinon, tout un chacun pourra décrypter le message codé. L'exemple ci-dessus a fait usage d'un système de cryptographie symétrique.

1.2) *La cryptographie asymétrique*

La cryptographie asymétrique met en œuvre deux clefs de chiffrement différentes, qui sont liées l'une à l'autre, la paire étant unique. La première clef est secrète: c'est la clef privée, qui est conservée par son propriétaire. L'autre clef est la clef publique correspondante, qui est diffusée par son proprié-

---

1 Pour tenir compte de ces différentes solutions techniques possibles la définition de la signature électronique dans le présent projet de loi ne se réfère pas à une technologie unique et est ainsi neutre par rapport aux éventuels changements technologiques.

taire pour pouvoir être utilisée par tous. Les algorithmes sont conçus de manière telle que l'on ne peut déduire la clef privée sur base de la clef publique, ni inversement, même en connaissant l'algorithme qui a servi à les créer.

La cryptographie asymétrique est d'usage le plus répandu à l'heure actuelle. De nombreux logiciels sont disponibles en ligne, même gratuitement, qui offrent des niveaux de sécurité importants à leurs utilisateurs. La fiabilité et la sécurité des systèmes de cryptographie asymétrique se mesurent essentiellement à la longueur des clefs. Cette longueur est exprimée en bits, soit des unités informatiques: une clef de 1024 bits est ainsi constituée de 1.024 signes numériques.

Les algorithmes mathématiques qui servent à générer les clefs de cryptographie asymétriques étant bien connus, la fiabilité et la sécurité du système résident donc dans la possibilité de deviner („cracker") les clefs de cryptographie, ce qui est toujours théoriquement possible. En effet, aucune clef n'est réellement inviolable. Mais il reste que, concrètement, l'opération est d'autant plus longue et coûteuse que les clefs de cryptographie sont elles-mêmes plus longues. Or, mathématiquement, la force d'une clef double quand sa longueur augmente d'un bit. Une clef de deux bits est ainsi deux fois plus facile à cracker qu'une clef de 3 bits, quatre fois plus qu'une clef de 4 bits, et ainsi de suite.

Par facilité, les clefs de cryptage sont contenues dans des fichiers informatiques de petite taille auxquels l'utilisateur a accès par un mot de passe qu'il définit, ce qui leur évite de devoir saisir à chaque opération tous les signes composant la clef utilisée.

2) Les fonctions de la cryptographie

La cryptographie peut tout au long des mécanismes de transmissions de messages remplir différentes fonctions, qui seront détaillées ci-dessous.

2.1) *L'authentification*

En premier lieu, la signature électronique utilise le cryptage asymétrique aux fins d'authentification:

Supposons que A veut acheter un bien en ligne à B. A va envoyer un message électronique confirmant sa volonté. Par sécurité, A va crypter son message avec sa clef privée, connue de lui seul. B, qui peut disposer de la clef publique correspondante de A, va décrypter le message que A lui a envoyé. Si, grâce à la clé publique de A, B parvient à décrypter le message, c'est qu'il a bien été crypté avec la clé privée de A, qui est donc l'expéditeur du message adressé à B.

Ce mécanisme ne permet cependant pas en soi de cacher le contenu du message, de s'assurer que le message n'a pas été altéré par un tiers malveillant ou un incident pendant son voyage sur le réseau, ni que la clef privée de l'expéditeur n'a pas été utilisée par un imposteur ou un escroc qui se ferait passer pour un expéditeur respectable.

Ceci pose le problème de la sécurisation du message et de l'identification du signataire:

2.2) *L'intégrité du message*

Elle est préservée par un autre mécanisme informatique, que l'on peut qualifier de „digestion". Le message, avant d'être expédié et crypté, est transformé („digéré") en une valeur de référence, constituée d'un nombre fixe et prédéterminé d'éléments, qui est propre au message (*hash value* en anglais) et expédiée au destinataire avec celui-ci.

Le système est conçu de telle sorte que cette valeur de référence est indépendante de la longueur du message et est unique pour un message donné. Elle résulte de l'application au message d'une fonction mathématique „à sens unique", de telle sorte que le message ne puisse pas être reconstitué sur base de la valeur de référence qui y est attachée.

Le destinataire, après avoir décrypté le message avec la clef publique de l'expéditeur (comme ci-dessus), lui fait subir le même traitement („digestion") que l'expéditeur, en utilisant bien entendu le même algorithme que l'expéditeur.

Si la valeur de référence (*hash value*) ainsi obtenue par le destinataire est la même que celle qui lui a été communiquée par l'expéditeur, c'est que le message n'a pas été altéré. En revanche, si le message a été altéré entre son émission et sa réception, la valeur de référence obtenue par le destinataire sera néces-

sairement différente de celle qui lui a été transmise par l'expéditeur. Le mécanisme (l'algorithme) mis en œuvre assure en effet que la valeur de référence est unique pour chaque message.

Les logiciels de cryptographie répandus procèdent automatiquement à toutes ces opérations et indiquent simplement à l'utilisateur que la signature est correcte pour telle personne (l'expéditeur signataire) et qu'elle a été générée à telle date.

La combinaison de ce mécanisme de sécurisation et du cryptage pour authentification constitue la signature électronique du message[1]. Par message, on peut entendre à la fois la convention juridique entre parties et le payement qui en résulte. En effet, les mécanismes de payements en ligne développés à l'heure actuelle mettent en œuvre les mêmes mécanismes de cryptage, et pour les mêmes motifs.

Voici un exemple, créé en utilisant un logiciel de cryptographie asymétrique gratuit, disponible sur le réseau Internet (intitulé *Pretty Good Privacy* ou *PGP*):

- **Message original**

  Je vous remercie de me livrer une télévision modèle KZ200 au prix de 50.000 francs.

- **Message signé électroniquement**

  ----- *BEGIN PGP SIGNED MESSAGE* -----

  Hash: SHA1

  Je vous remercie de me livrer une télévision modèle KZ200 au prix de 50.000 francs.

  ----- *BEGIN PGP SIGNATURE* -----

  Version: PGP for Personal Privacy 5.0

  Charset: noconv

  iQA/AwUBNXz8+s/YnOS6JTaTEQJ9KwCgq8k8J8Sh4GemKbzgu0E6jwrqON8AoNDvXuxsrhN WDQGX/GRtp46ECh6N=NapZ

  ----- *END PGP SIGNATURE* -----

2.3) *L'identité du correspondant: les prestataires de service de certification*

Il est nécessaire que celle-ci soit établie avec certitude, afin que chaque partie soit certaine de traiter avec la personne avec laquelle elle croit traiter. Ceci concerne à la fois l'identité physique des parties, mais aussi par exemple leur solvabilité, leur localisation, leurs pouvoirs éventuels (quand une personne physique agit pour une personne morale). La vérification de l'identité du signataire est nécessaire en matière de signature électronique, parce que ce type de signature, contrairement à la signature manuscrite, ne contient pas en soi d'éléments qui soient de nature à permettre de la rattacher à telle personne plutôt qu'à une autre.

La signature manuscrite est en effet écrite et l'on admet en général que l'écriture est une caractéristique individuelle des personnes. Cette individualité peut d'ailleurs être aisément vérifiée, en comparant la signature manuscrite apposée par l'intéressé avec celle qui figure par exemple sur un document officiel d'identification.

Composée de chiffres, de lettres ou d'autres signes informatiques, la signature électronique ne présente pas cette caractéristique. Rien ne permet a priori d'attacher une signature à telle personne plutôt qu'à une autre. Plus précisément, rien ne permet d'attacher une clef privée, utilisée pour générer la signature électronique, à telle personne plutôt qu'à une autre. Cela est d'autant plus vrai que les logiciels courants de cryptographie asymétrique permettent à l'utilisateur de générer lui-même sa (ou ses) propre(s) paire(s) de clefs de cryptographie, mais ne procurent toutefois aucune certitude quant à l'identification de l'utilisateur.

Le mécanisme le plus souvent suggéré actuellement pour résoudre ce problème est de faire appel à un tiers à la relation des parties, qui a pour rôle de certifier à celles-ci que telle signature électronique correspond bien à telle personne.

Appliqué aux systèmes de cryptographie asymétrique, le rôle de ce tiers est de pouvoir certifier à quiconque en ferait la demande que telle clé publique est associée à telle personne, et de fournir les

---

1 Source „Etude pour une législation sur la Signature Electronique pour le Grand-Duché de Luxembourg", A. BERENBOOM et E. JOORIS, Bruxelles 1998.

informations requises concernant celle-ci. Le destinataire d'un message utilise en effet la clef publique de l'expéditeur pour vérifier la signature électronique apposée par celui-ci en utilisant sa clef privée correspondante.

Le processus de vérification des signatures électroniques est donc complet si la signature est générée par l'utilisation de la clef privée de l'expéditeur signataire du message (dont par hypothèse celui-ci a le contrôle exclusif), qu'elle est vérifiée par le destinataire du message en utilisant la clef publique correspondante de l'expéditeur et qu'un tiers certifie au destinataire du message que cette clef publique, utilisée pour la vérification, correspond bien à la clef privée détenue par l'expéditeur signataire du message, tel qu'il est identifié par le certificateur (après une vérification préalable de cette identité).

Ces tiers certificateurs sont en général appelés **prestataires de service de certification**. Leur intervention peut être obligatoire ou facultative, comme leurs activités peuvent être réglementées ou non, mais en gardant à l'esprit que les parties doivent avoir confiance dans le prestataire de service de certification auquel elles font appel. Autrement dit, la réglementation éventuelle des prestataires de service de certification devra être conçue pour instaurer cette confiance et cette sécurité requise dans toutes les situations où celles-ci n'existent pas déjà entre les parties.

Dans ces situations en effet, la certification par un prestataire n'est pas utile puisque les parties accordent par hypothèse toute la foi requise à leurs signatures électroniques respectives. Cela sera par exemple le cas si les parties se connaissent préalablement à leurs relations électroniques ou si elles ont préalablement convenu des conditions dans lesquelles leurs signatures seront acceptées et considérées à la fois comme valables et sécurisées. En effet, si les parties sont en relations d'affaires depuis plusieurs années et si elles se communiquent leurs clefs publiques respectives avant de faire leur commerce sur le réseau Internet, alors tant que chacune conserve le contrôle exclusif de sa clef privée correspondante, aucune difficulté ne devrait se présenter.

La certification peut être faite par voie électronique, et est dans ce cas garantie par la signature électronique du prestataire de service de certification, que celui-ci appose sur les certificats qu'il délivre aux utilisateurs qui en font la demande, pour authentifier leurs signatures électroniques. La validité des certificats est à son tour assurée par la signature électronique du prestataire de service de certification, qui peut pour sa part être accrédité par une autorité supérieure de certification, en finale être un service central fourni par l'**autorité nationale d'accréditation et de surveillance**, créée auprès du Ministère de l'Economie.

Il faut en effet garder à l'esprit que le système légal qui sera mis en place pour la signature électronique doit viser à conquérir la confiance des marchés et des consommateurs, en préservant une sécurité maximale dans les transactions commerciales. L'accréditation est une sorte de label de qualité mais n'aura aucun effet juridique. L'accréditation n'est pas nécessaire pour fournir une signature électronique ayant force juridique. En effet, la directive relative à un cadre communautaire pour les signatures électroniques prévoit que l'accréditation est un système *volontaire*. C'est le principe de libre circulation dans le marché intérieur qui prime.

Par ailleurs, la certification ne présentant concrètement d'intérêt que si les parties concernées ne se connaissent et ne se rencontrent pas, les prestataires de service de certification réunissent en général les certificats qu'ils ont délivré dans des bases de données électroniques, qui sont mises en ligne sur le réseau Internet, et qui permettent d'attacher une clef publique donnée aux personnes identifiées dans les certificats. De la sorte, chacun peut vérifier à distance l'identité de ces personnes et l'authenticité des signatures électroniques qu'elles ont générées.

La publicité donnée de cette manière aux clefs publiques de ceux à qui un certificat a été délivré présente en outre un intérêt considérable pour l'utilisation de la cryptographie à des fins de confidentialité (ci-dessous).

Dans le système décrit, les prestataires de service de certification ne doivent donc qu'être dépositaires des clefs publiques permettant de vérifier les signatures électroniques. Les clefs privées correspondantes demeurent la propriété exclusive et sous le contrôle des utilisateurs dont la signature électronique est certifiée.

La directive relative à un cadre communautaire pour les signatures électroniques[1] prévoit l'instauration de prestataires de service de certification devant réunir un certain nombre de conditions minimales, destinées à sécuriser l'ensemble des mécanismes de certification qui en découlent.

---

1 Doc. du Conseil et du Parlement européen du 18 nov.1999, PE-CONS 3625/99 ECO 357 CODEC 643.

En résumé, la signature électronique nécessite donc une réglementation sur deux points[1]:

1. la cryptographie;
2. les prestataires de service de certification.

Cependant, la cryptographie peut également être utilisée pour assurer la confidentialité.

2.4) *La confidentialité*

En effet, admettre l'utilisation, à des fins commerciales, de mécanismes de cryptographie asymétrique pour la signature électronique, les plus répandus étant réputés inviolables, présente un risque: la même technique est en effet aussi utilisée pour assurer la confidentialité des communications en ligne. L'objectif poursuivi par les correspondants peut dans ce cas aussi bien être de protéger leur vie privée ou le secret de leurs affaires que de cacher des opérations illicites aux yeux des autorités.

Le mécanisme est en réalité exactement l'inverse de celui utilisé pour la signature électronique.

B souhaite envoyer un message confidentiel à A. Il va coder son message en utilisant la clé publique de A, diffusée sans entrave et donc connue de lui. Recevant le message, A le décryptera avec sa clé privée et secrète, qu'il est seul à posséder. Ainsi, personne d'autre que lui ne pourra décoder les messages codés avec sa clé publique. De la même manière, A codera un message confidentiel pour B avec la clé publique de celui-ci.

Confidentialité et signature électronique peuvent évidemment être combinées (A veut acheter un bien à B sans que l'on puisse savoir ce qu'il achète, ni que c'est lui qui l'achète). Et ceci sera d'autant plus simple à réaliser que les clefs publiques des destinataires de messages (utilisées par les expéditeurs de ces messages pour les rendre confidentielles) sont regroupées dans des bases de données publiques, auxquelles chacun peut par ailleurs avoir accès pour vérifier l'authenticité des signatures électroniques générées par ailleurs par ces utilisateurs (ci-dessus).

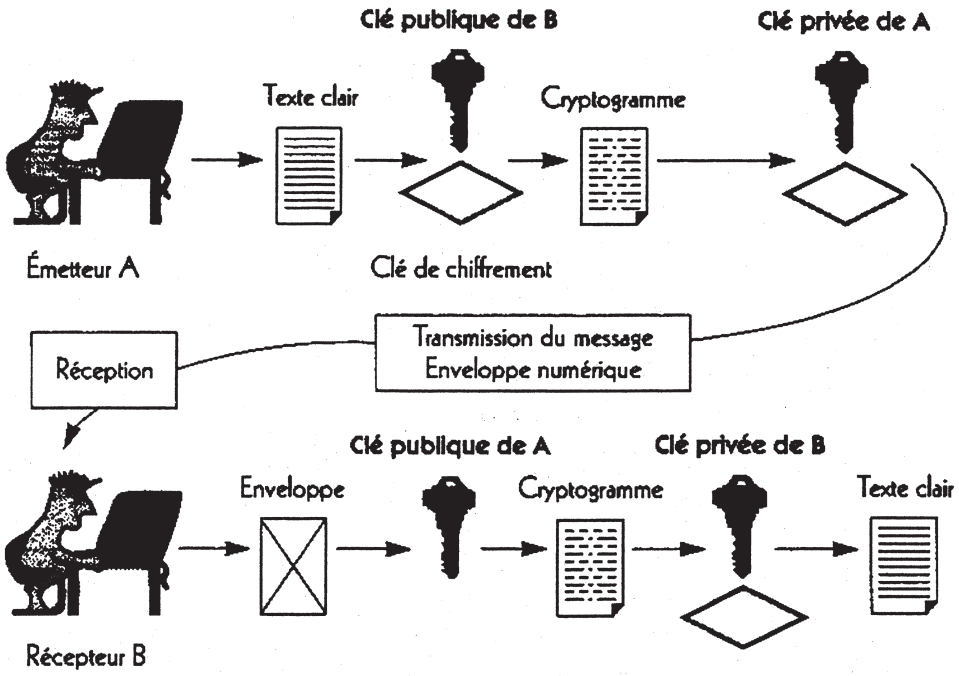
Le bon de commande électronique de A va d'abord être „digéré" (pour donner la hash value qui lui est propre), puis encodé avec la clé privée de A (le message pourra seulement être décodé avec la clé publique de A que B possède, certifiant ainsi que A est bien le signataire expéditeur). L'ensemble sera ensuite crypté avec la clé publique de B, qui sera de la sorte le seul à pouvoir lire le bon de commande de A, en utilisant sa propre clé privée pour décrypter l'ensemble. Il procédera ensuite à la vérification de la signature électronique de A, comme il a été expliqué ci-dessus.

Le graphique 4 ci-dessous retrace ces différentes étapes de l'envoi, de la transmission puis de la réception du message, ensuite quelques exemples utilisant différentes séquences d'encryptage sont présentés.

---

1 La manière dont le projet de loi transpose ces nécessités est présentée d'une manière plus détaillée dans le chapitre présentant les dispositions législatives.

Graphique 4: Transmission message avec clé asymétrique double[1]



Couplage algorithme asymétrique double : la clé publique de B chiffre le message et la clé privée de A authentifie l'émetteur.

Voici un exemple, créé en utilisant le même logiciel que celui employé ci-dessus pour générer un exemple de signature électronique (PGP):

- **Message original**

  Je vous remercie de me livrer une télévision modèle KZ200 au prix de 50.000 francs.

- **Message crypté (le contenu du message est confidentiel)**

  ----- BEGIN PGP MESSAGE -----

  Version: PGP for Personal Privacy 5.0

  MessageID: S+dYCoxU+Qo3lcmZfgJ8wwJKr/yw5/i9

  qANQR1DBwU4DsPQiXuHo2JAQB/9ag7pLWCtrrKXHifxTS4c0TVOyPZn/HhoDdaQ/6NvTi9
  4Xqe383wxS8/sv1HXZRgn9mpxHC+MJwiPsYSGbaCvC6Ay4LtI0QJDIB0JeysySlTdEbw5I
  6ICelLBbEJdlLPJtsZhGKQ4BB3nQOGjohXTbhqZanxsAJy30RvAZL+dmP4rNrX+E9jZOaw
  obujQ6h/csQhTCYR5H26gOaM2eQJ1Er+yMum81uLrhB/urWVlCdlT+DG1LtuNf937MoFPg
  AmSxCJ4zOJ59iTCqba4oozGR82HA0TwNjKuQQRtZKpteNEfc0ZLJWEkeXbhSVhajDZMR2
  Q5jeY08iqam+RDvPUcB/4ogi1ayNy+mIV0k5AUNMd/zYea23VsvYbIUogJWempSe4z+aYd
  x//YJ44Y9tqNQPrOZj/kJxsKq1E+b7bUWMjfCXixuobvntOmifslCHjiX4XwIyH40xDEWn
  4S5QzZPRXglgrrEp71myraCXhGEdzodWGOohofB6yIjutdo90HH8NL/AsKuGzTF90c2uEP
  CcvtC/8qsfXa47/wt0oQJInbJKUpvH3CV+9c1O7lc4TUaugs5s0WucjRKK1j5FMIli5zcq
  Nc0rM/N4bjkFu/DaXplTWx3z417Blj5y0jdLarawpH71WuSYKwkXp1nlH+EX0MX9SoQDJR
  SRXVf6iRBJyTyW4jl2vtba0RIfEWzCvaVUqfVoctz7bwlpKpH/8wEFi4AJldtWhE3tnV/C
  /VoVB64NOymrm648T1Htsd9xu4fkifn7stWDwZUlG58/WkanHxPizon/joRitrso1LjTOm
  JWUw5RK1gb/iCXVCt4vk0A===o/CB

  ----- END PGP MESSAGE -----

---

1 *Source*: FARAGGI B., 1998, „Commerce électronique et moyens de paiement“, Dunod, Paris.

- **Message crypté puis signé (le contenu du message n'est pas accessible, mais l'identité du signataire peut être vérifiée).**

  ----- BEGIN PGP SIGNED MESSAGE -----

  Hash: SHA1

  - ----- BEGIN PGP MESSAGE -----

  Version: PGP for Personal Privacy 5.0

  MessageID: S+dYCoxU+Qo3lcmZfgJ8wwJKr/yw5/i9

  qANQR1DBwU4DsPQiXuHo2JAQB/9ag7pLWCtrrKXHifxTS4c0TVOyPZn/HhoDdaQ/6NvTi9
  Xqe383wxS8/sv1HXZRgn9mpxHC+MJwiPsYSGbaCvC6Ay4LtI0QJDIB0JeysySlTdEbw5I6
  CelLBbEJdlLPJtsZhGKQ4BB3nQOGjohXTbhqZanxsAJy30RvAZL+dmP4rNrX+E9jZOawob
  jQ6h/csQhTCYR5H26gOaM2eQJ1Er+yMum81uLrhB/urWVlCdlT+DG1LtuNf937MoFPgAmS
  CJ4zOJ59iTCqba4oozGR82HA0TwNjfKuQQRtZKpteNEfc0ZLJWEkeXbhSVhajDZMR2Q5je
  08iqam+RDvPUcB/4ogi1ayNy+mIV0k5AUNMd/zYea23VsvYbIUogJWempSe4z+aYdx//YJ
  4Y9tqNQPrOZj/kJxsKq1E+b7bUWMjfCXixuobvntOmifslCHjiX4XwIyH40xDEWn4S5QzZ
  RXglgrrEp71myraCXhGEdzodWGOohofB6yIjutdo90HH8NL/AsKuGzTF90c2uEPCcvtC/8
  sfXa47/wt0oQJInbJKUpvH3CV+9c1O7lc4TUaugs5s0WucjRKK1j5FMIli5zcqNc0rM/N4
  jkFu/DaXplTWx3z417Blj5y0jdLarawpH71WuSYKwkXp1nlH+EX0MX9SoQDJRSRXVf6iRB
  yTyW4jl2vtba0RIfEWzCvaVUqfVoctz7bwlpKpH/8wEFi4AJldtWhE3tnV/C/VoVB64NOy
  rm648T1Htsd9xu4fkifn7stWDwZUlG58/WkanHxPizon/joRitrso1LjTOmJWUw5RK1gb/
  CXVCt4vk0A===o/CB

  - ----- END PGP MESSAGE -----

  ----- BEGIN PGP SIGNATURE -----

  Version: PGP for Personal Privacy 5.0

  Charset: noconv

  iQA/AwUBNX0iOs/YnOS6JTaTEQJfgQCfcCzfpJIrs5Uq6Qu6WmtZIge1nrwAmwcfBW504w
  TT/B/jz6nG/wi07T41=Ct3y

  ----- END PGP SIGNATURE -----

- **Message signé puis crypté (tant le contenu du message que l'identité du signataire sont cachés)**

  ----- BEGIN PGP MESSAGE -----

  Version: PGP for Personal Privacy 5.0

  MessageID: xeNWCNPtXdhfoZkWiZl6ruceIRYcg//h

  qANQR1DBwU4DsPQiXuHo2JAQB/91+gxisMVZnkd/AvQZM3INu7BEwnaFkQoxD0XmWEzjQb
  uFhi77CeQDo9ZrUsw+IVwIYuXYHNTkp94eYX9c6NMRPQzA7eWJDlTIJ/OzBLXbS4g9Nhzz
  VhsP2GrQU6Udakk9tfqh0zDIgAT6uxP+HsrMeu4WcdFMSxVfqSc3Zp34bW9eXvDm+imu81
  WbEhKs12uoAzizjIZXHiHPRsPcUM7xaMQIEFNzo8wkjgHNpg3dOyQFK3yfpfsZVUnrRc14
  9boLlkuyOIWxBLgGWpLIh3J8wCCPPumXM4TGyJJoIDh3mcVL6A3EiP8Sev3yYflLuqdw6F
  c5srGf/QeoaiDuaHGsCADb/UWtrARWpERcts2U7Vp2F58qhTYwSodOZ0qaSg1miwr15YOP
  PHdwWrfXt7Mk5lqeVZxPudn3hb2G+8xqedOAgkIm/Fa4RoRdAD17BsMhPifuEJvGcTLPOG
  pdFpipjRB9CDck9gUvYqYUCqdPsA+FchJE0UzXv19XdcDFcxFBnwoMdtax8n3JLrihdQfp
  a10y4DVkWGZQizqd2yJdjPJFTbndiLR+i9N6EGzUuvCx6Ek/iUrekH9Q/kFQj5KNOl1/tv
  QJ/Tg0oZWWVjCTQLUdxec6iZ1MR8DD/0rD/GfcJCrDWVxpIpoUPfDUAC5XndPsmWAdRUG6
  S+CPk03eO1bbybqMY1BPUnb2hxP7yYX4uA0I4LfVN6XE9Tqj07lLa8bx7Im1xDLQuhwZvC
  ajSbtONBH9+P41TT8i2QXCxYyhuKfR5if0M08Vnm0Ztusw+blbfLqrWS6LFCUrIFZtjUw8
  NUp4QzcMpMq9Zh6a8cImfckTQ4+u1MyqaBGVjqNntxlpFft44nsfEBseBW1TxCqbe+Q1hX
  gkSggHgZehmYflfd5FQzwQaXYo/tLJObHmlkAJ3ZclEIyPPQtR/wE==/mlB

  ----- END PGP MESSAGE -----

On voit donc que signature électronique et cryptage peuvent intervenir indifféremment l'une avant l'autre, suivant l'ordre choisi par l'utilisateur.

Admettre les signatures électroniques suppose admettre la licéité des systèmes de cryptographie asymétrique forte, dont l'utilisation doit être libre pour permettre aux utilisateurs de préserver la confidentialité de leurs échanges et communications électroniques. Pour autant, le système légal mis en place ne doit pas favoriser l'utilisation de la cryptographie à des fins illicites, en prévoyant la possibilité pour les autorités judiciaires d'accéder à des données décryptées qui présenteraient un caractère illicite. Cet accès doit être limité à des cas exceptionnels.

Et s'il faut interdire et réprimer l'usage illicite de la cryptographie, cela ne doit pas se faire au détriment de la promotion du commerce électronique, qui suppose une libéralisation la plus large possible de l'utilisation de la cryptographie asymétrique forte. Le projet de loi a donc par conséquent cherché la voie du compromis en libéralisant les instruments de la cryptographie tout en mettant à la disposition des autorités d'investigation judiciaire un dispositif adapté aux besoins de leurs enquêtes.

Rappelons que la cryptographie est libéralisée dans la quasi-totalité des pays, seule la France prévoyait un régime strict qu'elle est en passe d'abandonner[1].

La réglementation de la signature électronique est nécessaire, afin de faciliter et promouvoir le développement du commerce en ligne. Le système mis en place devra gagner la confiance des utilisateurs, tant en ce qui concerne la conclusion de leurs affaires que les moyens de payement électronique mis à leur disposition pour les exécuter. Cette confiance, comme aux premières heures de la monnaie scripturale ou des cartes de crédit, est encore insuffisante.

Il doit également permettre à ses utilisateurs de conclure et exécuter des transactions commerciales dans des conditions telles que l'acte juridique et son exécution puissent recevoir les mêmes effets qu'une convention traditionnelle. La reconnaissance de la valeur juridique des outils d'une transaction dans le monde virtuel d'Internet revêt donc également une importance capitale. En effet, si la signature et le message électroniques doivent d'abord assurer avec certitude l'identification des signataires et l'authentification du message, ils doivent en outre pouvoir, au même titre que l'écrit ou la signature manuscrite, constituer la preuve d'une transaction en cas de contestation.

Chapitre 4 – *Protéger le consommateur*

La protection des données personnelles sera traitée en détail dans un projet de loi annexe transposant les directives (voir supra introduction).

Dans le présent projet de loi, qui se limite au commerce électronique – et dont le champ d'application est donc nécessairement plus restreint que celui des directives précitées, la protection des données personnelles vise surtout les signataires. En effet, le prestataire de service de certification a l'obligation de respecter les textes sur la protection des données personnelles à l'égard du signataire.

Notons toutefois que la directive relative à un cadre communautaire pour les signatures électroniques contient des dispositions permettant de signer avec un pseudonyme afin de garder l'anonymat, et que notre projet contient bien évidemment une telle disposition (mais l'on ne peut intégrer un article général sur l'anonymat qui serait beaucoup trop large).

Hormis la seule protection des données personnelles et de la vie privée des utilisateurs d'Internet, tout projet de loi devra en outre viser à favoriser les échanges par une confiance accrue des acteurs sur Internet: une priorité étant d'assurer un cadre juridique sécurisant pour les consommateurs, afin d'offrir un niveau de protection comparable à celui des ventes traditionnelles ou encore des ventes à distance „classiques“ en Europe.

Comme pour la protection des données, l'ensemble du dispositif actuel de protection du consommateur, réglé d'ailleurs largement au niveau Union Européenne, est applicable à l'Internet. Cependant, il s'agira de garantir plus précisément trois principes fondamentaux:

- la transparence: concernant notamment l'affichage des prix et des qualités des produits offerts sur Internet,
- la possibilité de modification: concernant notamment la possibilité de changer à tout moment au cours d'une opération d'achat virtuelle la composition du panier des biens retenus avant la conclusion du contrat,

---

1 Voir déclaration d'Hourtin du Premier Ministre de janvier 1999 et plus généralement le site du gouvernement français, http://www.internet.gouv.fr.

• la garantie d'un délai de rétractation: concernant notamment la non-irréversibilité des choix des achats des consommateurs (garantie pour le consommateur de changer d'avis dans un certain délai).

Cependant, comme les transactions sur Internet s'effectueront pour une grande partie avec des commerçants non européens, la nécessité de négocier des conventions internationales relatives aux transactions électroniques s'impose. Un premier pas majeur dans cette direction a d'ailleurs été franchi avec les conclusions de la conférence ministérielle de l'OCDE à Ottawa[1] concernant non seulement les consommateurs mais également le traitement de la fiscalité. Et l'adoption le 10 décembre 1999 par l'OCDE des lignes directives sur la protection des consommateurs dans le cadre du commerce électronique.

Le projet de loi sur le commerce électronique inclut non seulement le dispositif des lois existantes mais transpose en même temps quelques dispositions pertinentes de la directive ventes à distance (non encore transposée en droit national et qui le sera dans le second volet de notre projet de loi relatif à la protection des consommateurs) et certaines dispositions de la proposition modifiée de directive relative à la vente à distance de services financiers qui rencontrent un accord.

La législation luxembourgeoise relative aux clauses abusives dans les contrats conclus avec les consommateurs et la future législation relative à la protection des consommateurs dans les ventes à distance constituent un acquis majeur pour la protection du consommateur et continuent donc à s'appliquer intégralement aux services de la société de l'information.

Le chapitre suivant présente de manière plus détaillée les différentes dispositions introduites dans le projet de loi luxembourgeois notamment en matière de protection du consommateur.

Chapitre 5 – *Les principales dispositions du projet de loi sur le commerce electronique*

1) Définitions et champ d'application

Le projet de loi contient de nouvelles définitions permettant de couvrir les innovations technologiques présentes et à venir et une clarification quant au champ d'application et à la loi applicable.

1.1) *Définitions*

Des définitions cruciales figurent dans le projet de loi:

– Les services de la société de l'information

– Le prestataire établi

– le destinataire du service.

La notion de service de la société de l'information est déjà définie dans le droit communautaire en vigueur, dans la directive 98/34/CE du Parlement européen et du Conseil[2]. La définition considérée englobe tout service presté normalement contre rémunération, à distance, par l'intermédiaire de réseaux, au moyen d'équipements électroniques de traitement[3] et de stockage de données et à la demande individuelle d'un destinataire de services[4].

Les services de la société de l'information englobent un large éventail d'activités économiques qui ont lieu en ligne. Ces activités peuvent consister à vendre des biens en ligne. Les activités telles que la livraison de biens en tant que telle ou la fourniture de services hors ligne ne sont pas couvertes.

Les services de la société de l'information ne se limitent pas exclusivement aux services donnant lieu à la conclusion de contrats en ligne mais dans la mesure où ils représentent une activité économique, ils

---

1 OCDE, „Déclaration des ministres sur la protection des consommateurs dans le contexte du commerce électronique", DSTI/CP(98)12/FINAL

2 Du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques , JO L 204, 21 juillet 1998, p. 37. La directive 98/84/CE du Parlement et du Conseil du 29 nov.1998, concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel, JO L320, 28 nov.1998, p. 54, s'est déjà référée à la définition fournie par la directive 98/34.

3 Y compris la compression numérique.

4 Que les services mentionnés dans la **liste indicative** de l'annexe V de la directive 98/34/CE, amendée par la directive 98/48/CE (JO L 217 5 août 1998, p. 18), **qui n'impliquent pas le traitement et le stockage de données ne relèvent pas de la définition des services de la société de l'information**.

s'étendent à des services qui ne sont pas rémunérés par ceux qui les reçoivent, tels que les services qui fournissent des informations en ligne ou des communications commerciales, ou ceux qui fournissent des outils permettant la recherche, l'accès et la récupération des données.

Les services de la société de l'information comportent également des services qui consistent à transmettre des informations par le biais d'un réseau de communication, à fournir un accès à un réseau de communication ou à héberger des informations fournies par un destinataire des services.

Les services de télévision au sens de la directive 89/552 et de radiodiffusion ne sont pas des services de la société de l'information car ils ne sont pas fournis à la demande individuelle d'un destinataire de services. En revanche, les services transmis de point à point, tels que les services vidéo sur demande ou de fourniture de communications commerciales par courrier électronique constituent des services de la société de l'information.

Par contre, l'utilisation du courrier électronique ou d'autres moyens de communication individuels équivalents par des personnes physiques agissant à des fins qui n'entrent pas dans le cadre de leurs activités commerciales ou professionnelles, y compris leur utilisation pour la conclusion de contrats entre ces personnes n'est pas un service de la société de l'information. En effet, cela serait soumettre les personnes physiques agissant à titre personnel et les prestataires à des obligations trop lourdes et inutiles.

Les employés ne voient pas leur protection remise en cause par la législation relative au commerce électronique en effet, **la relation contractuelle entre un employé et son employeur n'est pas un service de la société de l'information**.

De même, les activités qui par leur nature, ne peuvent être exercées à distance et par des moyens électroniques, comme la vérification légale des comptes de société ou les conseils médicaux exigeant un examen physique du patient, ne sont pas des services de la société de l'information.

Les acteurs du commerce électronique sont principalement au nombre de trois: le prestataire établi, le destinataire de service et le consommateur. Le projet de loi définit les deux premières notions, la troisième sera définie dans l'autre volet législatif concernant la protection du consommateur.

Au préalable, quelques mots concernant **la définition du prestataire**: toute personne fournissant un service de la société de l'information est un prestataire. Il peut s'agir d'une personne physique ou morale et s'il s'agit d'une personne morale, il peut s'agir de n'importe quelle forme de société.

Afin d'assurer efficacement la libre circulation des services au Luxembourg et dans la Communauté européenne, et la sécurité juridique pour les prestataires et leurs destinataires, les services de la société de l'information doivent être **uniquement soumis au régime juridique de l'Etat membre dans lequel le prestataire est établi**. Aussi le projet de loi définit-il le prestataire établi en se référant à l'article 2 c) de la future position commune[1] en vue de l'adoption de la directive du Parlement européen et du Conseil sur le commerce électronique.

Le lieu d'établissement d'un prestataire devrait être déterminé conformément à la jurisprudence de la Cour de Justice européenne, selon laquelle le concept d'établissement implique l'exercice effectif d'une activité économique au moyen d'une installation stable et pour une durée indéterminée. Cette exigence est également remplie lorsqu'une société est constituée pour une période donnée.

Le lieu d'établissement d'une société fournissant des services par le biais d'un site internet n'est pas le lieu où se situe l'installation technologique servant de support au site ni le lieu où son site est accessible mais **le lieu où elle exerce son activité économique**.

Quant à la **définition du destinataire d'un service**, elle couvre tous les types d'utilisation des services de la société de l'information, tant par des personnes qui fournissent l'information sur les réseaux ouverts tels que l'Internet, que par celles qui recherchent des informations sur Internet pour des raisons privées ou professionnelles.

1.2) *Champ d'application*

Le projet de loi s'applique aux prestataires de services de la société de l'information établis au Luxembourg et aux services qu'ils prestent.

---

1 Accord politique en vue d'une position commune du 7 décembre 1999.

L'objectif de l'article 2 du projet de loi est de garantir que les services de la société de l'information fournis par un prestataire de services établi au Luxembourg, ne soient soumis qu'aux prescriptions légales du Luxembourg (principe du pays d'origine) notamment lorsqu'ils sont prestés dans d'autres pays de la Communauté européenne.

Cela signifie que l'Etat luxembourgeois doit appliquer sa propre réglementation et le pays de destination (autre Etat membre) du service de la société de l'information ne peut pas imposer des restrictions issues de sa législation (car cela aboutirait à mettre les prestataires devant l'obligation de respecter 15 législations).

Le principe du contrôle du pays d'origine est une **véritable avancée, également du point de vue de la protection du consommateur**, puisque le Luxembourg (et les autres pays membres) pourra et devra contrôler que les services des prestataires établis au Luxembourg respectent la législation luxembourgeoise y compris pour ce qui est des services exportés (ce qui n'est pas le cas actuellement puisque par exemple, si un Etat membre interdit la publicité pour l'alcool il peut faire de la publicité en dehors de son territoire).

L'article 2 du projet est directement inspiré de l'article 3 de l'accord politique en vue de la position commune sur certains aspects juridiques du commerce électronique qui pose le principe du pays d'origine et celui de la reconnaissance mutuelle, qui est aussi présent dans d'autres textes communautaires tels que la directive sur un cadre communautaire pour les signatures électroniques[1], la directive relative à la Télévision sans Frontières.

Cet article 2 limitera la capacité d'appliquer des dispositions plus rigoureuses aux services de la société de l'information fournis au départ par d'autres Etats membres où le degré de protection est supposé moins élevé.

Cependant le texte de loi n'a pas pour objet d'établir des règles additionnelles de droit international privé relatives aux conflits de loi ni d'aborder les règles de compétence des tribunaux. Précisons toutefois, que les règles de droit international privé ne doivent pas restreindre la liberté de fournir des services de la société de l'information.

Le droit international privé vise à déterminer quelle loi nationale est applicable et quel tribunal est compétent et il couvre non seulement les lois applicables au droit contractuel mais aussi celles applicables au droit précontractuel et délictuel. Ces règles sont issues aussi bien de conventions internationales que des lois nationales.

Le droit international privé est d'application pour ce qui est des obligations contractuelles dans les contrats conclus avec les consommateurs[2] dans le projet de loi (art. 61 § 2 dans le titre V consacré aux contrats conclus par voie électronique) puisque ces obligations sont exclues du principe du contrôle du pays d'origine.

En tout état de cause, **les parties sont toujours libres de choisir la loi applicable à leur contrat ainsi que le tribunal compétent** (elles le font très souvent).

Comme la future position commune sur le commerce électronique, **le projet de loi n'exclut aucunement les services financiers,** en effet le projet de loi vise à favoriser ces services dans la société de l'information[3]. Le texte actuel, en liaison avec la très prochaine transposition de la future directive concernant la vente à distance de services financiers, **contribue à la création d'un cadre juridique pour la prestation en ligne de services financiers**.

Il est crucial de préciser que les dispositions du projet de loi n'excluent nullement la législation relative à la protection des données personnelles et celle propre à la protection des consommateurs. Cela signifie que la législation luxembourgeoise qui va transposer les directives 95/46[4] et 97/66[5] relatives aux données personnelles s'appliquera aux prestataires et aux services de la société de l'information qu'ils prestent. La mise en oeuvre et l'application du projet de loi doivent respecter intégralement les principes relatifs à la protection des données à caractère personnel, notamment en ce qui concerne les

---

1 Bruxelles le 18 nov.1999, PE-CONS 3625/99 ECO 357 CODEC 643.

2 Les obligations contractuelles de contrats conclus avec des consommateurs relèvent de la Convention de Rome sur la loi applicable aux obligations contractuelles du 19 juin 1980.

3 Voir **Jean-lou Siweck**, *Banquiers branchés: ebanking*, Lëtzeburger Land du 29 octobre 1999, p. 9.

4 JO L 281, 23 nov. 1995, p. 31.

5 JO L 24, 30 janv. 1998, p. 1.

communications commerciales non sollicitées et le régime de la responsabilité des intermédiaires. Le projet de loi ne saurait empêcher l'utilisation anonyme des réseaux ouverts tels que l'Internet.

De même, la protection des consommateurs concerne notamment la future législation transposant la directive relative à la vente à distance.

Les exclusions au champ d'application de la loi sont de deux ordres:

d'une part, des domaines, activités et contrats sont totalement exclus du champ d'application de la loi et d'autre part, certaines obligations contractuelles, les obligations contractuelles issues de contrats conclus par des consommateurs sont exclues du principe du contrôle du pays d'origine (art. 61 § 2) mais les obligations précontractuelles et les règles de formation du contrat de contrats conclus avec les consommateurs relèvent du principe du pays d'origine.

Le consommateur bénéficie donc toujours de la protection que lui procurent les règles obligatoires relatives aux obligations contractuelles (pour l'exécution du contrat) prévues par le droit de l'Etat membre dans lequel il a sa résidence habituelle.

Un exemple de domaine exclu du projet de loi peut être trouvé, ainsi en est-il de la fiscalité sous réserve de l'article 16. Par contre, les jeux d'argent ne sont exclus que du principe du contrôle du pays d'origine (ils relèvent de la législation du pays de destination du service de la société de l'information) donc ils sont soumis aux dispositions du projet de loi[1]. Il est très important que les „casinos virtuels" soient soumis à un cadre législatif car leur développement hors normes juridiques se révèle dangereux[2]. Nous avons opté pour ce type d'exclusion alors que la future position commune sur le commerce électronique les exclut totalement.

2) De la preuve et de la signature électronique

L'un des principaux obstacles juridiques au développement du commerce électronique se situe certainement au niveau du régime de la preuve des obligations émanant d'un contrat.

Sans réformer les principes essentiels du droit de la preuve luxembourgeois, le projet de loi sur le commerce électronique se propose d'adapter les règles du code civil aux besoins de la société de l'information et de créer un cadre pour la reconnaissance de la signature électronique dans un réseau ouvert tel le réseau Internet[3]. Il tient compte, à cet effet, tant des travaux conduits au niveau international, en particulier européen, que des réflexions menées dans plusieurs Etats qui viennent d'adapter leur législation ou projettent de le faire dans un proche avenir.

En ce qui concerne les premiers, une attention particulière a été portée aux travaux de la CNUDCI. Les principales références demeurent cependant les différents textes communautaires: la directive relative à un cadre communautaire pour les signatures électroniques du 13 décembre 1999 et l'accord politique en vue de la position commune relative au commerce électronique obtenu le 7 décembre au Conseil „marché intérieur".

Parmi les expériences étrangères, on peut notamment citer les textes adoptés dans certains Etats des Etats-Unis, en Allemagne (Loi allemande sur le multimédia du 13 juin 1997, art. 3 sur la signature digitale, Journal officiel allemand du 22 juillet 1997 (BGB, IS, 1870), entrée en vigueur le 1er août 1997) et en Italie (Décret présidentiel italien du 10 novembre 1997, No 513 on „establishing criteria and means for implementing Section 15 (2) of Law No 59 of March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems", in Gazetta Ufficiale, 13 mars 1998, No 60).

Cependant, le droit luxembourgeois de la preuve étant inspiré directement du code Napoléon, ce projet tient compte avant tout des projets discutés actuellement en France (Cf. l'étude du Conseil d'Etat sur l'Internet et les réseaux numériques produite le 2 juillet 1998 et le projet de loi déposé devant le Sénat le 1er septembre 1999 et adopté par le Sénat le 8 février 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique) et en Belgique (Cf. les

---

1 Obligation de transparence notamment.

2 **T. Verbiest**, *Les casinos virtuels: une nouvelle cybercriminalité?*, http://www.juriscom.net.

3 Voir aussi „Etude pour un avant-projet de loi sur le Commerce Electronique" Mission Commerce Electronique ABBL, A. PRUM et Y. POULLET, 1998, Laboratoire de Droit Economique (LDE), Centre de Recherche Public-Centre Universitaire et Centre de Recherche Informatique et Droit (CRID), Facultés Universitaires Notre-Dame de Namur.

avant-projets de la loi visant à modifier certaines dispositions du code civil relatives à la preuve des obligations et de celle relative à l'activité des prestataires de service de certification accrédités en vue de l'utilisation de signatures digitales).

Dans l'esprit de ces derniers projets et de la directive, sont suggérées, dans un premier temps, une série d'adaptations aux règles générales de la preuve littérale en vue de la reconnaissance de la signature électronique et, dans un deuxième temps, les règles permettant d'encadrer l'activité des prestataires de service dites de certification dont l'intervention s'impose pour l'usage de la signature électronique sur un réseau ouvert.

2.1) *De la preuve littérale*

Pour adapter le droit luxembourgeois de la preuve aux développements technologiques récents, trois voies étaient a priori concevables: l'instauration d'un régime de liberté probatoire, la légitimation de la preuve électronique par le biais d'exceptions ou l'adoption d'une conception ouverte et fonctionnelle des exigences posées par le code civil en matière de preuve littérale.

Conduisant à une suppression du régime de la preuve réglementée, la première tend à rendre recevable en justice tout mode de preuve quel qu'il soit. Elle s'inscrit, de ce fait, en rupture profonde avec nos principes traditionnels et n'offre de surcroît qu'une solution imparfaite. Dans un tel système de preuve dit morale, le problème se trouve, en effet, simplement déplacé dans la mesure où les juges sont appelés à apprécier souverainement tous les éléments de preuve qui leur sont présentés sans qu'aucune indication ne leur soit fournie sur leur valeur probante respective.

La seconde alternative passe par une extension du champ d'application des exceptions à l'article 1341 du code civil au demeurant déjà très étendu depuis la réforme du 22 décembre 1986. Elle présente l'inconvénient de ne pas permettre une pleine reconnaissance de la signature électronique. Admise au titre d'une exception à la règle de la preuve littérale, celle-ci serait en définitive condamnée à rester un mode de preuve subalterne, nécessairement subordonnée à la preuve manuscrite.

La troisième voie consiste, à ouvrir les règles existantes aux moyens de preuve issus des nouvelles technologies de l'information à travers une analyse fonctionnelle des concepts d'écrit, de signature et d'original. Préconisée par la CNUDCI et recueillant les faveurs de la doctrine et du législateur français et belge, la solution présente l'avantage de ne pas ébranler le principe de légalité des preuves ni l'équilibre des intérêts que celui-ci entend assurer. Quelques retouches aux règles consacrées par le code civil à la preuve littérale suffisent, en vérité, dans cette approche, pour reconnaître à l'acte sous seing privé électronique une valeur équivalente à celui revêtu d'une signature manuscrite.

Aussi est-ce cette dernière voie que suit le projet de loi luxembourgeois sur le commerce électronique.

2.2) *Des prestataires de service de certification et l'Autorité Nationale d'Accréditation et de Surveillance*

La première section donne les définitions nécessaires à l'établissement des principes généraux amenés à régler l'exécution du commerce électronique.

Comme cela ressort de la définition de la signature électronique, le concept ne se réfère pas à un mécanisme de signature unique mais à des technologies variées (code secret, techniques basées sur la cryptographie symétrique ou asymétrique, signature biométrique, …) qui méritent l'appellation de signature électronique dans la mesure où elles permettent la réalisation, par voie électronique, des fonctions de la signature classique, à savoir, l'identification du signataire et l'expression de sa volonté d'adhérer au contenu du message signé.

La principale fonction d'un prestataire de service de certification est d'assurer un lien formel entre une personne et son identifiant: la signature électronique est créée à l'aide d'une clé privée, la clé publique correspondante et le certificat permettent de vérifier que la signature provient réellement de la clé privée associée, qu'elle est bien celle du signataire et que le message n'a pas été altéré. Ce lien sera confirmé dans un certificat électronique émis par le prestataire de service de certification. Ce certificat contient ainsi différentes informations relatives non seulement à l'identité du titulaire du certificat (celui qui veut signer et s'identifier comme tel), et à son identifiant, mais également à l'identité du prestataire de service de certification. Le certificat est réalisé et signé par le prestataire de service de certification à

l'aide de sa propre clé privée et est, de ce fait, protégé contre les altérations. Le prestataire de service de certification peut ensuite se faire accréditer auprès de l'autorité nationale d'accréditation afin d'offrir des garanties supplémentaires à ses clients.

Le schéma ci-dessous (graphique 5) reprend les explications quant à la certification de la signature électronique et de l'accréditation volontaire reprise dans les articles relatifs aux prestataires de service de certification.

Graphique 5: Certification et Accréditation selon l'avant-projet de loi sur le commerce électronique

Usager 1 ——> certification ——> certificat qualifié + disposition sécurisé de création de signature que le signataire puisse garder sous son contrôle exclusif + signature électronique au sens de l'art. 1322-1 du code civil = effet juridique (art. 18) sauf preuve contraire
Usager 2 ——> signature électronique mais pas de certificat qualifié = pas d'effet juridique sauf preuve contraire
——> certificat qualifié délivré par un prestataire de service de certification non accrédité = pas d'effet juridique sauf preuve contraire
——> certificat qualifié + signature électronique au sens de l'article 1322-1 c.c mais pas de dispositif sécurisé de signature = pas d'effet juridique sauf preuve contraire.

Le rôle du prestataire de service de certification n'est en effet pas minime. Il doit mettre en place une infrastructure qui permette de collecter des informations et d'assurer leur intégrité en toute sécurité. L'efficacité du processus d'identification représente un élément déterminant de la responsabilité du prestataire de service de certification.

C'est pour ces raisons qu'il est indispensable de réglementer l'activité des prestataires de service de certification:

1°) Avant toute chose, il convient de préciser que le projet de loi s'inscrit dans la droite ligne des travaux qui sont actuellement menés au niveau des instances internationales. Il se fonde plus particulièrement sur la directive sur un cadre communautaire pour les signatures électroniques.

2°) Un des objectifs du présent projet a été de ne pas privilégier une technique de signature particulière. Le projet s'étend à cet effet à toute technique de signature, qu'elle soit ou non basée sur la cryptographie asymétrique, actuellement le système le plus utilisé. C'est pourquoi certaines définitions qui n'étaient pas technologiquement neutres ont été insérées dans des règlements grand-ducaux[1] et que toutes les exigences techniques sont insérées dans des règlements grand-ducaux (annexes de la directive).

3°) Conformément à la directive, ce chapitre ne s'applique, en revanche, qu'aux signatures électroniques utilisées en réseau ouvert. Il est considéré que pour les réseaux fermés, le principe de la liberté contractuelle doit continuer à prévaloir. Rien n'empêche toutefois que, par convention, les parties se réfèrent à la présente loi.

4°) Dans la droite ligne de la directive, le projet de loi prévoit un régime volontaire d'accréditation pour les prestataires de service de certification. Un prestataire de service de certification n'a donc pas l'obligation de demander l'accréditation pour exercer ses activités de création, délivrance et gestion des certificats. L'obtention et le maintien de l'accréditation ont toutefois pour conséquence de soumettre les prestataires de service de certifications accrédités à certaines dispositions spécifiques.

5°) Si certaines dispositions sont spécifiques aux prestataires de service de certification accrédités, le présent projet de loi soumet toutefois tous les prestataires de service de certification à des obligations techniques afin de favoriser le climat de confiance indispensable au développement du commerce électronique.

6°) Conformément aux dispositions de la directive les certificats qualifiés délivrés par un prestataire de service de certification dans un autre Etat membre de l'Union européenne, ont la même valeur au Luxembourg que ceux délivrés par un prestataire de service de certification au Luxembourg[1], tandis

1 Par exemple dispositif de création de signature, données afférentes à la création de signature.

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

- si le prestataire de service de certification remplit les conditions posées par le présent projet de loi et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi par un Etat membre de l'Union européenne; ou
- si un prestataire de service de certification établi dans un Etat membre de l'Union européenne garantit ces certificats ou;
- 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.

L'Autorité Nationale d'Accréditation est créée auprès du Ministère de l'Economie qui a déjà compétence pour les dossiers d'accréditation dans le domaine des services et de l'industrie. Les dispositions finales du projet prévoient un renforcement des ressources humaines pour développer ces activités.

Le projet de loi ne contient pas de sanctions pour les prestataires qui usurpent la qualité de prestataire accrédité car ils peuvent être sanctionnés au titre de la loi du 27 novembre 1986 réglementant la concurrence déloyale[2].

3) Des dispositions d'ordre pénal

3.1) *Des sanctions pénales*

La réglementation du commerce électronique, en particulier la modification des dispositions du Code civil sur la preuve littérale, requiert également certaines adaptations du Code pénal.

Un aménagement de l'infraction de **faux** en écritures et d'usage de faux s'impose en vue de protéger l'écrit électronique au même titre que l'écrit traditionnel.

Mais, au-delà de cette modification ponctuelle, se pose la question d'une adaptation plus générale d'autres dispositions du Code pénal affectées par l'informatique.

Il faut, en effet, savoir que l'informatique et les données transmises par ce moyen ou ce support peuvent être l'objet ou l'instrument de nombre d'infractions dans tous les secteurs du droit pénal.

A côté des atteintes aux droits de la personne, qui peuvent résulter de la création ou de l'utilisation de fichiers ou de traitements informatiques de données personnelles, ce sont les crimes et délits contre les biens qui sont concernés, au premier chef, par les nouvelles technologies.

Les valeurs nouvelles que constituent les biens dits informationnels ou informatiques peuvent être l'objet d'atteintes au même titre que les biens matériels traditionnels. Or, force est de constater que les infractions classiques sanctionnant l'atteinte contre les biens, en particulier le vol, l'abus de confiance ou l'escroquerie, de même que l'extorsion ou le recel, présupposent la matérialité de l'objet du délit.

Le vol est l'archétype du délit d'appropriation illicite ou d'atteinte juridique aux biens. C'est à propos de cette infraction que s'est engagée la discussion fondamentale sur la répression des atteintes à un bien immatériel.

L'article 461 du Code pénal luxembourgeois, identique aux articles 379 du Code pénal français et 461 du Code pénal belge, vise la soustraction frauduleuse de la chose d'autrui.

Un large courant doctrinal, notamment en France, a soutenu la thèse que les termes de cette infraction s'opposaient à son extension aux atteintes portées à des biens immatériels.

Sans entrer dans tous les détails techniques de ces discussions, on peut schématiquement retenir que les obstacles élevés à l'encontre d'un élargissement du champ d'application de l'infraction de vol ont porté sur les points suivants:

– L'objet du vol serait une chose, c'est-à-dire un meuble corporel. Les biens incorporels seraient exclus du domaine du vol, sauf s'ils sont intégrés dans un support matériel objet de la soustraction frauduleuse.

---

1 Principe de la reconnaissance mutuelle.

2 Loi du 27 novembre 1986 réglementant certaines pratiques commerciales et sanctionnant la concurrence déloyale telle qu'elle a été modifiée par la loi du 14 mai 1992. Mémorial A No 35, 29 mai 1992, p. 1119.

A cela on a ajouté que l'information, cas type du bien incorporel, ne peut pas être un objet de propriété au sens du droit civil. Certains des biens immatériels seraient tout au plus protégés par les réglementations sur les droits de propriété intellectuelle qui sanctionnent notamment l'acte de contrefaçon.

– Une autre critique avancée contre une extension de l'infraction de vol a été tirée du concept de soustraction. La soustraction impliquerait un déplacement de la chose ou une usurpation de la possession ce qui exigerait qu'elle porte sur un meuble corporel.
– Il a encore été soutenu que la soustraction présuppose un dépouillement du propriétaire au profit du voleur; or, dans le vol d'informations, le titulaire légitime ne serait pas privé de cette information, mais tout au plus du droit exclusif d'en disposer[1].
– Un autre courant doctrinal, qui a précédé de peu l'évolution jurisprudentielle décisive de la fin des années 1980, a considéré que le concept de chose pouvait s'appliquer à des biens immatériels et que ceux-ci étaient susceptibles d'appropriation et de soustraction frauduleuse au détriment de leur propriétaire[2].

Dans deux arrêts de 1989, considérés à l'époque comme des arrêts de principe, la Cour de cassation française a jugé que les biens incorporels étaient susceptibles de vol.

Dans l'arrêt Bourquin du 12 janvier 1989[3] la haute juridiction a reconnu que le vol pouvait porter sur le „contenu informationnel" de disquettes informatiques contenant le fichier des clients d'une entreprise.

Dans l'arrêt Antoniolli du 1er mars 1989[4], elle a jugé qu'un employé, qui avait transmis à un tiers des „données comptables et commerciales", avait été à juste titre condamné pour vol. Selon la Cour, ces données constituent „des biens incorporels qui se trouvent être juridiquement la propriété exclusive de l'entreprise".

De même, dans deux arrêts des 24 octobre 1990 et 18 juin 1991, la Cour de cassation a refusé de sanctionner la qualification de vol qu'une Cour d'appel avait retenu pour la prise en photocopie d'un document[5].

Il est vrai que cette jurisprudence a été, par la suite, partiellement remise en cause par la Cour de cassation même et qu'elle continue à être contestée par les juges du fond.

Ainsi, dans un arrêt du 12 décembre 1990, la Cour de cassation a jugé que les „communications téléphoniques constituent des prestations de service non susceptibles d'appropriation et n'entrent pas de ce fait dans la catégorie des choses visées par l'article 379 du Code pénal"[6].

Plus important est un arrêt du 3 avril 1995 dans lequel la Cour de cassation a jugé qu'une information, qu'elle qu'en soit la nature ou l'origine, échappe aux prévisions de l'article 460 (ancien) du Code pénal sur le recel[7].

Il est vrai que cet arrêt est intervenu à un moment où avait déjà été adopté le nouvel article 321-1 du Code pénal français qualifiant comme recel „le fait … de bénéficier, par tout moyen, du produit d'un crime ou d'un délit".

---

1 Pour la thèse opposée à une extension de l'infraction, au cours des années 1980 en France, voir: J. Pradel et Ch. Feuillard, Les infractions commises au moyen de l'ordinateur, Rev. dr. pén. et crim. 1985, p. 307; Masse, in Informatique et droit pénal, Cujas 1983, p. 30; J. Huet, La modification du droit sous l'influence de l'informatique: aspects de droit privé, JCP 1983, I. 3095; Vivant, Informatique et propriété intellectuelle, JCP 1984, I. 3169; Goutal, La protection juridique du logiciel, D 1984, chr. p. 197; voir, pour les années 1990, W. Jeandidier, Droit pénal des affaires, précis Dalloz;

pour la Belgique, voir: J.P. Buyle, L. Lannoye et A. Willems, Chronique de jurisprudence, JT 1988, p. 119;

2 Pour les protagonistes d'une extension de l'infraction de vol, au cours des années 1980 en France, voir: J. Devèze, Le vol de „biens informatiques", JPC 1985, I. 3210; M.P. Lucas de Leyssac, Une information est-elle susceptible de vol ou d'une autre atteinte juridique aux biens, D 1984. chr. p. 43; Corlay, Réflexion sur les récentes controverses relatives au domaine et à la définition du vol, JCP 1984, I. 3160;

pour la Belgique, voir : B. de Schutter, La criminalité liée à l'informatique, Rev. dr. pén. et crim. 1985 p. 383; J.P. Spreutels, Le vol de données informatiques, même Revue, 1991, p. 1027;

3 Bull. crim. No14.

4 Bull. crim. No 100.

5 JCP, éditions techniques Droit pénal 1991, Art. 379 No 11 et 1992, Art. 379 No 7.

6 Bull. crim. No 430.

7 Bull. crim. No 142, JCP, 1995 II 22429, Revue de science criminelle, 1995, p. 599.

De même, certaines cours d'appel ont refusé de suivre la jurisprudence Bourquin et Antoniolli en jugeant que le vol exigeait la soustraction frauduleuse d'une „chose matérielle ou corporelle", ou que le fait d'utiliser clandestinement des terminaux Minitel ne constituait pas un vol[1].

En Belgique, une évolution similaire, quoique moins nette, s'est opérée au niveau des juridictions de fond.

Ainsi, les Cours d'appel d'Anvers et de Bruxelles ont condamné le vol de programmes de logiciel[2].

D'autres juridictions belges ont refusé de franchir ce pas. Ainsi, la Cour d'appel de Liège a jugé que le fait de copier un programme électronique n'était pas un vol ni un abus de confiance parce que „les signaux" sont „des choses incorporelles qui ne peuvent pas être transmises par la tradition"[3].

Au Luxembourg, la jurisprudence admet traditionnellement que seuls les meubles corporels sont susceptibles de vol[4] et que la soustraction doit être entendue comme le fait matériel d'appréhender une chose[5]. Il ne semble pas que, dans une période plus récente, les juridictions, notamment supérieures, aient été appelées à préciser la jurisprudence luxembourgeoise au regard des évolutions intervenues en France.

Devant cette situation, plusieurs voies sont ouvertes au législateur luxembourgeois.

– Renoncer à toute modification législative et laisser au juge luxembourgeois le soin d'interpréter les textes existants pour les adapter aux nécessités de la société contemporaine. Le législateur luxembourgeois suivrait ainsi l'exemple du législateur français qui n'a pas modifié les dispositions sur le vol compte tenu des positions adoptées par la Cour de cassation. Ce faisant, le législateur luxembourgeois devrait toutefois anticiper une évolution jurisprudentielle qui est loin d'être acquise et perpétuerait l'état actuel d'insécurité juridique qui n'est pas propice au développement du commerce électronique.

  Par ailleurs, cette façon de procéder n'est pas sans soulever des critiques, dans la mesure où elle oblige le juge, appelé à appliquer des dispositions techniquement inadaptées, à recourir à une interprétation extensive du texte, voire contraire à sa lettre. Or, la méthode d'interprétation littérale ou restrictive en matière pénale est essentielle pour sauvegarder les droits du prévenu et assurer la sécurité juridique.

– Une deuxième voie consisterait dans l'adoption d'une réglementation spécifique pour les infractions dites informatiques.

  C'est le choix opéré au Luxembourg par la loi du 15 juillet 1993 relative à certaines infractions en matière informatique (articles 509-1 et suivants du Code pénal). Cette solution a encore été retenue en France à propos des dispositions spécifiques du Code pénal sanctionnant les atteintes aux systèmes de traitement automatisé de données (articles 323-1 à 323-7 du Code pénal français).

  Cette méthode a pour avantage de permettre l'élaboration de textes qui répondent, avec une grande précision, aux caractéristiques des technologies modernes.

  Elle se conçoit aisément, voire s'impose, si les infractions envisagées sont „inédites", inhérentes à la nouvelle technologie, et ne peuvent pas être rattachées au droit pénal traditionnel.

  Ces conditions étaient données pour les dispositions nouvelles insérées dans le Code pénal luxembourgeois par la loi du 15 juillet 1993, précitée, qui sanctionnent des actes d'atteinte à un système informatique et aux données traitées dans ce système.

– La troisième solution consistant à aménager les dispositions existantes du Code pénal est toutefois préférable si „l'infraction informatique" ne constitue pas un acte délictueux nouveau mais une forme que prend une infraction existante. L'élément informatique n'apparaît dans ce cas que comme une modalité technique de la réalisation de l'infraction ou une caractéristique de son objet.

Tel est assurément le cas pour les infractions contre les biens incorporels que constituent les informations contenues dans un système informatique ou transmises par ce système. En effet, l'atteinte au patri-

---

1 CA Paris 25 novembre 1992, GP 1993, 2e semestre, p. 474; CA Aix-en-Provence, 23 octobre 1996, GP trihebdomadaire. 20-22 juillet 1997, p. 34.

2 CA Anvers, 13 décembre 1984, Pas. belge 1985, II, 48; CA. Bruxelles 5 décembre 1986 cité dans J.P. Speutels, op. cité p. 1045; voir, dans le même sens, Tribunal correctionnel de Bruxelles, 19 novembre 1992, Rev. dr. pén. et crim. 1993, p. 355 et 24 juin 1993, même Revue 1994, p. 1262.

3 CA Liège, 25 avril 1991, Rev. dr. pén. et crim. 1991, p. 1013.

4 Cour de cassation 12 juillet 1928, P. 11, 330.

5 Cour d'appel 26 septembre 1966, P. 20, 239.

moine d'autrui peut porter indifféremment sur des biens de nature matérielle ou incorporelle. La nouvelle jurisprudence française sanctionnant le „vol informatique", sur la base des textes existants, s'inscrit d'ailleurs dans cette ligne de raisonnement.

Rattacher les atteintes aux biens incorporels aux dispositions pénales traditionnelles présentent encore l'avantage de maintenir la cohérence du droit pénal, y compris au niveau des circonstances aggravantes et des peines, et d'assurer l'unité dans l'interprétation jurisprudentielle.

Ces raisons ont amené à opter, dans le présent projet de loi, pour cette troisième solution et à proposer des modifications des dispositions pénales existantes.

Au niveau de la technique des aménagements, le présent projet de loi est inspiré par deux soucis: rester le plus près possible des textes actuels et consacrer un concept nouveau valable pour toutes les atteintes contre les biens. Le recours occasionnel à des notions nouvelles s'explique par des nécessités „techniques" inhérentes aux technologies informatiques.

Pour ce qui est du champ d'application matériel, les modifications envisagées concernent, à côté du faux en écritures, les crimes et délits contre les biens, en particulier le vol et les infractions voisines que sont l'abus de confiance, l'escroquerie, l'extorsion ainsi que le recel. Il s'agit, à propos de chacune de ces formes d'atteinte aux biens, de préciser que, parmi les objets des infractions, figurent également les biens qui ne sont pas des „choses" selon la terminologie classique de l'infraction de vol.

Le projet de loi a retenu à cet égard le concept de bien incorporel. Ce terme est en relation antinomique avec celui de chose signifiant un objet corporel. Ce concept est consacré dans l'arrêt de la Cour de cassation française du 1er mars 1989. Il est à préférer à ceux de bien informatique, d'information, de bien informationnel utilisés dans la doctrine française, parce que son domaine d'application est plus large; en effet, le concept de bien incorporel est susceptible d'englober non seulement les informations au sens restreint du terme, mais toute donnée, voire tout bien qui n'est pas matériel. La consécration du terme de bien incorporel permet encore de protéger contre une atteinte illicite toute donnée, même celle qui ne figure pas au moment de l'infraction sur un support informatique. L'utilisation de ce terme, à portée générale, permet de faire l'économie de modifications ponctuelles variées qui, de toute façon, s'avéreraient insuffisantes.

La démarche du législateur français, qui a complété certaines dispositions pénales en recourant à des concepts chaque fois différents, n'est pas sans soulever des problèmes au niveau de la cohérence du droit pénal[1].

Le terme de bien met en évidence que l'infraction n'est établie que si son objet immatériel a une valeur patrimoniale et est susceptible d'appropriation. Cette appropriation doit être entendue comme le droit exclusif du titulaire de disposer du bien incorporel.

Des adaptations mineures des textes existants visent à réprimer l'utilisation de moyens informatiques aux fins d'atteinte aux biens d'autrui. Il s'agit, pour l'essentiel, d'insérer dans les textes l'instrument des (fausses) clés électroniques.

Finalement, il y a lieu de faire une remarque générale relative à l'impact des modifications proposées aux articles 509-1 et suivants du Code pénal sanctionnant certaines infractions en matière informatique. Ainsi qu'il a déjà été expliqué, la loi du 15 juillet 1993 a pour objectif de protéger les systèmes informatiques et les données figurant dans ces systèmes contre des atteintes, alors que les modifications envisagées dans le présent projet visent à protéger les biens incorporels assimilés, à cet égard, à des choses corporelles.

Des problèmes de délimitation peuvent éventuellement se poser entre les articles 509-4 et 509-5 du Code pénal relatifs à la falsification de documents informatisés ou à l'usage de ces documents et les articles révisés 196 et 197 sur le faux en écritures et l'usage de faux.

Les articles 196 et 197 visent le faux en écritures, ce concept étant entendu par la jurisprudence comme un écrit (matériel ou électronique) susceptible de faire preuve et de causer ainsi préjudice.

Les articles 509-4 et 509-5 incriminent la falsification de documents informatisés, c'est-à-dire de toutes les données figurant dans un système informatique. Ces textes ne visent pas la falsification d'un écrit précis susceptible d'avoir une valeur probatoire.

---

1 L'article 311-2 du nouveau Code pénal français sanctionne comme vol la soustraction frauduleuse d'énergie; L'article 312-1 vise l'extorsion d'un secret; L'article 313-1 condamne l'escroquerie d'un service; L'article 321-1 a étendu le recel au bénéfice du produit d'un crime ou d'un délit.

Les champs d'application des textes sont dès lors a priori différents.

Même si un fait délictueux donné devait relever des dispositions des articles 196 et 509-4, cette circonstance ne soulèverait pas des problèmes au niveau de l'application du droit pénal.

Le juge répressif serait en présence d'un concours idéal d'infraction et, appliquerait, sur base de l'article 65, la peine la plus forte, en l'occurrence la peine criminelle comminée par l'article 196 du Code pénal.

3.2) *De l'instruction*

La gestion de données dans un système informatique, combinée avec les possibilités techniques du cryptage ou de la protection de ces données, pose des défis nouveaux au magistrat instructeur.

Pour l'heure, les dispositions de l'article 66 du Code d'instruction criminelle permettent au juge d'instruction de procéder à une saisie du support matériel de données informatiques, qu'il s'agisse des disquettes ou de l'ordinateur comportant le disque dur.

De même, le juge d'instruction fait procéder à la confection de copies des données figurant dans un système sur un autre support aux fins de l'exploitation ultérieure des données visées.

La question de savoir si le juge d'instruction peut interdire l'accès à certaines données qu'il a saisies, devrait également recevoir une réponse affirmative.

Même si les dispositions actuelles offrent une base légale, a priori suffisante, pour ce type de mesures d'instruction, il est préférable de clarifier les textes et de préciser les pouvoirs du juge d'instruction.

En effet, l'article 66 du Code d'instruction criminelle peut soulever des problèmes d'interprétation et d'application analogues à ceux posés par la formulation actuelle des délits contre les biens. L'article 66, de même que l'article 31 auquel il renvoie, a pour objet la saisie d'objets, de documents, d'effets et d'autres choses; cette énumération vise des objets corporels, à moins d'interpréter le concept de chose dans un sens très large. Si la saisie du support informatique relève de ce cadre légal, quitte à accepter que le support matériel, sans valeur pour les besoins de l'instruction, absorbe en quelque sorte l'information recherchée, la saisie de l'information en tant que telle, fût-ce par copie ou simple prise de connaissance, est plus problématique.

Le respect des droits de la défense au cours de l'instruction exige une clarification des pouvoirs du magistrat instructeur.

Dans le souci de maintenir la cohérence des différentes mesures d'instruction, quelles que soient les caractéristiques techniques de leur objet, le projet de loi renonce à proposer un régime spécifique, techniquement complexe, de saisie de données informatiques. L'objectif est d'instituer un régime légal qui reste le plus proche possible de celui des saisies traditionnelles d'objets corporels et qui consacre et précise dans les textes les pratiques actuelles.

Le système envisagé s'inspire des mesures prévues dans le projet de loi relatif à la criminalité informatique actuellement débattu en Belgique, même si les mécanismes proposés sont moins complexes et s'inscrivent dans la logique des saisies traditionnelles d'objets corporels.

A cet effet, le projet de loi prévoit de compléter l'article 66 actuel du Code d'instruction criminelle par un nouvel article 66-1, qui consacre expressément le droit du juge d'instruction de saisir les données informatiques et d'opérer, à cet effet, la saisie de leur support matériel ou de les copier sur un autre support. Il est encore indiqué de préciser que le juge d'instruction peut interdire l'accès aux données saisies ou les retirer du système.

En vue d'assurer à ce type de saisie la plus grande portée possible, il est précisé que les données susceptibles de saisie sont celles stockées, traitées ou transmises dans un système informatique.

Les pouvoirs reconnus au juge d'instruction par les deux premiers alinéas du nouvel article 66-1 doivent être étendus à l'officier de police judiciaire agissant à l'occasion d'un flagrant délit.

A cet effet est inséré un nouvel article 33-1 qui précise les pouvoirs de l'officier de police judiciaire de procéder à la saisie de données informatiques dans les mêmes termes que ceux prévus pour les saisies opérées par le juge d'instruction.

Ce texte se réfère, expressément, aux articles 31 et 33 relatifs aux saisies opérées sur le lieu du crime et au domicile des personnes qui paraissent être les auteurs de l'infraction.

Une des difficultés majeures auxquelles est confronté le juge d'instruction est celle de l'accès à des données cryptées ou protégées. Au regard de l'amélioration des mécanismes de cryptage et de protec-

tion, du recours de plus en plus fréquent à ces méthodes et des moyens de décryptage limités dont disposent les services de police judiciaire, il s'impose de prévoir un instrument juridique par lequel le juge d'instruction peut obliger une personne à lui donner accès à un système protégé ou à des données cryptées.

Le régime qu'il est proposé d'instituer, au troisième alinéa de l'article 66, doit constituer à la fois un instrument efficace entre les mains du juge d'instruction qui voudrait obtenir l'accès à des données protégées ou cryptées et sauvegarder les principes fondamentaux de l'instruction relatifs aux droits de la défense.

Le juge d'instruction peut ordonner à une personne qu'il désigne qu'elle lui donne accès au système saisi ou aux données qu'il contient ainsi qu'à la compréhension des données saisies protégées ou cryptées. Pour pouvoir désigner une personne, le juge d'instruction doit considérer qu'elle a une connaissance particulière du système informatique ou des mécanismes de protection ou de cryptage. Le texte précise que la personne désignée a l'obligation de prêter son concours. Cette obligation légale est sanctionnée par une amende que le juge d'instruction impose en cas de refus de collaboration.

Pour garantir que cet instrument dont disposera le juge d'instruction ne puisse conduire à des violations de certains principes fondamentaux de l'instruction contradictoire, un certain nombre de garanties sont prévues.

– Notons d'abord, même s'il s'agit d'une évidence, que seul le juge d'instruction peut recourir à cette mesure, à l'exclusion de l'officier de police judiciaire en cas de flagrant délit.
– Le juge d'instruction procède par ordonnance motivée, ce qui implique une obligation de justifier la mesure d'instruction, notamment au regard de l'identité de la personne désignée.
– Peut uniquement être désignée une personne dont le juge d'instruction considère qu'elle dispose des connaissances techniques permettant l'accès aux données.
– L'inculpé ne pouvant être forcé de fournir des preuves à sa charge, ne peut pas non plus être obligé de prêter son concours.
– Ne peuvent pas davantage faire l'objet d'une ordonnance du juge d'instruction les personnes protégées par les articles 72, 73 et 76 du Code d'instruction criminelle, à savoir les personnes nommément visées par une plainte avec constitution de partie civile, les personnes contre lesquelles il existe des indices graves et concordants de culpabilité et les enfants au-dessous de 15 ans.
– Enfin, garantie essentielle, le texte s'applique sous la réserve expresse des cas où la personne visée est obligée de garder secrets les renseignements lui confiés dans le cadre de son activité professionnelle.

L'amende qui sanctionne le refus de collaboration est celle comminée par l'article 77 (2) pour le refus de témoigner.

Il est proposé de relever le taux de cette amende à 100.000.– francs pour souligner l'importance de l'obligation de témoigner ou de donner accès à des données informatiques protégées ou cryptées.

Il est intéressant de noter que le projet de loi relative à la criminalité informatique élaboré en Belgique prévoit d'instituer un mécanisme similaire, même si les références aux dispositions sur les dépositions testimoniales sont moins prononcées.

Pour terminer, il convient de relever qu'une adaptation des articles 88-1 et suivants du Code d'instruction criminelle relatifs aux mesures spéciales de surveillance ne s'impose pas. En effet, les textes actuels sont formulés de façon suffisamment large pour permettre la surveillance de moyens de communication informatique si de telles méthodes de surveillance devaient être techniquement possibles.

4) Des communications commerciales

Les communications commerciales sont essentielles pour le financement des services de la société de l'information et le développement d'une large variété de nouveaux services gratuits. L'expression „communications commerciales“[1] couvre toutes formes de publicité, de marketing direct, de par-

---

1 *Livre vert sur les communications commerciales dans le marché intérieur*, novembre 1992, voir site de la DGXV, rubrique „communications commerciales“ , http://www.europa.eu.int., VT4 5 juin 1997 C-56/96 pt 19.

rainage, de promotion des ventes et de relations publiques destinées à promouvoir des produits et des services.

La référence à la promotion directe ou indirecte vise à empêcher les cas de contournement de l'interdiction de faire de la communication commerciale pour certains produits ou services.

Dans l'intérêt des consommateurs et de la loyauté des transactions, les communications commerciales, y compris les jeux promotionnels et les offres, doivent respecter un certain nombre d'obligations relatives à la transparence et ces obligations doivent être sans préjudice de la législation relative à la protection des consommateurs[1] et à la protection des données personnelles.

L'envoi par courrier électronique de communications commerciales non sollicitées peut être inopportun pour les consommateurs et pour les fournisseurs de services de la société de l'information et susceptible de perturber le bon fonctionnement des réseaux interactifs. Le Luxembourg autorise l'envoi par courrier électronique de communications commerciales non sollicitées car cela constitue un avantage indéniable pour le développement des PME.

Comme le précisait déjà la directive 97/7/CE on ne peut envoyer des communications commerciales non sollicitées sans le consentement du consommateur[2] c'est-à-dire **sans opposition manifeste de sa part** et cela est précisé à l'article 59 § 2 qui vise tout destinataire donc tout utilisateur[3].

Ainsi que l'utilisateur exprime son consentement ou son absence de consentement, il existe deux systèmes: l'opt out et l'opt in. Nous avons opté pour le système de l'opt out qui offre plus de souplesse pour les opérateurs. Le système d'opt out revient à autoriser les communications commerciales non autorisées (spamming) sauf opposition expresse du destinataire qui peut, à cet effet, s'inscrire sur une liste d'opt out que les opérateurs devront consulter.

L'opt in revient à interdire le spamming sauf autorisation expresse de la part du destinataire; or nous n'avons pas choisi ce système car il se révèle rigide et sa mise en application est difficile d'un Etat membre de l'Union européenne.

En tout état de cause, les communications commerciales non sollicitées doivent être clairement identifiables en tant que telles afin d'améliorer la transparence. En pratique, la communication commerciale non sollicitée doit faire l'objet d'une mention particulière sur „l'enveloppe" afin que celui qui reçoit un tel courrier puisse immédiatement identifier qu'il s'agit de la communication commerciale sans avoir à l'ouvrir[4].

La mise en place de listes d'opt out par les entreprises établies au Luxembourg est encouragée.

5) Des contrats conclus par voie électronique

En l'état actuel, le droit luxembourgeois protège les consommateurs dans le seul cadre des contrats conclus par correspondance (article 7 de la loi du 25 août 1983), la loi n'ayant pas encore été étendue aux ventes et prestations de services à distance. La directive 97/7 du 20 mai 1997 concernant les contrats à distance n'a pas encore été transposée en droit luxembourgeois mais va l'être très prochainement. A cet égard nous faisons déjà figurer dans le projet de loi certaines dispositions de protection du consommateur. L'objet du projet de loi sur le commerce électronique n'est pas de transposer intégralement cette directive dont la portée dépasse largement celle des contrats conclus par voie électronique, mais de retenir certaines dispositions jugées utiles dans le contexte du commerce électronique.

Voici donc le cadre législatif qui a été mis en place, précisons toutefois que ce titre ne contient pas que des dispositions protectrices du consommateur mais aussi des dispositions protectrices des utilisateurs.

En premier lieu, est déterminé le champ d'application du texte en matière de contrats par voie électronique. Une liste des contrats exclus du champ d'application du titre V est dressée et comprend les

---

1 Notamment la future législation qui va transposer la directive 97/7/CE du Parlement européen et du Conseil concernant la protection des consommateurs en matière de contrats à distance, JO L 144 du 4 juin 1997, p.19.

2 Art.10 de la directive.

3 Et pas uniquement le consommateur.

4 Par exemple par email mention de courrier électronique comme objet du message. Cette exigence figure déjà dans l'article 12 § 2 de la directive 97/66/CE du Parlement et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

contrats emprunts d'un formalisme important tels que les contrats de transfert de droits immobiliers, le cautionnement[1]. Par contre, les contrats portant sur des services financiers ne sont pas exclus afin de bénéficier du texte de loi qui vise à assurer la sécurité juridique et la confiance des opérateurs et des consommateurs.

En second lieu, certaines règles de base en matière contractuelle et par voie électronique sont introduites dans le Titre V et s'inspirent de la position commune sur le commerce électronique mais où la future directive laisse des options, nous exerçons des choix. Ainsi le projet de loi choisit-il de fixer, en univers électronique, le moment de conclusion du contrat alors que la future position commune ne parle que du „moment de passation de la commande". Or il nous semble impératif de clarifier ce point afin d'apporter toute la sécurité juridique nécessaire. En effet, c'est à partir de ce délai que naissent les droits du cocontractant, que les délais courent (droit de rétractation …).

En troisième lieu, l'introduction dans le présent projet de certaines dispositions dont l'intérêt dépasse le seul cadre du commerce électronique, a été rendue nécessaire pour remédier temporairement à l'absence de règles générales régissant précisément toutes les formes de commerce à distance.

Ce titre suit la logique suivante: le projet part du général pour aller au particulier. Le premier chapitre traite des dispositions communes à tous les contrats conclus par voie électronique et le second chapitre ne traite que des dispositions propres aux contrats conclus avec des consommateurs.

Pour le premier chapitre, une obligation d'information générale est due à tout utilisateur (art. 62) et le moment de conclusion du contrat est déterminé afin d'apporter toute la sécurité juridique nécessaire.

Pour le second chapitre, une obligation d'information est exigée pour la protection du consommateur (art. 64) et le professionnel est tenu d'une obligation de confirmation concernant notamment les conditions contractuelles, le contenu de la transaction (art. 65) et les conditions d'exercice du droit de rétractation. A cet égard, le droit de rétractation du consommateur figure à l'article 66 et il possède un régime particulier en ce qui concerne certains services financiers (art. 66 § 4). Par ailleurs, en cas d'exercice du droit de rétractation, le consommateur a droit à la restitution des sommes qu'il a déjà versées ce qui est prévu dans l'article 67.

6) De la responsabilité des prestataires intermédiaires

Si la responsabilité de l'éditeur d'un contenu fait l'objet d'un consensus, la question de la responsabilité de ces intermédiaires reste une question controversée généralement liée au débat sur le contrôle des informations diffusées sur Internet.

Compte tenu de la connaissance limitée que ces intermédiaires ont des informations qu'ils transmettent ou stockent sur les réseaux, la difficulté est de déterminer l'étendue de leur responsabilité par rapport à la responsabilité des personnes ayant mis ces informations en ligne.

Aux Etats-Unis, la loi dite „Digital Millenium Act"[2] contient notamment des dispositions spécifiques sur la responsabilité des prestataires techniques en matière de contrefaçon. Le DCMA limite la responsabilité des fournisseurs techniques à certaines conditions. Les fournisseurs remplissant les conditions posées pour être exonérés ne peuvent se voir réclamer aucun dommage et intérêts ou toute autre sanction pécuniaire pour contrefaçon. La limitation de responsabilité est appréciée en fonction du type d'activité exercée et non en fonction du statut de l'opérateur. Les exonérations de responsabilité prévues peuvent donc non seulement être invoquées par les fournisseurs d'accès commerciaux, mais également par les universités, les entreprises ou toute autre entité, dès lors qu'elle exerce des activités décrites dans la loi.

La future position commune s'est inspirée du DCMA[3] pour le titre VI consacré à la responsabilité des prestataires intermédiaires.

Cette future position commune sur le commerce électronique dans le marché intérieur[4] contient des dispositions prévoyant une limitation de la responsabilité des prestataires de trois types particuliers de

---

1 On sait combien ce contrat est formel notamment pour protéger la caution.

2 Du 28 octobre 1998, texte complet du DMCA pouvant être consulté depuis le site web du Copyright Office américain à l'adresse: http://lcweb.loc.gov/copyright.

3 Voir in Colloque du CRID des 8, 9 et 10 nov.1999 à Namur, *Vers un nouveau droit des technologies de l'information*, **Lisa Peets**, Covington et Burling, *Sum+mary of US DMCA service provider provisions*.

4 Doc No14263/99 ECO 419 CONSOM 80 CODEC 826.

service intermédiaire: le „simple transport“ (art. 12, mere conduit), la forme de stockage dit „caching“ (art. 13) et „l'hébergement“ (art. 14). En ce qui concerne l'article 14 du projet de directive, les prestataires de services (fournisseurs d'hébergement) ne peuvent bénéficier de cette limitation de leur responsabilité que lorsque qu'ils n'ont pas connaissance du fait que l'activité ou l'information hébergée était illicite. Ce test de connaissance n'a pu être étendu aux activités de simple transport et de caching car ils ne peuvent en avoir connaissance, c'est techniquement impossible. Les rendre responsables serait les empêcher d'exercer toute activité sur Internet, choisir de rendre responsables des opérateurs qui sont des intermédiaires techniques et donc refuser de rechercher les véritables coupables, les éditeurs de contenu. De plus cela aboutirait à la délocalisation de ces intermédiaires hors Union européenne.

En revanche, un prestataire de service qui collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales va au-delà des activités de „simple transport“ ou de „caching“ et il ne peut alors pas bénéficier des dérogations en matière de responsabilité prévues pour ce type d'activités.

Cependant, les évolutions technologiques futures pourraient conférer aux intermédiaires la possibilité de surveiller les données qu'ils transmettent, une absence de responsabilité pourrait ne plus être appropriée c'est pourquoi il faudra réexaminer le projet de directive.

L'article 15 du projet de directive interdit aux Etats membres d'imposer aux prestataires intermédiaires des obligations générales de surveillance sur les informations qu'ils transmettent ou stockent, ni aucun devoir général de procéder à une recherche active de faits ou de circonstances indiquant des activités illicites. Cet article est dans la logique des trois articles précédents. En effet, les prestataires ne peuvent voir leur responsabilité limitée et ensuite avoir une obligation de surveillance large car qui dit obligation dit possibilité d'agir en justice pour manquement à son obligation. Par ailleurs, techniquement ces intermédiaires ne peuvent surveiller les milliers voire millions de données qu'ils transportent chaque jour.

Le projet de loi s'est inspiré de ce projet de directive afin de rédiger le titre VI du projet de loi (articles 71 à 74) ainsi assura-t-il la sécurité juridique nécessaire aux prestataires intermédiaires qui veulent s'installer au Luxembourg afin de ne pas se voir imposer une obligation de filtrage ou ce que l'on nomme une obligation de surveillance passive. De plus, ils se verront confiants d'avoir une responsabilité limitée, qu'elle soit civile ou pénale. Il faudra prouver, selon l'activité, qu'ils n'ont pas rempli ou respecté certaines conditions et que leur responsabilité est engagée[1].

Le système de limitation de responsabilité institué a vocation à s'appliquer aussi bien en matière de concurrence déloyale, de publicité trompeuse, de contrefaçon, diffamation et concerne aussi bien la responsabilité civile que pénale. Cependant, ce système de limitation de responsabilité est sans préjudice de la possibilité d'actions en cessation de différents types[2].

Ultérieurement, comme le Parlement européen et la Commission européenne, une réfléxion devra être apportée pour une législation propre à la responsabilité des moteurs de recherche[3] (par exemple yahoo, altavista … c'est-à-dire instruments qui permettent de faire de la recherche sur Internet par mot clé ou autre procédé) et des fournisseurs d'hyperliens (liens sur lesquels vous cliquez sur une page et vous allez sur une autre page web). Mais l'urgence était de réglementer les trois activités traitées qui ont donné lieu à de nombreux litiges chez nos voisins[4].

7) Des paiements électroniques

Avant tout, il a fallu définir certaines notions et faire des choix. En effet, les définitions issues de la recommandation européenne du 30 juillet 1997 relative aux opérations effectuées au moyen d'instru-

---

1 Que ce soit en matière de responsabilité civile ou pénale.

2 Ces actions peuvent revêtir la forme de décisions de tribunaux ou d'autorités administratives exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible.

3 Voir par exemple, **A. STROWEL**, *Liaisons dangereuses et bonnes relations sur l'Internet, à propos des hyperliens*, Auteurs et Médias, 1998, p. 296.

4 Affaire française Estelle Hallyday du 9 juin 1998 où un fournisseur d'hébergement a été déclaré coupable car il n'a pas voulu révéler l'identité de l'éditeur de contenu; Le juge des référés a considéré que pesait sur le fournisseur d'hébergement un devoir actif de vérification du contenu des sites hébergés, v. Revue *Expertises*, octobre 1998, p. 319; v. aussi **V. SEDALLIAN**, *La responsabilité des prestataires techniques sur Internet dans le Digital Millenium Act américain et le projet de directive européen sur le commerce électronique*, http://www.juriscom.net janvier 1999.

ments de paiement électronique[1], en particulier la relation entre émetteur et titulaire, nécessitaient des adaptations.

L'emploi du terme „*instrument de transfert électronique de fonds*" a été préféré à celui d'„*instrument de paiement électronique*", en tout état de cause le contenu est le même[2].

Quant au terme d'instrument de monnaie électronique, nous avons préféré employer le terme plus neutre d'instrument rechargeable et là aussi, l'esprit est le même. Ainsi, le législateur luxembourgeois aura le soin de définir dans un autre texte le terme de monnaie électronique[3].

Ce texte fait suite à deux autres recommandations, l'une du 8 décembre 1987 portant sur un code européen de bonne conduite en matière de paiement électronique, et l'autre du 17 novembre 1988 concernant les systèmes de paiement et en particulier les relations entre titulaires et émetteurs de carte. La Commission y affirme clairement sa volonté de susciter la confiance des utilisateurs en leur assurant un degré de protection élevé dans l'utilisation des moyens de paiement électroniques.

Dans le but de promouvoir le commerce électronique, il paraît opportun d'envisager des mesures tendant à protéger les utilisateurs de moyens de paiements électroniques contre une utilisation frauduleuse de ceux-ci. Par ailleurs, le développement des instruments rechargeables permettra de les utiliser plus tard sur Internet et ainsi de ne courir que très peu de danger puisque ce type d'instruments est détaché du compte bancaire contrairement aux cartes bancaires[4].

Bien que les mesures envisagées soient destinées au premier chef aux transactions conclues par voie électronique, il convient d'observer que le champ d'application du texte proposé dépasse largement le cadre du commerce électronique dans la mesure où ces règles ont vocation à s'appliquer à tout type de transaction, dès lors que le mode de paiement utilisé fait appel à une technique électronique. En effet, par exemple, la définition d'un instrument de transfert électronique de fond mentionne bien que sont visés les systèmes permettant d'effectuer par voie entièrement ou partiellement électronique certaines opérations.

*

1 JOCE L 208/52 du 2.8.1997.

2 Puisque les mêmes opérations sont visées: transferts de fonds, retraits d'argent liquide …

3 Définition à laquelle il sera procédé dans la législation qui transposera la future directive relative à l'accès à l'activité des établissements de monnaie électronique et son exercice, position commune en date du 29 novembre 1999, doc. No 12004/2/99 REV2EF36, ECOFIN 190 CODEC 577.

4 Voir **G. VACHER**, *E-commerce: les cartes de crédit virtuelles ont-elles un avenir?*, http://www.zdnet.fr/actu/busi/a0011395.htm.

PARTIE B

TEXTE DU PROJET DE LOI

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;

Cette définition est volontairement large afin de couvrir des services innovants tels que les journaux en ligne et tous les nouveaux métiers liés à Internet tels que yahoo. En effet, elle ne se limite pas aux contrats électroniques ni à la publicité mais à des activités incluant des moteurs de recherche par exemple. Les services de la société de l'information s'arrêtent là où la voie électronique s'arrête.

Cette définition des services de la société de l'information est reprise de l'art. 2 a) de l'accord politique en vue de la position commune arrêtée par le Conseil le 7 décembre relative à la future directive „sur le commerce électronique“. Cette définition est issue des art. 49 et 50 (art. 59 et 60 ancienne numérotation) du Traité de Rome. Cette dernière recouvre une multitude d'activités économiques très diverses qui peuvent être faites en ligne. Il peut s'agir de services d'entreprise à entreprise ou d'entreprise à consommateurs, de services de vente aussi bien que de services gratuits, de services permettant de faire des transactions électroniques en ligne pour acheter des marchandises comme le téléachat interactif, de journaux électroniques.

Nous envisageons le commerce électronique au sens large comme couvrant l'ensemble des services de la société de l'information.

prestataire: toute personne physique ou morale qui fournit un service de la société de l'information.

Cette définition est directement inspirée de l'article 2 b) de la position commune arrêtée en vue de l'adoption de la directive „commerce électronique“. Cette définition repose sur les articles 59 et 60 du Traité de Rome. Cette dernière, avec celle de prestataire établi constitue un des piliers de cette proposition de directive.

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 tel un établissement du prestataire.

Cette définition est directement inspirée de l'article 2 c) de la position commune en vue de l'adoption de la directive „sur le commerce électronique“. Cette définition constitue l'un des piliers du dispositif mis en place par ce texte. Cette définition fixe le critère qu'il faut prendre en compte pour déterminer la loi applicable. La définition proposée repose sur la jurisprudence de la Cour qui a eu l'occasion de préciser que „la notion d'établissement, au sens des articles 52 et suivants du traité, comporte l'exercice effectif d'une activité économique au moyen d'une installation stable dans un autre Etat membre pour une durée indéterminée“. Cette définition repose sur des critères qualitatifs de l'effectivité et de la stabilité de l'activité économique et non sur des critères formels (simple boîte aux lettres) ou technologiques (emplacement des moyens techniques …) qui permettent facilement aux opérateurs d'échapper à tout contrôle.

Ne constituera pas, par exemple, un établissement au Luxembourg, l'hébergement de pages web ou d'un site au Luxembourg d'une entreprise établie dans un autre Etat membre.

„*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 de l'information;

Ce terme couvre tout type d'utilisateur, que se soit un professionnel ou un consommateur.

Ainsi, le considérant 9bis de la future position commune en vue de l'adoption de la directive sur le commerce électronique précise que la définition du destinataire de service couvre tous les types d'utilisation des services de la société de l'information tant par les personnes qui fournissent l'information sur les réseaux ouverts tels que l'Internet, que par celles qui recherchent des informations sur l'Internet pour des raisons privées ou professionnelles.

Par exemple, une personne qui utilise un service consistant à organiser un forum de discussion et qui y dépose un message.

Nous n'avons pas repris la définition de consommateur issue de l'art. 2 e) de la future position commune en vue de l'adoption de la directive sur le commerce électronique car elle ferait double emploi avec la définition issue de la directive 97/7/CE relative à la vente à distance qui va être transposée.

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.

Ce paragraphe 2, deuxième alinéa vise à empêcher que les prestataires de service échappent au droit de la concurrence en ayant des activités sur Internet, notamment des activités commerciales.

§ 2.– Les dispositions de la présente loi ne s'appliquent pas aux activités suivantes:

– les activités de notaires ou de professions équivalentes dans la mesure où ils supposent un lien direct et spécifique avec l'exercice d'une autorité publique;

– la représentation d'un client et la défense de ses intérêts devant les tribunaux;

Quant au § 2, il est largement inspiré de l'article 1er § 4 d) de l'accord politique en vue de la position commune, pour le premier tiré sont seulement visés les actes authentiques, l'activité de notaire en tant qu'officier public. Par contre, nous n'avons pas repris l'exception qui vise les jeux d'argent, nous ne voulons pas que les jeux d'argent soient exclus du projet de loi mais seulement qu'ils soient une exception au principe du pays d'origine. En effet, il serait utile que ce type de jeux soit soumis aux exigences de certains articles du projet (obligation d'information générale, art. 5, informations précontractuelles, art.61, responsabilité des intermédiaires, art. 66 à 69) afin de garantir certaines exigences minimales notamment aux consommateurs.

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

Ce § 3 vise à préciser que cette loi est d'application horizontale, elle n'empêche pas que la législation relative à la protection des données personnelles issue de la très prochaine transposition des directives 95/46/Ce et 97/66/CE s'applique au commerce électronique.

§ 4.– Les prestataires de services de la société de l'information établis au Luxembourg et les services qu'ils prestent ne sont tenus que par la présente loi.

§ 5.– Il est fait exception au principe de l'application de la loi du lieu d'établissement du prestataire:

– pour les 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 des paris.

– pour les obligations contractuelles de contrats conclus avec des consommateurs.

Cet article s'inspire de l'article 3 de l'accord politique en vue de la position commune „commerce électronique“ qui pose le principe du pays d'origine. Cet article permet de déterminer la loi applicable, ainsi les prestataires qui ont leur établissement au Luxembourg ne relèvent que de la loi luxembourgeoise même s'ils fournissent des services de la société de l'information dans les autres pays de l'Union européenne. Ce principe du pays d'origine figure aussi dans l'article 4 de la directive relative à un cadre communautaire pour les signatures électroniques[1]. Ainsi l'article 4 dispose-t-il que „chaque Etat membre applique les dispositions nationales qu'il adopte aux prestataires de service de certification établis sur son territoire et aux services qu'ils fournissent.“

---

1 Du 13 décembre 1999, op. cit.

Quant à l'exception concernant les jeux d'argent, elle signifie que ces activités ne se voient pas appliquer le principe de libre circulation des services ni celui du principe du pays d'origine. Ainsi, les Etats membres peuvent légitimement restreindre ou interdire la libre prestation de services en matière de jeux d'argent sur leur territoire.

L'idée de ne pas exclure totalement les jeux d'argent du champ d'application de la proposition de directive, est pertinente car cette dernière fournit une certaine sécurité juridique dans le marché intérieur sur plusieurs points:

- *l'obligation de transparence de tous les acteurs: lieu d'établissement de la société qui organise les loteries, son numéro d'inscription au registre du commerce …;*
- *l' identification claire des communications commerciales (publicité, parrainage …).*

Le § 2 est issu de l'annexe (dérogations à l'article 3 qui pose le principe du pays d'origine) de l'accord politique en vue de la future position commune relative au commerce électronique afin de protéger les consommateurs, cette exception fait référence à l'article 5 de la Convention de Rome de 1980 sur la loi applicable aux obligations contractuelles[1]. Au préalable précisons que nous visons précisément les obligations contractuelles et non, plus largement les contrats conclus avec les consommateurs. Ainsi, les règles de formalisme juridique, les conditions générales de vente relèvent de la législation du pays d'origine.

L'article 5 de la Convention de Rome dispose que le choix par les parties de la loi applicable au contrat ne peut avoir pour résultat de priver le consommateur de la protection des dispositions impératives de la loi du pays où il a sa résidence habituelle sous trois conditions:

– *la conclusion du contrat ait été précédée dans ce pays d'une proposition spécialement faite ou d'une publicité et si le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat.*

Art. 3.– *De l'usage de la cryptographie*

L'usage des techniques de cryptographie est libre.

Pour promouvoir le commerce électronique, cet article souligne le principe de liberté quant à l'application de la cryptographie aux fins du commerce électronique, contrairement à d'autres pays où l'utilisation de la cryptographie est interdite ou restreinte.

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

L'accès à l'activité de prestataire ne fait, en tant que telle, l'objet d'aucune autorisation préalable spécifique.

L'objectif de cet article est de favoriser le développement des activités de prestation de services sur Internet. La disposition s'explique par la volonté du Luxembourg de ne pas ajouter aux dispositions déjà existantes pour certaines professions des contraintes réglementaires pour l'utilisation des nouvelles potentialités des autoroutes de l'information pour l'offre de services de la société de l'information. En d'autres termes, conformément aux dispositions de la position commune arrêtée par le Conseil en vue de l'adoption de la directive du Parlement Européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le Marché intérieur[2] (article 8), il s'agit de poser le principe général suivant lequel la mise sur site d'activités commerciales ne fait l'objet d'autres réglementations que celles déjà existantes et non spécifiques à la société de l'information.

En outre, il va de soi que la disposition ne préjudicie en rien à l'application de la loi luxembourgeoise de 1988 sur l'accès à la profession et des régimes de notification ou de licence prises en application de la directive 97/13/CE du 15 décembre 1997. En d'autres termes, le commerçant qui souhaite offrir ses services via Internet devra satisfaire aux conditions éventuellement imposées sur base de la loi d'accès à la profession de 1988 mais ne pourra se voir imposer des obligations supplémentaires du fait de l'utilisation d'Internet pour l'exploitation de ses services. De plus, cette disposition de non-autorisation préalable n'affecte pas les régimes d'accréditation volontaire, notamment pour les prestataires de services de signature électronique et de certification.

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,

---

1 Version consolidée JO No C 027 du 26 janvier 1998, pp. 34-46.

2 „Directive sur le commerce électronique", doc. No 14263 ECO 419 CONSOM 80 CODEC 826.

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.

L'idée est reprise de l'article 5 de la future position commune pour l'adoption de la directive „commerce électronique" qui crée une obligation générale de transparence à la charge des prestataires de services de la société de l'information, quelle que soit leur activité dès l'instant qu'il s'agit d'une activité de la société de l'information. Elle ne fait pas double emploi avec les dispositions reprises dans le chapitre sur la conclusion des contrats électroniques dans la mesure où elle vise tous les sites web même si l'installation de ces sites ne conduit pas à des propositions transactionnelles en ligne. Elle permet à l'internaute et à l'administration de connaître qui se cache derrière un site web.

Nous avons adopté la terminologie „numéro d'identification à la TVA" car cette dernière est reprise à la fois dans la 6ème directive TVA et dans la loi luxembourgeoise TVA du 12 février 1979.

§ 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.

Cette disposition est directement inspirée de l'article 5 § 2 de la future position commune sur le commerce électronique[1]. Elle marque une volonté de transparence tarifaire afin de protéger les destinataires de services et plus particulièrement les consommateurs.

Par ailleurs, il est très important pour le consommateur de savoir si le prix indiqué par le prestataire établi au Luxembourg inclut ou pas les taxes luxembourgeoises ou étrangères, en l'occurrence la TVA, ainsi que les frais additionnels.

*

TITRE II

DE LA PREUVE ET DE LA SIGNATURE ELECTRONIQUE

Chapitre I. – *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."

La doctrine française et belge, aussi bien que les études menées dans ces deux pays en vue de l'adaptation de leur législation aux besoins de la société de l'information sont unanimes à reconnaître que l'admission de nouvelles formes de signatures à côté de la signature manuscrite passe par une définition de la signature.

Les suggestions faites ci-dessus s'inspirent directement de ces travaux afin que notre régime probatoire reste, sur cette question fondamentale, en concordance étroite avec celui en vigueur en France et en Belgique.

N'ayant fait l'objet que de retouches mineures depuis 1804, les dispositions consacrées par les codes civils luxembourgeois, français et belge à la preuve des actes juridiques (chapitre VI du titre III du livre

---

1 DOC. 14263/99, ECO 419, CONSOM 80, CODEC 826.

troisième du code civil) demeurent aujourd'hui, pour l'essentiel, identiques. Le juriste luxembourgeois y trouve l'immense avantage de pouvoir se référer non seulement à la jurisprudence abondante des tribunaux français et belge mais aussi aux travaux et opinions de la doctrine universitaire de ces deux pays.

L'approche préconisée dans la présente étude consiste dès lors à se rattacher le plus étroitement possible aux solutions qui se dessinent sur ce point en France et en Belgique.

Il est prévu dans le projet de loi français portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique déposé au Sénat le 1er septembre[1], d'introduire dans le code civil une définition de la signature (après l'article 1322-1 du code civil, il est inséré un article 1322-2). Le projet de nouvel article 1322-2 du code civil est ainsi rédigé: „la signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son consentement aux obligations qui découlent de l'acte."

Un consensus s'est formé en France et en Belgique qu'il convient de ne lier la définition de la signature ni au mode d'expression de la signature, ni à son support. Celle-ci doit être caractérisée à travers ses deux fonctions essentielles: l'identification du signataire et son adhésion au contenu de l'acte. Mise en évidence depuis longtemps par la doctrine et la jurisprudence, la double fonction d'identification et de validation de l'acte apparaît, en effet, comme la qualité indispensable de toute signature.

L'absence de toute référence aux possibles formes que celles-ci peut revêtir, permet d'ouvrir le concept aux procédés d'authentification et d'identification les plus divers offerts par les nouvelles technologies (signatures digitales, biométriques …). Elle évite aussi l'imprécision et partant de là, l'insécurité inhérente à toute définition matérielle de la signature, telle qu'elle avait été envisagée lors de la réforme de 1986.

Le deuxième alinéa de l'article précise que la signature manuscrite n'est plus la seule forme de signature admissible. Le dernier alinéa entend répondre à un risque lié spécifiquement à sa dématérialisation, celui de voir l'acte auquel elle se rapporte modifié en dehors du consentement du signataire. Ainsi, la signature électronique n'est reconnue que si elle remplit la condition supplémentaire d'être liée de façon indissociable à l'acte et d'en garantir l'intégrité.

Observons enfin que la définition retenue de la signature électronique ne paraît pas impliquer de modifications des articles 1323 et 1324 du code civil alors que certaines retouches aux articles 289 et s. du Nouveau Code de Procédure civile (anciens articles 193 et s.) semblent utiles. Voir ci-après.

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."

a) Nouvelle conception de l'originalité

L'article 1322-2 concerne la notion d'original. Celle-ci reçoit une description fonctionnelle. Classiquement, la distinction original-copie s'appuie sur une différenciation relative à la nature du support. A cette différenciation correspond un traitement juridique différent. L'information contenue sur le support original se voit reconnaître une force probante supérieure à celle apparaissant sur la copie.

L'avènement de l'informatique remet en question la notion même de support, du moins de support matériel. Il n'en reste pas moins que la notion d'originalité d'un document reste primordiale. Cette originalité ne se ramène pas, comme par le passé, à une absence de modification du support, mais cette originalité découle de ce que l'intégrité d'une information puisse être établie de son origine à nos jours.

L'article 8 de la loi type de la CNUDCI sur le commerce électronique préconise cette approche en disposant qu'il est satisfait à l'exigence de forme originale s'il existe une garantie fiable quant à l'intégrité de l'information, à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre. De la sorte on adopte une vue élargie de l'originalité (par opposition à une vision qui ramenait la question de l'originalité à la nature du support). Cette approche permet de rendre compte de ce que la technique informatique autorise la reproduction d'un document tout en assurant l'originalité de l'information contenue. Tel est le cas par exemple pour la technique de signature digitale qui permet de figer le document et d'assurer ainsi son intégrité.

En dehors de l'hypothèse du maintien de l'originalité du document électronique par la maîtrise et la garantie de l'intégrité du document, on aurait uniquement à faire à des copies, reproductions auxquelles l'article 1334 actuel associe une moindre force probante. La copie rend compte d'un document original mais sans que l'intégrité de l'information originale puisse être contrôlée. Si toutefois ces

1 Projet adopté par le Sénat le 8 février et accessible sur le site du Sénat français: http://www-senat.fr/leg/pjl98-488.html.

copies ont été effectuées dans le respect des conditions fixées par le règlement grand-ducal de 1986, alors une force probante égale à celle de l'original peut leur être reconnue.

b) Nouvelle problématique posée par l'archivage d'un document électronique signé digitalement

Un problème nouveau apparaît en ce qui concerne l'archivage d'un document électronique signé digitalement. En effet, la paire de clés utilisée pour signer un document par la technique du cryptage et le certificat émis par un prestataire de service de certification (Cf. infra chapitre II relatif aux prestataires de service de certification) n'a qu'une „durée de vie" limitée. Après une certaine période, on considère que cette paire de clés n'a plus un niveau de sécurité suffisant car le risque de découvrir la clé privée au départ de la clé publique augmente. L'utilisateur devra donc recréer une nouvelle paire de clés et un nouveau certificat pour signer les messages antérieurs et les nouveaux messages. Dès lors que l'on signe à nouveau un message antérieurement signé, il est indispensable que celui-ci garde la même valeur juridique que le message initialement signé. Cela ne semble pas poser de problème s'il s'agit des mêmes parties qui signent une nouvelle fois. Mais on peut également imaginer que les parties confient à un tiers de confiance (un prestataire de service de certification ou une autre entité) la tâche de signer lui-même le document tout en maintenant à celui-ci une valeur identique. C'est le problème de l'archivage électronique, qui dépasse certainement notre propos, mais mériterait qu'on s'y intéresse par la suite.

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".

Modifications suggérées aux dispositions du N.C.P.C. relatives à la procédure de vérification des écritures:

A la lecture des articles 289 et s. du Nouveau Code de Procédure Civile (anciens articles 193 et s. du code de procédure civile), il semble que la procédure telle qu'elle est décrite peut s'appliquer, sans difficulté, à la signature électronique, sous réserve de quelques légères modifications.

A l'article 291, le terme „vérification" peut rester. En effet, on peut vérifier tant une signature manuscrite qu'électronique, l'idée étant de vérifier si la signature émane ou pas de la personne qui la dénie. Sans doute, la vérification s'opérera de manière différente de celle utilisée pour la signature manuscrite. Le juge se référera non à un graphologue mais à un spécialiste en cryptographie ou a un audit de sécurité pour mesurer notamment la robustesse des clés ou détecter des manipulations informatiques.

A l'article 292, les mots „pièce à vérifier" ne doivent pas être modifiés. La pièce peut viser à la fois un document papier signé de manière manuscrite et un document électronique signé électroniquement (un fichier qui peut être stocké sur une disquette par exemple).

En revanche, les mots „signée et paraphée" posent problème. Le verbe „signer" peut être interprété largement, surtout avec la nouvelle définition de la signature, et viser tant la signature manuscrite que la signature électronique. Par contre, le paraphe s'envisage plus dans l'environnement papier. Il a essentiellement pour vocation d'être apposé sur toutes les pages (papier) dans le but d'assurer l'intégrité du document sans contraindre le signataire à signer chacune de ces pages, la signature n'étant apposée que sur la dernière page. Dans l'environnement électronique, ce paraphe n'est pas nécessaire puisque la fonction d'intégrité est assurée par la signature électronique elle-même, qui porte par définition sur tout le document. Aussi est-il proposé d'ajouter les mots suivants en italique „signée et, en cas de signature manuscrite, paraphée …".

Aux articles 296, 297 et 298, les mots „pièces de comparaison" peuvent rester. La pièce de comparaison peut être un document signé de manière manuscrite mais aussi un document signé électroniquement.

A l'article 302, les mots „corps d'écritures" peuvent s'interpréter largement. On peut défendre qu'il s'agit de tous les éléments jugés utiles par les experts pour effectuer leur travail de vérification, éléments qui peuvent varier suivant que l'on est dans l'environnement papier ou électronique.

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."

Par nature, les actes sous seing privé électronique peuvent être établis et conservés en plusieurs exemplaires originaux. Il a donc paru utile d'écarter à leur propos l'obligation de les dresser en un nombre d'exemplaires déterminé et surtout celle de devoir indiquer sur chacun d'eux le nombre exact d'originaux.

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."

Afin de permettre qu'un engagement unilatéral puisse être pris tant sous forme papier que sous forme électronique, il est suggéré pour les derniers une protection équivalente à celle résultant de la mention manuscrite de la somme de l'engagement. L'apposition d'une signature distincte sur l'indication du montant de l'engagement, qui suppose d'appliquer spécifiquement le dispositif de création de signature à ce montant, devrait retenir suffisamment l'attention du signataire afin de lui éviter de s'obliger de façon inconsciente ou irréfléchie.

Par ailleurs, suivant une recommandation faite par la Cour Supérieure de Justice dans son avis du 5 juillet 1985, une légère correction est proposée dans la rédaction de l'article 1326 pour faire apparaître, sans ambiguïté, que la partie de phrase „en toutes lettres" se rapporte non seulement à la quantité mais aussi à la somme.

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."

Le présent paragraphe, déjà abrogé depuis la loi du 22 décembre 1986, contient deux articles nouveaux. Le premier est relatif à la valeur des copies, lorsque le titre original subsiste (nouvel article 1333 reprenant le contenu de l'article 1334 actuel); le second a trait à la valeur des copies lorsque le titre original n'existe plus (nouvel article 1334 reprenant le contenu de l'article 1348, alinéa 2 actuel).

Le nouveau paragraphe ne contient aucune disposition novatrice, mais, de par son contenu, permet de traiter de la problématique des copies de façon plus systématique. En effet, l'article 1348, alinéa 2 traitant de la valeur des copies lorsque l'original n'existe plus, a davantage sa raison d'être sous la section 1 consacrée à la preuve littérale , et plus spécifiquement sous un paragraphe consacré aux copies, que sous la section 2 relative à la preuve testimoniale. Par ailleurs, mieux vaut traiter de la problématique des copies par le biais de principes généraux plutôt que par le biais d'exceptions (tel que c'est actuellement le cas pour l'article 1348, alinéa 2).

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."

Le nouvel article 1333 du Code civil reprend les termes de l'article 1334 actuel du Code civil. Celui-ci prévoit que „les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée".

De par sa situation dans le Code civil (sous le paragraphe consacré aux copies d'actes sous seing privé), il ne peut être contesté que cette disposition concerne uniquement les actes sous seing privé.

Une modification, sous forme de rajout, a cependant été apportée à cette disposition, afin de l'étendre expressément aux actes faisant foi d'original au sens de l'article 1322-2.

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 un règlement grand-ducal."

Le contenu de l'article 1334 actuel est repris à l'article 1333. Il est remplacé par celui de l'article 1348, alinéa 2 actuel, relatif aux copies d'actes sous seing privé avec destruction de l'original. Cette disposition doit en effet trouver sa place parmi celles consacrées aux copies plutôt que comme une exception au principe de l'article 1341 du Code civil.

Cette disposition complète la précédente. Elle est relative aux copies qui ont été réalisées selon les conditions fixées par règlement grand-ducal et dont l'original n'existe plus.

Le contenu de l'article 1348, alinéa 2 a été légèrement remanié. Il ne traite plus seulement des reproductions micrographiques et des enregistrements informatiques, mais bien des copies en général. Une telle modification est justifiée pour les raisons suivantes:

- *il est préférable de ne pas faire état dans le Code civil de techniques spécifiques qui risquent de devenir rapidement obsolètes.*
- *l'article 1334 deviendrait ainsi le pendant de l'article 1333: tous deux seraient relatifs aux copies, l'un avec destruction de l'original, l'autre avec conservation de l'original.*

– *un tel amendement ne fait pas obstacle à l'application du règlement grand-ducal existant (s'il est préférable de ne pas parler de techniques particulières dans le Code civil, rien n'empêche d'en faire état dans un règlement).*
– *enfin, il fait écho au fait que ce sont les copies qui doivent être réalisées dans le cadre d'une méthode de gestion régulièrement suivie (et non les originaux qui doivent être détruits dans le cadre d'une telle méthode).*

Il conviendrait de modifier le règlement grand-ducal pris en application de l'article 1348, alinéa 2 actuel. L'article 1 devrait faire écho à la modification du Code civil.

* *article 1, a) Les copies visées à l'article 1334 du Code civil …*
* *„… est réputée durable toute reproduction indélébile du document original et tout enregistrement qui entraîne une modification irréversible du support" pour qu'ainsi cette phrase n'entre pas en contradiction avec l'approche fonctionnelle de la notion d'original (voir article 7 du présent projet de loi).*

Art. 14.– L'Article 1348, alinéa 2 du Code civil est supprimé.

Puisque son contenu est repris par le présent avant-projet de loi à l'article 1334 du Code civil, il convient de supprimer l'alinéa 2 de l'article 1348 du Code civil.

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."

L'article 11 du code de commerce tel que formulé n'est guère satisfaisant. Il doit être modifié de façon à traiter des copies en général et non plus seulement de la conservation en micrographie ou sur support informatique.

Par ailleurs l'article 11 tel que formulé actuellement exige notamment que les reproductions ou enregistrements correspondent au contenu et qu'ils soient disponibles, ce qui est une évidence, surtout à la lecture du règlement grand-ducal auquel l'article 11 fait référence.

Enfin, l'article 11 dispose que les reproductions et enregistrements doivent être disponibles sous une forme „directement lisible". Cette expression est source d'ambiguïté dans le contexte électronique.

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.

Concernant la perception et le contrôle des impôts et taxes dus d'après la législation fiscale en vigueur, et la lutte contre la fraude fiscale en particulier, les administrations compétentes doivent avoir la possibilité de vérifier sur support papier les détails d'une transaction commerciale, même si elle est effectuée sous forme électronique. En plus, les principes de neutralité et de l'équité fiscale, confirmées dernièrement par l'OCDE et l'UE en matière de commerce électronique, exigent que des transactions fonctionnellement équivalentes soient imposées et contrôlées de la même façon, quel que soit le support des données transmises. Ainsi, bien que les techniques cryptographiques, qui sont destinées à garantir l'authentification des parties, l'intégrité, la non-répudiation, de même que la confidentialité des messages, ont l'avantage, d'un côté, d'assurer la confiance des consommateurs et commerçants dans les transactions numériques, elles peuvent, d'un autre côté, faire obstacle à la vérification par les services fiscaux de l'exacte perception de la taxe ou de l'impôt dû.

Finalement, les administrations établiront des règles techniques normatives permettant d'éviter que, sur le plan du contrôle des pièces à transmettre par les contribuables en vertu d'obligations légales existantes, les administrations fiscales ne soient techniquement dans l'impossibilité de remplir leur mission.

Chapitre II. – *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.

Cette définition, directement issue de la directive du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, nous semble plus précise que celle adoptée lors du précédent projet de loi No 4554 puisqu'elle parle de détention du dispositif de création de signature. La notion de signataire a été définie dans le but de préciser qu'une signature peut émaner tant d'une personne physique que d'une personne morale.

„*Dispositif de création de signature*“, un dispositif qui satisfait aux exigences définies au règlement grand-ducal relatif au certificat qualifié.

Nous renvoyons à un règlement grand-ducal afin de rester technologiquement neutre sinon nous réduirions la portée de la loi à la signature digitale et nous ne couvririons pas les évolutions technologiques.

„*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 de l'article 25 de la présente loi.

Conformément à la directive sur un cadre communautaire pour les signatures électroniques, un certificat n'est considéré comme „qualifié“ qu'à la condition, d'une part, qu'il ait été émis dans des conditions sûres et, d'autre part, qu'il contienne un minimum d'informations.

Le terme qualifié est préféré à celui d'agréé car ce dernier renvoie à des procédures d'approbation qui ne sont pas visées ici.

„*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.

Ce terme est repris de la directive sur les signatures électroniques.

Le prestataire de service de certification, ayant pour mission la création, la délivrance et la gestion de certificats peut aussi bien être une personne physique que morale. A sa demande le prestataire de service de certification crée un certificat. Une fois ce certificat créé, il le délivre à la personne qui en a fait la demande et l'inscrit, après consentement du titulaire, dans le registre électronique créé à cet effet. En cas de nécessité, il procède à sa suspension ou à sa révocation. Le prestataire de service de certification n'est pas tenu d'assurer seul toutes les étapes du processus de certification. En effet, il peut se référer, pour la collecte des informations, aux renseignements détenus par les autorités d'enregistrement. Toutefois, il répond, à l'égard des utilisateurs des certificats, du dommage qui est la conséquence des obligations qui lui sont imposées par ou en vertu de la présente loi et des règlements grand-ducaux.

La fonction du prestataire de service de certification n'est pas limitée à la délivrance et à la gestion des certificats; il couvre également d'autres services connexes à l'utilisation des signatures électroniques (horodatage, archivage, etc.).

„*Titulaire de certificat*“, toute personne, physique ou morale, à laquelle un prestataire de service de certification a délivré un certificat.

Le titulaire de certificat est la personne identifiée dans le certificat, ce qui n'implique nullement que le certificat doit reprendre l'identité véritable de son titulaire. Celui-ci peut en effet demander à apparaître sur le certificat sous un pseudonyme afin que soit garanti l'anonymat. Soulignons en outre que toute personne peut faire certifier plusieurs dispositifs de vérification de signature et devenir ainsi titulaire de plusieurs certificats.

La notion de titulaire de certificat est distincte de la notion de détenteur du dispositif de création de signature, qui est une notion plus matérielle. En effet le dispositif de création de signature sera souvent stocké sur un support matériel telle qu'une carte à puce. Or le titulaire du certificat peut être mais ne sera pas toujours détenteur du dispositif de création de signature. Par exemple une personne morale est titulaire de certificat mais ne sera pas détentrice du dispositif de création de signature car n'existant pas

matériellement, elle n'est pas capable de détenir ce dispositif (cette carte à puce). Une personne physique (habilitée à représenter la société) sera donc nécessairement détentrice du dispositif de création de signature.

Le concept se trouve défini, à côté de celui de „signataire" dans la mesure où le titulaire assume en cette seule qualité certaines obligations. Le signataire est, quant à lui détenteur du dispositif de création de signature.

„*Accréditation*", procédure par laquelle un organisme faisant autorité reconnaît formellement qu'un organisme ou un individu est compétent pour effectuer des tâches spécifiques.

Définition d'après la norme EN 45020, in Normalisation et activités connexes, vocabulaire général, février 1998, „Guide ISO/CEI 2: 1996".

La directive relative à un cadre communautaire pour les signatures électroniques définit l'accréditation volontaire or cela ne nous semble pas nécessaire de reprendre cette définition puisque nous précisons plus loin dans le texte que l'accréditation est volontaire ou plutôt le système d'accréditation est volontaire.

„*Système d'accréditation*" système ayant des propres règles de procédure et de gestion et destiné à procéder à l'accréditation.

Définition d'après le „Guide ISO/CEI 2: 1996".

„*L'Autorité Nationale d'Accréditation et de Surveillance*", est le Ministère de l'Economie qui dirige et gère un système d'accréditation et qui prononce l'accréditation.

Un projet est en cours d'élaboration sur l'accréditation.

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.

L'article 18 précise les effets juridiques des signatures électroniques en se référant à la nouvelle rédaction de l'article 1322-1 du Code civil. L'objectif de la disposition est d'établir un lien entre, d'une part, la réforme des règles du Code civil relatives à la preuve, et plus précisément l'introduction de la définition ouverte et fonctionnelle du concept de signature et, d'autre part, les principes édictés au présent chapitre.

Deux hypothèses méritent d'être envisagées:

- *Si la signature employée a été créée par un dispositif sécurisé de création de signature que le signataire puisse garder sous son contrôle exclusif et qu'elle est combinée à un certificat qualifié, émis par un prestataire de service de certification, elle a une force probante équivalente à une signature manuscrite au sens de l'article 1322-1 du code civil. Cela se justifie eu égard au niveau de sécurité requis.*
- *Si, en revanche, la signature électronique ne satisfait pas aux exigences du § 1 de l'article 18 de la présente loi, la directive sur les signatures électroniques contient une clause de non-discrimination à l'article 5 § 2 que nous avons repris dans le § 2 de l'article 18.*

Comme le précise toutefois le § 2, elle ne saurait être rejetée par le juge pour cette seule raison (cf. article 5 § 2 de la directive sur un cadre communautaire pour les signatures électroniques). Il appartiendra à la personne qui s'en prévaut d'apporter la preuve de la fiabilité de la technique utilisée afin d'établir que la signature répond aux critères posés par l'article 1322-1 du Code civil. Ainsi, l'acte auquel elle est attachée servira de commencement de preuve par écrit ou d'indice.

L'approche fonctionnelle de la signature préconisée à l'article 1322-1 du Code civil permet de la sorte une très large reconnaissance des signatures électroniques.

Le dispositif sécurisé et le certificat qualifié sont définis à l'article 17 du projet de loi qui renvoie à des règlements grand-ducaux afin de garder la neutralité technique dans le corps du texte.

Précisons aussi que le recours à un prestataire accrédité n'a aucune incidence juridique, en effet, la signature électronique possède des effets juridiques si elle est dotée d'un certificat qualifié qu'il provienne d'un prestataire accrédité ou pas.

Section 2. Des prestataires de service de certification

Sous-Section 1. Des prestataires de service de certification

Il s'agit ici des prestataires qui n'émettent pas des certificats qualifiés, ces derniers sont soumis, en vertu de la directive à certaines obligations moins nombreuses que les prestataires émettant des certificats qualifiés. Quant à la responsabilité, la directive ne prévoit un régime de responsabilité spécifique que pour les prestataires émettant des certificats qualifiés (article 6). Cette sous-section contient des obligations auxquelles sont soumis tous les prestataires, qu'ils émettent ou non des certificats qualifiés, qu'ils soient ou non accrédités. En tout état de cause, les prestataires n'émettant pas de certificats qualifiés sont, pour le reste, soumis au droit commun.

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 réviseurs et experts 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.

La rédaction de cette disposition est directement inspirée de l'article 41 de la loi modifiée du 5 avril 1993 relative au secteur financier. Le § 1 impose aux prestataires de service de certification une obligation de secret concernant les informations qui leur sont transmises dans le cadre de l'exercice de leurs activités. Cette obligation vise essentiellement le respect de l'anonymat lorsque le titulaire d'un certificat utilise un pseudonyme. (Ce secret professionnel est d'ordre public.

Le § 2 pose comme limite à l'obligation de secret les révélations autorisées ou imposées par ou en vertu d'une loi, qu'elle soit antérieure ou postérieure au présent texte. Toute violation est sanctionnée par l'article 458 du Code pénal.

Le § 3 énonce le principe selon lequel il n'existe pas d'obligation de secret à l'égard de l'Autorité Nationale d'Accréditation et de Surveillance, laquelle doit être en mesure d'assurer la surveillance des prestataires de service de certification placés sous son contrôle. (Mais attention ce principe ne serait valable qu'à l'égard des prestataires accrédités.)

Le § 4 impose la même obligation de secret professionnel à l'Autorité Nationale d'Accréditation et de Surveillance ainsi qu'aux personnes liées à elle et qui pourraient être amenées à connaître des informations confidentielles dans le cadre de leurs activités.

Le § 5 pose une limite générale à toute utilisation non autorisée de renseignements confidentiels qui ont pu être révélés.

Le § 6 protège celui qui aura révélé de bonne foi et en vertu d'une disposition légale un renseignement confidentiel contre d'éventuelles actions en responsabilité civile.

Pour le surplus, l'interprétation de la disposition pourra se référer utilement à celle de l'article 41 de la loi du 5 avril 1993 relative au secteur financier.

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, et dans les cas prévus à l'article 19 § 2.

Le § 1 vise à assurer qu'en matière de signature électronique, l'autorité nationale d'accréditation et les prestataires de service de certification satisfont aux exigences de la directive 95/46, directive-cadre en matière de protection des données personnelles.

Cet article est directement inspiré de l'article 8 de la directive sur les signatures électroniques. La collecte d'informations nécessaire à la constitution du certificat ne peut se faire que directement auprès de la personne qui a introduit une demande de certificat et uniquement dans la mesure où cela est nécessaire à la délivrance du certificat. Moyennant le consentement du candidat titulaire, la collecte d'informations peut en outre avoir lieu auprès de tiers et notamment d'une autorité d'enregistrement, telle que l'ordre des avocats, des médecins, etc. Enfin, les données à caractère personnel ne peuvent, sauf consentement du titulaire, être utilisées par les prestataires de service de certification que dans le cadre de leurs activités de certification.

Le titulaire ne désirant pas que son nom apparaisse sur le certificat peut choisir un pseudonyme. Cette disposition s'inspire également de la directive sur les signatures électroniques. Les effets juridiques donnés aux pseudonymes relèvent de la législation nationale.

Il convient toutefois de souligner que, bien que l'anonymat soit garanti, le signataire est identifié auprès du prestataire de service de certification. La véritable identité du titulaire ne pourra être révélée par le prestataire de service de certification que si le titulaire a marqué son consentement et que cette révélation est autorisée ou imposée en vertu des dispositions du code pénal et du code d'instruction criminelle.

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 du dispositif de création de signature qu'il utilise. Toute utilisation de celui-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 du dispositif de création de signature ou de perte de la conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire suspendre, voire de révoquer immédiatement le certificat conformément aux articles 26 et 27 de la présente loi.

§ 4. Lorsqu'un certificat est arrivé à échéance, a été suspendu ou 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.

Le titulaire doit assurer la confidentialité et l'intégrité de son dispositif de création de signature.

Lorsque la signature a pu être authentifiée par un certificat, le message assorti de cette signature est réputé émaner de son titulaire.

Le prestataire de service de certification étant responsable des informations qu'il aura certifié, le titulaire est tenu de lui signaler toute modification de ces informations.

Pour de multiples raisons, il pourrait se faire que la confidentialité du dispositif de création de signature soit compromise ou que le titulaire de certificat craigne qu'il en soit ainsi.

Deux procédures, l'une de suspension (article 26), l'autre de révocation (article 27), sont prévues par la présente loi afin de parer à cette éventualité. Le titulaire du certificat doit les mettre en œuvre au moindre doute relatif au maintien de la confidentialité du dispositif. Les procédures de suspension ou de révocation sont également applicables dans l'hypothèse où l'une des mentions certifiées ne serait plus conforme à la réalité.

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

La directive relative à un cadre communautaire pour les signatures électroniques prévoit de nombreuses obligations à la charge des prestataires émettant des certificats qualifiés (annexe II).

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.

Dans la perspective de promouvoir la confiance nécessaire à l'utilisation des signatures électroniques il est prévu de mettre à la charge de tous les prestataires de service de certification une obligation d'information portant sur:

- *la procédure à suivre pour produire et vérifier une signature électronique.*
- *la nécessité de signer au moyen d'un nouveau dispositif de création de signature les messages de données signés électroniquement avant que la durée du certificat ne soit écoulée. Dans le cadre de la cryptographie asymétrique, la paire de clés et le certificat n'ont qu'une „durée de vie" limitée. Après une certaine période, on considère que cette paire de clés n'a plus un niveau de sécurité suffisant car le risque de découvrir la clé privée à partir de la clé publique augmente. L'utilisateur devra donc se doter d'une nouvelle paire de clés et se voir attribuer un nouveau certificat pour signer les messages antérieurs et les nouveaux messages.*
- *les obligations qui pèsent sur le prestataire de service de certification (obligation de vérification des informations avant d'émettre un certificat, obligation de délivrer un certificat avec un contenu minimum, obligation de tenir un registre électronique, obligation de protéger la confidentialité et d'utiliser des moyens techniques fiables et sûrs lorsqu'elle génère des dispositifs de création et de vérification de signature, règles relatives à la suspension et à la révocation des certificats, dispositions relatives à la vie privée, régime de responsabilité, …).*
- *les obligations qui pèsent sur le titulaire de certificat (obligation de garder secret le dispositif de création de signature, pleine responsabilité de l'utilisation de celui-ci, obligation de demander la suspension ou révocation en cas de perte de la confidentialité ou perte de la conformité à la réalité des informations contenues dans le certificat, …) et sur le destinataire du message signé électroniquement (obligation de vérifier la signature électronique, de consulter le registre électronique de certificats, confiance).*
- *Quand au d) du § 1, il paraît nécessaire de préciser au titulaire du certificat que ce dernier a été délivré par un prestataire accrédité car même si cela n'a pas d'effet juridique, il s'agit d'un label de qualité qui pourra jouer sur le marché.*

– *les conditions contractuelles de délivrance d'un certificat, y compris les limites éventuelles de responsabilité du prestataire de service de certification.*

– *les procédures de réclamation et de règlement des litiges.*

Le paragraphe 2 provient du k) de l'annexe II de la directive sur les signatures électroniques. Elle étend l'obligation d'information aux tiers sous réserve de l'acceptation du titulaire du certificat. Nous l'avons réadapté en effet, l'information aux tiers est faite par inscription du certificat dans l'annuaire électronique prévu dans un règlement grand-ducal.

Art. 23.– § 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.

Le prestataire de service de certification fournit un exemplaire du certificat au demandeur pour qu'il en vérifie le contenu et l'accepte. Une fois le certificat accepté le demandeur devient titulaire de certificat.

Le titulaire est invité par ailleurs à accepter la publication du certificat. Dans le souci du respect de l'anonymat, il peut s'opposer à cette publication. A défaut, le prestataire de service de certification inscrit le certificat dans un registre public accessible à tous les utilisateurs.

Le prestataire de service de certification a l'obligation de conserver un annuaire électronique. Pour plus de détails se rapporter au règlement grand-ducal relatif aux exigences concernant les prestataires de service de certification délivrant des certificats qualifiés.

Art. 24.– ***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. Lorsque qu'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.

Le prestataire de service de certification atteste que toutes les informations visées dans le certificat qu'il délivre sont exactes. Le contenu du certificat qualifié est précisé dans un règlement grand-ducal.

Il est tenu de vérifier le lien entre le candidat titulaire et son dispositif de vérification de signature et de le confirmer. C'est l'existence et la véracité de ce lien qui constituent l'essence du certificat.

Si le certificat est délivré à une personne morale, le prestataire de service de certification, pour éviter les abus ou les fraudes, doit vérifier l'identité de la personne physique se présentant à lui et la validité de son pouvoir de représentation. Cependant, les informations relatives à l'identité et au pouvoir de représentation de la personne physique ne sont pas destinées à être inscrites sur le certificat.

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

§ 1. Seuls les prestataires de service de certification qui satisfont aux exigences de sécurité et de fiabilité déterminées par règlement grand-ducal peuvent émettre des certificats qualifiés.

§ 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 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.

Conformément à l'article 2 § 10 de la directive sur les signatures électroniques, un certificat ne peut être considéré comme un certificat qualifié qu'à condition, d'une part, qu'il soit émis par un prestataire de service de certification qui satisfait à certaines exigences (annexe II de la directive) et, d'autre part, qu'il comporte un contenu minimum (annexe I de la directive). Bien entendu ces annexes sont transposées dans des règlements grand-ducaux.

Conditions d'émission du certificat:

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 satisfait aux exigences arrêtées par voie de règlement grand-ducal (Cf. annexe II de la directive). Une signature électronique reposant sur un certificat qualifié émis par un prestataire de service de certification et un dispositif sécurisé de signature aura la même force probante qu'une signature manuscrite conformément à l'article 18 du projet, et ce en raison de l'environnement extrêmement sécurisé qui entoure sa création. Ceci ne veut pas dire qu'une signature électronique ne reposant pas sur un certificat qualifié émis par un prestataire de service de certification mais satisfaisant néanmoins aux exigences du règlement grand-ducal (Cf. annexe II de la directive) ne puisse pas bénéficier de cette reconnaissance juridique. Dans les deux cas il faudra prouver devant le juge que les conditions exigées dans l'article 18 sont réunies, de même il existe une procédure de vérification d'écriture pour la signature manuscrite.

L'ancien § 4 relatif à la signature électronique du prestataire de service de certification du certificat qualifiée a été supprimé, puisque cette condition figure dans un règlement grand-ducal avec les autres conditions relatives à un certificat qualifié. Tout ceci afin de demeurer cohérent.

Art. 26.– ***De la suspension des certificats***

§ 1. A la demande de son titulaire, le prestataire de service de certification suspend le certificat qualifié immédiatement. Il lève cette suspension dans les mêmes conditions.

§ 2. Le prestataire de service de certification suspend également le certificat qualifié lorsqu'il existe des raisons sérieuses pour admettre que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité, que la confidentialité des données afférentes à la création de signature a été violée, ou que le certificat a fait l'objet d'une utilisation frauduleuse.

§ 3. Le prestataire de service de certification informe le titulaire du certificat de la suspension en motivant sa décision.

La suspension doit être levée immédiatement lorsqu'un examen plus approfondi démontre le caractère correct de l'information ou la non-violation de la confidentialité du dispositif de création de signature.

Afin d'être fiable, la fonction de certification exige, outre la délivrance de certificats, la gestion de ceux-ci. Celle-ci suppose que le prestataire de service de certification procède à la suspension ou à la révocation du certificat dans les conditions et selon la procédure prévues par le présent projet.

La suspension vise à interrompre jusqu'à nouvel ordre l'usage d'un certificat. Elle empêche le titulaire d'utiliser le certificat et évite que les tiers puissent s'y fier.

La suspension est assurée par le prestataire de service de certification qui a délivré le certificat, soit à la demande de son titulaire, soit d'office.

Lorsqu'elle a lieu à la demande du titulaire, que cette demande soit ou non motivée, le prestataire de service de certification a l'obligation de procéder immédiatement à l'exécution de l'ordre de suspension. Il lève cette suspension dans les mêmes conditions.

Lorsque la suspension du certificat a lieu à l'initiative du prestataire de service de certification, celui-ci a l'obligation d'en avertir immédiatement le titulaire et de motiver sa décision. Elle ne peut avoir lieu que s'il existe des raisons sérieuses pour admettre soit que le certificat a été délivré sur la base d'informations erronées ou falsifiées, soit que les informations contenues dans le certificat ne sont plus conformes à réalité, soit que la confidentialité du dispositif de création de signature a été violée.

La suspension du certificat constitue une mesure transitoire et ne pourrait par conséquent constituer une étape ultime dans le processus de certification. C'est pourquoi, lorsqu'il a procédé d'office à la suspension d'un certificat, le prestataire de service de certification a l'obligation de procéder à un examen plus approfondi afin de déterminer s'il y a lieu de lever la suspension ou de procéder à la révocation du certificat conformément à l'article 27.

Art. 27.– ***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.

La révocation vise à mettre fin au certificat avant son terme. Elle est assurée par le prestataire de service de certification qui a délivré le certificat, soit à la demande de son titulaire, soit d'office.

Lorsqu'elle a lieu à la demande du titulaire, que cette demande soit ou non motivée, le prestataire de service de certification a l'obligation de procéder immédiatement à l'ordre de révocation.

Lorsque la révocation du certificat a lieu à l'initiative du prestataire de service de certification, celui-ci a l'obligation d'en avertir immédiatement le titulaire et de motiver sa décision. Elle ne peut avoir lieu que dans les conditions prévues au § 2.

Lorsque le certificat arrive à échéance, le prestataire de service de certification prévient le titulaire de l'échéance du certificat au moins un mois à l'avance.

La décision de révocation est définitive et donc irréversible.

La suspension et la révocation sont opposables au titulaire et aux tiers à partir de sa publication au registre. En effet, dès cette publication, le titulaire de certificat et le prestataire de service de certification pourront se prévaloir du fait que le certificat est suspendu ou révoqué vis-à-vis des tiers, et particulièrement du destinataire du message signé électroniquement qui est tenu de vérifier que le certificat n'est ni suspendu ni révoqué.

Lorsqu'il est appelé à suspendre ou à révoquer un certificat à la demande du titulaire, le prestataire de service doit procéder immédiatement à l'inscription de cette information sur le registre, en indiquant clairement que le certificat a fait l'objet de suspension ou de révocation. Notons que le terme „immédiatement" aura une valeur temporelle différente suivant qu'il s'agit d'une demande de suspension ou de révocation. En effet, avant de procéder à la suspension ou à la révocation, le prestataire de service de certification est tenu d'identifier la personne qui effectue la demande. Cette identification prendra un certain temps. Toutefois ce laps de temps doit nécessairement être extrêmement court en cas de demande de suspension. La suspension suppose que l'on veuille agir vite et bloquer rapidement le certificat afin d'éviter toute utilisation frauduleuse. Le prestataire de service de certification pourra donc se contenter de procéder à une identification succincte voire tout à fait superficielle. On estime, dans ce cas, que les inconvénients qui résulteraient de la non-suspension immédiate sont supérieurs à ceux qui découleraient d'une suspension demandée par une personne mal intentionnée qui se ferait passer pour le titulaire du certificat. Par contre, une demande de révocation a des conséquences plus graves qu'une demande de suspension, notamment de par le fait qu'une révocation ne peut être levée. Il est dès lors indispensable que le prestataire de service de certification identifie de manière certaine la personne qui effectue la demande de révocation pour s'assurer qui est le véritable titulaire du certificat, même si cette identification peut prendre du temps. Dans ce cas, il existe peu de risques car toute révocation peut être précédée d'une suspension.

Art. 28.– ***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;

– 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;

– 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 suspension ou 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.

§ 4.– Toute convention contraire aux dispositions du présent article est réputée non écrite.

Ces dispositions sont directement inspirées de la directive relative aux signatures électroniques du 13 décembre 1999.

Le prestataire de service de certification répond du dommage qui est la conséquence de l'inexécution des obligations qui lui sont imposées par ou en vertu de la présente loi et qui tendent toutes vers un même but: l'exactitude des informations certifiées; et vers une même fin: la sécurisation des échanges électroniques de données.

Au regard du degré de spécialisation technique que l'on est en droit d'attendre de tout prestataire de service de certification ainsi que de la confiance qu'un régime de certification est censé susciter, la responsabilité du prestataire est engagée dès lors que l'émission de certificats entraîne un dommage. Le régime mis en place est fondé sur la présomption simple de responsabilité du prestataire de service de certification. Celui-ci pourrait toutefois réfuter cette présomption en démontrant qu'il n'a commis aucune négligence, que la personne qui se fie au certificat est de mauvaise foi ou que le dommage résulte du non-respect des restrictions posées à l'utilisation du certificat pour autant que celles-ci soient indiquées dans le certificat. La responsabilité du prestataire de service de certification est également engagée lorsqu'il n'a pas suspendu ou révoqué un certificat alors qu'il aurait dû le faire en application des articles 26 et 27 de la présente loi.

Enfin, un prestataire de service de certification peut émettre des restrictions à l'utilisation d'un certificat pour autant qu'elles ne violent pas les dispositions de la présente loi. Il doit toutefois en informer les utilisateurs. Dans ce cas, le prestataire de service de certification ne pourrait être tenu responsable des dommages résultant de l'usage contre-indiqué d'un certificat.

Donc il est ici organisé un système de responsabilité à double détente, les prestataires voient leur responsabilité engagée mais il existe des limites liées au montant et à l'utilisation du certificat.

Cette responsabilité est engagée si la personne se fie „raisonnablement", ce qui signifie que certaines informations sont très difficiles à vérifier par le prestataire par exemple la qualité de signataire donc elles sont probablement sûres à 99%.

La bonne foi n'a pas besoin d'être précisée puisqu'elle est présumée.

Les données afférentes à la création de signature et les données afférentes à la vérification de signature sont définies dans un règlement grand-ducal.

Quant au paragraphe 4, il répute nulles les clauses contraires aux trois paragraphes précédents, c'est-à-dire qu'il évite, de la part des prestataires de service de certification des clauses d'exonération de responsabilité ou des clauses de limitation de responsabilité trop larges.

Art. 29.– ***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) si un prestataire de service de certification établi dans un Etat membre de l'Union européenne garantit ces certificats; ou

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.

Afin de revêtir une réelle utilité, toute infrastructure de certification adoptée à un niveau national doit être envisagée dans une perspective internationale. L'article 21 du projet, en traitant de la reconnaissance des certificats communautaires et des certificats de pays tiers, font écho à cette préoccupation. Ils sont directement inspirés de l'article 7 de la directive relative aux signatures électroniques.

De la reconnaissance des certificats étrangers: par cette disposition, le Grand-Duché de Luxembourg entend susciter la confiance des utilisateurs et ouvrir ses portes au commerce international.

Toutefois, les certificats émis par un prestataire de service de certification établi dans un pays tiers à l'Union européenne auront uniquement la même valeur que ceux délivrés par un prestataire de service de certification établi au Luxembourg, pour autant qu'ils répondent à une des trois conditions visées à l'article 21.

L'article 7 de la directive sur les signatures électroniques est étroitement liée à l'article 5 § 1 et § 2. En effet, l'art. 7 a) remplit les conditions de l'art. 5 § 1 donc la signature électronique possède les effets juridiques d'une signature manuscrite. Pour le b) il va de soi puisque l'article 5 § 2 établit un principe de non-discrimination.

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

Art. 30.– ***L'Autorité Nationale d'Accréditation et de Surveillance***

L'Autorité Nationale d'Accréditation et de Surveillance veille au respect par les prestataires de service de certification de la présente loi et des règlements qui s'imposent à eux.

Plus particulièrement, elle a pour missions:

– d'octroyer et de retirer les accréditations;
– de coordonner l'application cohérente et transparente des principes et procédures d'accréditation en application de la présente loi et des règlements.

L'Autorité Nationale d'Accréditation et de Surveillance exerce une mission de surveillance générale des prestataires de service de certification.

A cet effet, elle vérifie si un prestataire de service de certification non accrédité ne fait pas croire qu'il est accrédité. (Elle peut aussi, en cas de litige, être chargé comme expert de vérifier qu'un prestataire de service de certification non accrédité respecte les exigences de l'annexe II de la directive sur un cadre communautaire relatif aux signatures électroniques.) Elle vérifie également que les prestataires de service de certification accrédités se conforment aux conditions d'accréditation ainsi qu'aux dispositions stipulées par ou en vertu de la loi. Elle peut procéder à la suspension ou au retrait de l'accréditation si nécessaire.

Le Ministère de l'Economie est désigné comme Autorité Nationale d'Accréditation et de Surveillance.

Art. 31.– ***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.

Le § 1er consacre un principe de liberté, celui de se faire accréditer ou pas. Il peut ainsi coexister sur le marché des prestataires de service de certification accrédités et non accrédités.

Si un prestataire de service de certification désire obtenir une accréditation, il pourra introduire sa demande auprès de l'Autorité Nationale d'Accréditation et de Surveillance. L'accréditation ne sera accordée et maintenue que si le prestataire de service de certification répond aux conditions d'accréditation stipulées par ou en vertu de la loi (article 32), et appréciées par l'Autorité Nationale d'Accréditation et de Surveillance. Ces conditions ont pour objectif de garantir un ensemble d'impératifs de nature à accroître la confiance dans les prestataires de service de certification accrédités. L'Autorité Nationale d'Accréditation et de Surveillance exerce la surveillance du respect de ces conditions (Règlement grand-ducal concernant la procédure, la suspension et le retrait de l'accréditation).

Les §§ 2 et 3 consacrent le principe de la variabilité du contenu des accréditations. La loi donne la possibilité pour un prestataire de service de certification de demander une accréditation plus ou moins étendue en fonction des personnes auxquelles il souhaite délivrer des certificats.

Un prestataire de service de certification peut demander une accréditation large qui couvre la délivrance de certificats à la fois à des personnes physiques et morales (de droit privé ou de droit public) ou à certaines catégories de personnes seulement. Par exemple, un prestataire de service de certification peut se spécialiser dans la certification de la profession d'avocat ou de médecin: il sera donc qualifié pour certifier une personne physique ayant l'attribut d'avocat ou de médecin mais ne pourra pas se prévaloir de son statut pour les autres catégories de personnes physiques (notaire, architecte, …) ni pour les personnes morales. Toutefois, le prestataire de service de certification pourra délivrer un certificat à toute personne physique ne se prévalant d'aucun attribut particulier.

La variabilité du domaine des accréditations permet d'alléger les exigences requises à l'égard d'un prestataire de service de certification qui désire se spécialiser dans la certification d'un attribut précis. Admettre au contraire un système d'accréditation uniforme aurait pour conséquence d'obliger le prestataire de service de certification:

- *à mettre en place un système capable de délivrer des certificats à tout type de personne et tout type d'attribut c'est-à-dire un processus contraignant mais superflu de vérification des informations;*
- *à engager des coûts non négligeables pour obtenir une accréditation qu'il n'exploiterait que partiellement;*
- *à faire l'objet d'un audit plus astreignant que ce qui est nécessaire.*

Art. 32.– ***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.

L'article 28 fixe les conditions qui doivent impérativement être remplies par un prestataire de service de certification pour obtenir et conserver une accréditation.

Le § 1er renvoie à un règlement grand-ducal pour fixer les conditions de l'accréditation. Ce règlement est aussi visé au § 2. En répondant à ces conditions, un prestataire de service de certification démontre la crédibilité et la confiance que les utilisateurs peuvent avoir en lui.

S'agissant tout d'abord des garanties d'intégrité, de disponibilité et de sécurité, le prestataire de service de certification doit notamment utiliser un système informatique fiable. Cela implique que le prestataire de service de certification tienne un registre électronique accessible en permanence à toute personne et qu'il soit protégé contre toute modification non autorisée. En outre le prestataire de service de certification doit faire en sorte de protéger de manière adéquate la confidentialité de son dispositif de création de signature utilisé afin de signer les certificats qu'il émet. Il doit ensuite posséder l'expertise nécessaire pour assurer ses activités de certification. A cette fin, les employés du prestataire de service de certification doivent posséder des qualités professionnelles en matière de certification ou dans un domaine connexe. Ils doivent par ailleurs justifier de leur intégrité (absence de condamnation pour fraude, faux en écriture …). Le prestataire de service de certification doit utiliser des procédures et méthodes administratives et de gestion adaptées et conformes à des normes reconnues. Enfin, il doit offrir des garanties financières suffisantes pour exercer ses activités et, le cas échéant, indemniser les

utilisateurs ayant subi un dommage à la suite de l'inexécution des obligations qui lui sont imposées par ou en vertu de la loi. Pour ce faire, il souscrira utilement une assurance couvrant sa responsabilité professionnelle.

Le prestataire de service de certification doit se conformer aux exigences de fiabilité technique posées par l'Autorité Nationale d'Accréditation et de Surveillance ou par règlement grand-ducal. En effet, l'article 22 impose à tout prestataire de service de certification d'utiliser des moyens techniques fiables et sûrs.

Le règlement grand-ducal visé au § 2 fixe les modalités techniques relatives à la délivrance de l'accréditation et précise les conditions stipulées au § 1er. Il pourrait déterminer par ailleurs le niveau d'indépendance dont les prestataires de service de certification accrédités devraient bénéficier vis-à-vis des utilisateurs de leurs services.

Le § 3 vise à tirer profit de la possibilité offerte par l'article 3 § 7 de la directive sur les signatures électroniques qui dispose que „Les Etats membres peuvent soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires, et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. De telles exigences ne peuvent pas constituer un obstacle aux services transfrontières pour les citoyens".

Art. 33.– ***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 lesquels 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 28.

§ 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.

Les héritiers, tuteurs, curateurs et, le cas échéant, liquidateurs du prestataire de service de certification accrédité sont tenus des obligations posées par ou en vertu de la présente loi résultant de la cessation des activités du prestataire de service de certification accrédité.

Si un prestataire de service de certification met fin volontairement ou non à ses activités, il est tenu d'en avertir l'Autorité Nationale d'Accréditation et de Surveillance dans un délai raisonnable pour lui permettre de contrôler l'opération. En vue d'assurer la continuité du service, le prestataire de service de certification doit tout mettre en œuvre pour que ses activités soient reprises par un autre prestataire de service de certification accrédité conformément aux conditions fixées par le § 2. S'il ne trouve pas de repreneur, il procède à la révocation des certificats un mois après en avoir averti les titulaires et prend les mesures nécessaires pour que les données soient conservées.

Le § 4 énumère les cas principaux de cessation d'activité.

Art. 34.– ***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.

Puisque l'Administration est chargée de la surveillance des prestataires de service de certification accrédités, il convient de lui fournir les moyens d'agir dans les cas où elle constaterait l'irrespect des prescriptions de la loi.

Si l'Administration constate qu'un prestataire de service de certification accrédité ne se conforme pas aux prescriptions de la loi, elle peut fixer un délai pour régulariser, ce délai est fixé discrétionnairement par l'Administration en fonction du cas d'espèce. Elle peut éventuellement suspendre.

Par sécurité juridique, le prestataire de service de certification est tenu de mentionner immédiatement dans son annuaire le retrait de l'accréditation (sauf si le titulaire s'est opposé à cette publication) et d'en informer immédiatement les titulaires de certificat.

Sous-section 4. Du recommandé électronique

Art. 35.– 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.

Le recommandé déposé électroniquement offre à l'instar de celui déposé matériellement la possibilité pour l'expéditeur d'un message signé digitalement de se constituer une preuve de l'envoi, de la date et, le cas échéant, de la réception de ce message.

Dans le contexte des échanges électroniques de données, effectués en temps réel, il est nécessaire de prévoir, en outre, une certification de temps.

Preuve de l'envoi: l'intérêt qu'offre le recommandé est celui pour l'expéditeur de se ménager une preuve de son envoi. Cette preuve pourra être réalisée, pour le recommandé électronique grâce au récépissé électronique qui lui sera remis lors du dépôt électronique.

Preuve de la date et de l'heure de l'envoi: la loi impose, dans certains cas, un délai pour l'envoi d'une lettre ou d'un document. Tout comme pour la preuve de l'envoi, le recommandé offre à l'expéditeur la possibilité de se ménager la preuve que les délais ont été respectés.

Preuve de la réception: grâce au recommandé avec accusé de réception, l'expéditeur peut prouver que le destinataire a reçu l'envoi et a été en mesure d'en prendre connaissance.

L'expéditeur du document est responsable des moyens techniques à mettre en oeuvre pour garantir efficacement le contenu du message contre les risques d'atteinte à l'intégrité et à la confidentialité de celui-ci.

La signature digitale permet de garantir les messages contre les risques d'atteinte à son intégrité. Puisque cette fonction revêt une importance capitale dans le contexte électronique, il était nécessaire de faire de la signature digitale une condition de l'envoi recommandé. C'est la raison pour laquelle, cette disposition relative au recommandé électronique trouve sa place dans la présente loi.

*

TITRE III

DISPOSITIONS PENALES

Section 1. Des sanctions pénales

Art. 36.– 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 écritures électroniques,

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."

Un des objectifs du présent projet de loi est de conférer à la signature électronique la valeur juridique traditionnellement attachée à la signature manuscrite. A cet effet, sont proposées des modifications substantielles des articles 1322 et suivants du Code civil.

La signature électronique, définie dans le nouvel article 1322-1 du Code civil, revêt la même valeur que la signature manuscrite traditionnelle; dès lors, sa contrefaçon doit être sanctionnée de manière identique. A cet effet, il est proposé d'étendre le champ d'application de l'article 196 sur le faux en écritures aux „écritures électroniques".

Le texte actuel de l'article 196 vise, d'une façon générale, les écritures, même si, pour des raisons historiques évidentes, seul l'écrit traditionnel était à envisager.

Compte tenu de la formulation générale du texte, il suffit d'ajouter la précision que les écrits protégés peuvent également être de nature électronique. Apporter cette précision s'impose au regard de la concordance nécessaire des concepts entre le droit pénal et le droit civil dans cette matière.

L'article 441-1 du nouveau Code pénal français a opéré un élargissement identique du faux en visant „toute altération frauduleuse de la vérité … dans un écrit ou tout autre support d'expression de la volonté".

La formulation proposée dans le présent projet présente l'avantage de ne pas substituer aux termes anciens des dispositions nouvelles, de surcroît assez complexes, et de maintenir l'unité du concept d'écrit qui semble avoir été abandonnée dans le texte français.

Une modification de l'article 194 du Code pénal sur le faux en écritures publiques ne s'impose pas, les actes délivrés par les fonctionnaires ou officiers publics revêtant, pour l'heure, nécessairement une nature corporelle.

Art. 37.– 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."

Il s'agit d'une modification formelle qui consiste à remplacer les termes d'acte ou de pièce, qui pourraient suggérer un objet corporel, par le terme plus neutre de faux. Ce terme de faux est d'ailleurs utilisé dans le texte actuel en relation avec l'auteur de l'infraction.

Art. 38.– L'article 213 du code pénal est modifié comme suit:

„L'application des peines portées contre ceux qui auront fait usage des monnaies, effets, coupons, billets, sceaux, timbres, poinçons, marques, dépêches télégraphiques et écrits y compris électroniques contrefaits, fabriqués, falsifiés ou altérés, n'aura lieu qu'autant que ces personnes auront fait usage du faux, dans une intention frauduleuse ou à dessein de nuire."

Le terme écrit figurant dans cette disposition est complété par la précision que l'écrit peut être électronique.

Le terme de chose fausse est remplacé par celui de faux, objet de l'infraction.

Art. 39.– L'article 240 du code pénal est modifié comme suit:

„Sera puni de la réclusion de cinq à dix ans tout fonctionnaire ou officier public, toute personne chargée d'un service public, qui aura détourné des deniers publics ou privés, des effets en tenant lieu, des pièces, titres, actes, effets mobiliers ou biens incorporels qui étaient entre ses mains, soit en vertu, soit à raison de sa charge.

Si le détournement n'excède pas le cautionnement, le coupable sera puni d'un emprisonnement d'un mois à six mois."

Il s'agit de compléter le texte de l'article 240 en précisant que le détournement opéré par le fonctionnaire peut porter sur des biens incorporels.

Art. 40.– L'article 461 du code pénal est modifié comme suit:

„Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol.

Est également coupable de vol quiconque s'est frauduleusement rendu maître d'un bien incorporel qui ne lui appartient pas.

Est assimilé au vol, le fait de soustraire frauduleusement un véhicule automoteur ou un cycle appartenant à autrui en vue d'un usage momentané et avec l'intention de le restituer."

Pour les raisons plus amplement développées dans la partie générale de l'exposé des motifs, il est proposé de sanctionner l'atteinte aux biens incorporels qui, au regard de leur valeur économique, entrent dans le patrimoine de leur propriétaire.

Ainsi qu'il est expliqué ci-dessus, le terme de bien incorporel est repris de certains arrêts de la Cour de cassation française.

Au niveau de sa formulation, le nouveau deuxième alinéa, qu'il est proposé d'ajouter à l'article 461, reste le plus près possible de la terminologie et du style du 1er alinéa.

Par la formule introductive „Est également coupable de vol", il est précisé que la mainmise frauduleuse sur un bien incorporel d'autrui constitue un vol et n'est pas seulement assimilé à un vol au sens du nouveau troisième alinéa visant le vol d'usage.

Le nouveau deuxième alinéa s'écarte de la terminologie retenue pour le vol d'un objet corporel en ce qu'il omet toute référence à la „soustraction". Au terme de „soustraire", qui implique, selon une certaine doctrine, une exclusivité dans la possession „animo domini", est préféré celui de „se rendre maître" qui couvre le cas de figure où un bien est appréhendé par le voleur qui en obtient la disposition au même titre que le propriétaire légitime.

Art. 41.– L'article 467 du code pénal est modifié comme suit:

„Le vol sera puni de la réclusion de cinq à dix ans:

S'il a été commis à l'aide d'effraction, d'escalade ou de fausses clefs, y compris électroniques;

S'il a été commis par un fonctionnaire public à l'aide de ses fonctions;

Si les coupables, ou l'un d'eux, ont pris le titre ou les insignes d'un fonctionnaire public ou ont allégué un faux ordre de l'autorité publique."

L'informatique peut non seulement être l'objet, mais également l'instrument d'une infraction.

L'utilisation de fausses clés, qui constitue une circonstance aggravante du vol, doit être étendue aux clés électroniques.

Art. 42.– L'article 469 du code pénal est modifié comme suit:

„Est assimilé au vol commis à l'aide de violences ou de menaces le cas où le voleur surpris en flagrant délit, a exercé des violences ou fait des menaces, soit pour se maintenir en possession des objets soustraits ou des biens incorporels dont il s'est rendu maître, soit pour assurer sa fuite."

La modification de ce texte consiste dans l'ajout à la notion „d'objets soustraits" des termes de „biens incorporels dont il s'est rendu maître", en concordance avec la modification proposée pour l'article 461.

Art. 43.– L'article 470 du code pénal est modifié comme suit:

„Quiconque aura extorqué, par violences ou menaces, soit la remise de fonds, valeurs ou objets mobiliers, soit la signature ou la remise d'un écrit, d'un acte, d'une pièce quelconque contenant ou opérant obligation, disposition ou décharge ou d'un bien incorporel sera puni des peines portées aux articles 468, 471, 472, 473, 474 et 475, d'après les distinctions qui y sont établies.

Quiconque, à l'aide de la menace écrite ou verbale de révélations ou d'imputations calomnieuses ou diffamatoires, aura extorqué, soit la remise de fonds, valeurs ou objets mobiliers, soit la signature ou la remise des écrits énumérés ci-dessus, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000 francs à 1.200.000 francs.

La tentative de ce dernier délit sera punie d'un emprisonnement de six mois à trois ans et d'une amende de 10.001 à 400.000 francs."

L'objet de l'infraction d'extorsion doit, comme celui du vol, être étendu aux biens incorporels.

Art. 44.– L'article 471 du code pénal est modifié comme suit:

Le vol commis à l'aide de violences ou de menaces dans une maison habitée ou ses dépendances, sera puni de la réclusion de dix à quinze ans:

S'il a été commis avec effraction, escalade ou fausses clefs, y compris électroniques;

S'il a été commis par un fonctionnaire public à l'aide de ses fonctions;

Si les coupables, ou l'un d'eux, ont pris le titre ou les insignes d'un fonctionnaire public ou ont allégué un faux ordre de l'autorité publique;

S'il a été commis la nuit par deux ou plusieurs personnes;

Si des armes ont été employées ou montrées.

Il sera puni de la réclusion de quinze à vingt ans, s'il a été commis avec deux des circonstances précitées.

Art. 45.– 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. 46.– 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."

Dans la logique de la modification de l'article 467, il y a lieu de compléter les articles 471, 487 et 488 par une référence aux fausses clés électroniques.

Le deuxième alinéa de l'article 488 sanctionnant la fabrication de fausses clés par un serrurier est à supprimer. Cette circonstance aggravante a perdu toute raison d'être, au regard de l'évolution des techniques et des professions, et ne peut d'ailleurs pas s'appliquer à la contrefaçon de clés électroniques.

Art. 47.– L'article 491 du code pénal est modifié comme suit:

„Quiconque aura frauduleusement soit détourné, soit dissipé au préjudice d'autrui, des effets, deniers, marchandises, billets, quittances, écrits de toute nature contenant ou opérant obligation ou décharge ou des biens incorporels et qui lui avaient été remis à la condition de les rendre ou d'en faire un usage ou un emploi déterminé, sera puni d'un emprisonnement d'un mois à cinq ans et d'une amende de 10.001 francs à 200.000 francs.

Quiconque, dans une intention frauduleuse, se sera fait servir des boissons ou des aliments qu'il aura consommés sur place en tout ou en partie, ou se sera fait donner un logement dans les établissements à ce destinés, ou se sera fait transporter sur les voies publiques par un voiturier qui fait du transport de personnes sa profession, ou aura rempli ou fait remplir, à une station exploitée par un professionnel de la distribution, les réservoirs d'un véhicule ou d'autres réservoirs, en tout ou en partie, de carburants ou lubrifiants, et sans avoir payé le prix, sera puni d'un emprisonnement de huit jours à six mois et d'une amende de 10.001 francs à 200.000 francs. Les délits prévus au présent alinéa ne pourront être poursuivis que sur la plainte de la personne lésée. L'action publique sera éteinte par le paiement de la dette ou par le désistement de la partie plaignante.

Le coupable pourra, de plus, être condamné à l'interdiction, conformément à l'article 24."

Toujours dans la logique de l'adaptation des dispositions sur le vol, il y a lieu de prévoir que l'abus de confiance peut avoir pour objet un bien incorporel.

Art. 48.– L'article 496 du code pénal est modifié comme suit:

„Quiconque, dans le but de s'approprier une chose ou un bien incorporel appartenant à autrui, se sera fait remettre ou délivrer ou aura tenté de se faire remettre ou délivrer des fonds, meubles, obligations, quittances, décharges, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses pour persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, pour faire naître l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique, ou pour abuser autrement de la confiance ou de la crédulité, sera puni d'un emprisonnement d'un mois à cinq ans et d'une amende de 10.001 francs à 1.200.000 francs. Le coupable pourra de plus être condamné à l'interdiction, conformément à l'article 24."

Tout comme le vol, l'extorsion ou l'abus de confiance, l'escroquerie peut porter sur un bien incorporel.

Art. 49.– 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."

Les modifications proposées visent à sanctionner la tromperie sur la vente d'un bien incorporel.

A cet effet, il s'impose de remplacer le terme de „chose", figurant aux deuxième et troisième alinéas actuels du texte, par la notion plus large de bien et de préciser, au troisième alinéa, que le texte s'applique aux biens mobiliers, y compris les biens incorporels, et aux biens immobiliers.

En effet, dans la distinction opérée par le droit civil entre droits immobiliers et mobiliers, les biens incorporels relèvent en principe des droits mobiliers.

Art. 50.– 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."

Le vol, l'extorsion, l'abus de confiance ou l'escroquerie pouvant porter sur des biens incorporels, il y a lieu d'étendre, dans la même mesure, l'objet du recel.

Art. 51.– Le premier alinéa de 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 un an et d'une amende de 20.000 francs à 1.000.000 francs ou de l'une de ces deux peines."

L'article 509-1 ainsi que les articles 509-2 et 509-3 du code pénal relatifs à certaines infractions en matière informatique sont modifiés afin de les adapter au commerce électronique. En effet, le commerce électronique représente une réalité technologique plus vaste que l'informatique. Il part des ordinateurs où l'information est traitée, reçue, envoyée, conservée, pour aller sur les réseaux et notamment sur la „toile d'Internet".

Art. 52.– 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 20.000 francs à 500.000 francs ou de l'une de ces deux peines."

Art. 53.– 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 20.000 francs à 500.000 francs ou de l'une de ces deux peines."

Section 2. De l'instruction

Art. 54.– Un nouvel article 33-1 rédigé comme suit, est inséré dans le code d'instruction criminelle:

„L'officier de police judiciaire peut, dans les conditions prévues aux articles 31 et 33, saisir des données stockées, traitées ou transmises dans un système informatique.

A cet effet, il peut saisir le support matériel des données ou copier les données sur un autre support. Il peut interdire l'accès aux données saisies contenues dans le système ou retirer les données saisies du système."

Art. 55.– Un nouvel article 66-1 rédigé comme suit, est inséré dans le code d'instruction criminelle:

„Le juge d'instruction peut, dans les conditions prévues à l'article 66, saisir des données stockées, traitées ou transmises dans un système informatique.

A cet effet, le juge d'instruction peut saisir le support matériel des données ou copier les données sur un autre support. Il peut interdire l'accès aux données saisies contenues dans le système ou retirer les données saisies du système.

Le juge d'instruction peut, par ordonnance motivée, enjoindre à une personne, hormis l'inculpé, dont il considère qu'elle a une connaissance particulière du système informatique ou du mécanisme de protection ou de cryptage, qu'elle lui donne accès au système saisi ou aux données saisies contenues dans ce système ainsi qu'à la compréhension de données saisies protégées ou cryptées. Sous réserve des dispositions des articles 72, 73 et 76 ci-dessous et des cas où la personne est obligée de garder secrets les renseignements lui confiés dans le cadre de son activité professionnelle, la personne désignée est tenue de prêter son concours. En cas de refus, le juge d'instruction peut la condamner à l'amende prévue à l'article 77 (2)."

Art. 56.– L'article 77 du code d'instruction criminelle est modifié comme suit:

„(1) Toute personne citée pour être entendue comme témoin est tenue de comparaître, de prêter serment et de déposer, sous réserve des dispositions des articles 72, 73 et 76 ci-dessus et de l'article 458 du Code pénal.

(2) Si le témoin ne comparaît pas, le juge d'instruction peut, sur les réquisitions du procureur d'Etat, l'y contraindre par la force publique et le condamner à une amende de 10.001 à 100.000 francs. S'il comparaît ultérieurement, il peut toutefois, sur production de ses excuses et justifications, être déchargé de cette peine par le juge d'instruction, après réquisition du procureur d'Etat.

(3) La même peine peut, sur les réquisitions de ce magistrat, être prononcée contre le témoin qui, bien que comparaissant, refuse de prêter serment et de faire sa déposition.

(4) Le témoin condamné à l'amende en vertu des alinéas précédents peut interjeter appel de la condamnation dans les trois jours de ce prononcé; s'il était défaillant ce délai ne commence à courir que du jour de la notification de la condamnation. L'appel est porté devant la chambre du conseil de la Cour d'appel.

(5) La mesure de contrainte dont fait l'objet le témoin défaillant est prise par voie de réquisition. Le témoin est conduit directement et sans délai devant le magistrat qui a prescrit la mesure.“

*

TITRE IV

DES COMMUNICATIONS COMMERCIALES

Art. 57.– ***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.

La définition des communications commerciales est très directement inspirée de l'approche retenue par la position commune en vue de l'adoption de la directive relative à certains aspects juridiques des services de la société de l'information dans le Marché intérieur (article 2 f)) (voir également le Livre vert „Les communications commerciales dans le marché intérieur" Com (96) 192; Suivi du Livre vert „Les communications commerciales dans le marché intérieur – Communication de la Commission", http://www.europa.eu.int/comm/dg15/fr/index.htm, mars 1998 (page 7)). La Commission entend agir à plusieurs niveaux et de façon coordonnée sur „toutes les formes de publicités, de marketing direct, de parrainage, de promotion des ventes et de relations publiques, de même que sur l'utilisation faite des services de communications commerciales dans la conception des emballages, à l'exception de l'étiquetage (Suivi du Livre vert „Les communications commerciales dans le marché intérieur – Communication de la Commission" préc., p. 12). Concrètement, elle souhaite procéder dans les meilleurs délais à une évaluation complète de toutes les réglementations nationales qui influent sur la validité ou le développement des communications commerciales. Parallèlement, elle accélère le traitement des plaintes reçues en cette matière, et n'exclut pas de favoriser une harmonisation progressive de la législation applicable. Dans cette perspective, la Commission a affirmé son intention d'examiner, par priorité, les disparités entre les dispositions nationales portant notamment sur les réductions de prix, le couponnage, les cadeaux-primes, ou encore sur les concours et loteries commerciales. C'est dire si la nouvelle politique communautaire amorcée en matière de communications commerciales sera susceptible d'influer, dans un avenir proche, sur les cadres réglementaires nationaux, lesquels devront nécessairement évoluer vers une plus grande libéralisation.

L'alinéa 2 de l'article 57 contient une définition négative des communications commerciales qui est issue de l'article 2 f) de l'accord politique en vue de la position commune relative au commerce électronique. Le premier tiret peut être illustré par un exemple: sur un site X sur la vente de vins on trouve le nom de domaine Y qui renvoie à son site pour des promotions portant sur des téléphones mobiles, or la mention de ce nom de domaine ne constitue pas de la communication commerciale car la publicité n'est pas directe mais elle sera faite sur le site de Y. Le second tiret peut être illustré par un autre exemple: sur un site on mentionne la possibilité de comparer les prix et la qualité des produits, le site offre un système de tests comparatifs, il ne s'agit pas de communication commerciale car elle n'est pas faite de manière indépendante et pas dans l'intérêt direct des entreprises visées, il s'agit de ce que l'on pourrait appeler de la communication critique.

Art. 58.– ***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.

Les communications commerciales sont en passe de devenir une immense source de richesse sur Internet. Elles couvrent toutes les formes de publicité, de marketing direct, de parrainage, de promotion des ventes et de relations publiques. De même que toute l'utilisation qui est faite de ces outils de communication par tous les secteurs de biens et de services, les organismes publics et semi-publics, et les organisations caritatives et politiques. Ces dispositions s'inspirent directement de l'article 6 sur les communications commerciales de la future position commune en vue de l'adoption de la directive sur le commerce électronique. Cet article énonce le principe de l'identification claire de la communication commerciale comme telle. En effet, il est essentiel que le consommateur sache qui procède à cette communication commerciale, que l'opérateur commercial ne soit pas caché. Cette identification claire passe, par exemple, par une adresse de retour de celui qui a fait la communication commerciale.

Selon la future position commune, dans son article 6, les offres promotionnelles, si elles sont autorisées par la législation luxembourgeoise, peuvent faire l'objet de communications commerciales par les sociétés établies au Luxembourg, ce qui ne semble pas être le cas pour le moment (selon les articles 16 à 20 de la loi du 27 novembre 1986 réglementant certaines pratiques commerciales et sanctionnant la concurrence déloyale telle qu'elle a été modifiée par loi du 14 mai 1992) aussi n'avons-nous pas introduit la disposition suivante:

les offres promotionnelles, telles que les rabais, les primes et les cadeaux, doivent être clairement identifiables comme tels et les conditions pour en bénéficier doivent être aisément accessibles et présentées de manière précise et non équivoque. Par contre, les sociétés établies dans les autres Etats membres peuvent faire de la communication commerciale sur ces offres au Luxembourg puisque c'est le principe du pays d'origine qui s'applique. Ces sociétés seront alors soumises à cette obligation de transparence conformément à la législation de leur pays.

De plus, la personne pour le compte de laquelle cette communication est faite doit être identifiable, imaginons par exemple le cas des ventes pyramidales.

Art. 59.– ***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" où les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces personnes. Dans le cas contraire, les autorités compétentes peuvent prendre des sanctions contre ces prestataires. Les autorités compétentes et les sanctions seront déterminées par règlement grand-ducal.

§ 1: Directement inspirée par l'article 7 de la future position commune en vue de l'adoption de la directive sur le commerce électronique, ***l'obligation d'identifier clairement les communications commerciales non sollicitées*** *trouverait également sa place dans un texte général sur la publicité de manière à imposer le respect de cette exigence, non seulement aux opérateurs dont les messages sont diffusés par voie électronique, mais aussi aux acteurs économiques utilisant des techniques publicitaires rédactionnelles par voie de presse.*

Le § 2 consacre la technique de opt out ***qui vise à interdire toute communication commerciale par courrier électronique en cas d'opposition manifeste du destinataire du service****, consommateur ou utilisateur.*

La future position commune relative au commerce électronique n'exige pas explicitement que les Etats membres mettent en place des registres d'opt out dans le § 2 de l'art. 7 consacré aux communications commerciales non sollicitées mais elle les y incite. Ces registres conféraient à tout destinataire du service de la société l'information le droit de s'opposer, sur simple demande et gratuitement, à la réception de communications commerciales. La reconnaissance de ce droit suppose, en pratique, que les professionnels mettent en place ou adhèrent à des structures destinées à centraliser les refus exprimés par les destinataires des communications commerciales. Comme la future position commune précitée le précise, il est exigé que les Etats membres prennent des mesures pour assurer que les prestataires de services procédant à des communications commerciales non sollicitées consultent régulièrement et respectent les registres d'opt out dans lesquels les personnes physiques qui ne veulent pas recevoir de telles communications s'inscrivent.

*

TITRE V

DES CONTRATS CONCLUS PAR VOIE ELECTRONIQUE

Chapitre I. – *Dispositions communes*

Art. 60.– ***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.

Cette définition est directement issue de la proposition modifiée de directive relative aux ventes à distance de services financiers et du document du Conseil du 29 octobre 1999 No 12383/99.

La directive 97/7 relative aux ventes à distance fait référence à la notion de support durable mais n'en fournit aucune définition. A la lecture de ce texte, il apparaît cependant que le consommateur doit être en mesure non seulement d'accéder à des données fiables, mais aussi de les conserver sans que les informations délivrées puissent être altérées.

Service financier: tout service fourni par un établissement de crédit, un autre professionnel du secteur financier ou une entreprise d'assurance et de réassurance.

Il est proposé de se référer à l'ensemble des services fournis par les établissements de crédit, les autres professionnels du secteur financier, et les entreprises d'assurance et de réassurance. Ainsi dispose-t-on d'une définition large et donc adaptable à la future évolution de la proposition de directive relative aux contrats négociés à distance de services financiers.

Art. 61.– ***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 caution et de garantie 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 64 à 70 s'appliquent uniquement entre professionnels et consommateurs.

Cette liste est directement inspirée de l'article 9 § 2 de l'accord politique en vue de la position commune relative au commerce électronique. Ces contrats sont exclus car ils présentent un formalisme trop important et protecteur, pour être conclus par voie électronique.

Le § 2 précise que les articles 64 à 70 visent à protéger plus spécifiquement les consommateurs et ne s'appliquent pas entre professionnels alors que les articles 62 et 63 s'appliquent entre professionnels et entre consommateurs et professionnels.

Cela provient du fait que les articles 64 à 70 intègrent des articles issus de la directive relative aux ventes à distance, directive de protection des consommateurs alors que les articles 62 et 63 intègrent des dispositions provenant de l'accord politique en vue de la position commune relative au commerce électronique.

Art. 62.– ***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 l'identification et la correction des erreurs figurant dans les données introduites 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.

Cet article est directement inspiré de l'article 10 (§ 1 et § 2 a)) de la future position commune relative au commerce électronique. Elle a pour but un consentement éclairé et complet des parties dans les différentes étapes à suivre pour la conclusion d'un contrat.

Ces informations sont à fournir indépendamment de la volonté de conclure un contrat ou pas. Il s'agit ici de la formation du contrat.

Les dispositions de l'alinéa c) permettent d'éviter la conclusion d'un contrat par erreur ou d'autres erreurs dans la conclusion du contrat lui-même.

§ 3.– Les deux premiers paragraphes du présent article ne s'appliquent pas aux contrats conclus exclusivement par échange de courrier électronique ou par des communications individuelles équivalentes.

Ce § 3 est directement inspiré du § 3 de l'article 10 de la future position commune arrêtée par le Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil relative à certains aspects

juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur. Elle vise à ne pas imposer aux prestataires de service des charges techniques trop lourdes quand les contrats sont passés par simple email. Cependant, cette future position commune[1] *contient un nouveau considérant qui précise bien que „les exceptions relatives aux contrats passés exclusivement au moyen d'un échange de messages électroniques ou au moyen de communications commerciales équivalentes …, en ce qui concerne les informations à fournir et les obligations relatives à la conclusion d'un contrat, ne sauraient avoir comme conséquence de permettre le contournement de ces dispositions par les prestataires de services de la société de l'information".*

Art. 63.– ***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.

Afin d'assurer la sécurité juridique pour les contrats conclus sur Internet, il est indispensable de déterminer le moment de conclusion du contrat. La détermination du moment de conclusion du contrat correspond à la proposition modifiée de directive relative à certains aspects juridiques du commerce électronique dans le marché intérieur du 30 août 1999[2]*. Si on ne détermine pas ce moment il le sera selon les règles de droit commun de droit civil qui risqueraient d'être difficiles à transposer en univers électronique.*

Ce moment est donc celui où le destinataire reçoit du prestataire un accusé de réception de l'acceptation du destinataire. Et à partir de la date où le contrat est considéré comme conclu commencent à courir tous les délais, par exemple le délai de rétractation pour un consommateur.

Comme moyens technologiques pour manifester son acceptation il y a par exemple le fait de cliquer sur un icône.

L'accusé de réception par un prestataire peut être constitué par la fourniture en ligne d'un service payé.

§ 2.– Les dispositions du premier paragraphe du présent article ne sont pas applicables aux contrats conclus exclusivement au moyen d'un échange de messages électroniques ou au moyen de communications commerciales équivalentes.

Ce paragraphe 2 atteste de la même préoccupation que le § 3 de l'article 62.

Chapitre II. – *Des contrats conclus avec les consommateurs*

Ce chapitre contient des dispositions spécifiques à la protection des consommateurs qui sont inspirées de la directive 97/7 relative à la vente à distance et sont ensuite adaptées au commerce électronique puisqu'un texte plus général sur la vente à distance va être élaboré.

Art. 64.– ***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, 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;

---

1 Doc. 14263/99 ECO 419 CONSOM 80 CODEC 826.

2 Dossier interinstitutionnel No 98/0325(COD), doc. No 10644/99 ECO 280, CONSOM 48 CODEC 462.

- 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 66 § 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.

Dans les articles 64 à 70 propres à la protection du consommateur, nous utilisons une terminologie différente sur un point:

nous parlons de prestataire de services de la société de l'information au lieu de fournisseur, terme utilisé dans la directive relative aux ventes à distance. Le terme de prestataire de services pouvant couvrir certains prestataires qui ne fournissent pas forcément un service contre rémunération directement par le client ou le consommateur.

L'information complète du consommateur avant la conclusion du contrat est une condition essentielle de la validité de la convention future et de la qualité du consentement des contractants. L'obligation d'information mise à la charge du prestataire revêt en matière de commerce électronique une importance d'autant plus considérable qu'il n'existe par définition aucun contact physique possible entre prestataire et consommateur. Dans cette perspective, l'information préalable et complète du consommateur apparaît comme une condition indispensable, non seulement à la protection des consommateurs, mais aussi à la confiance des utilisateurs (destinataires de services de la société de l'information) de ces nouvelles formes de communication et corrélativement au développement du commerce électronique. Bien évidemment, l'article 5 du projet, qui prévoit une obligation générale d'information à la charge du prestataire et envers tout destinataire, bénéficie aussi au consommateur. Il est en effet utile pour le consommateur d'avoir par exemple l'adresse électronique et géographique du prestataire. De plus, les obligations d'information figurant dans les textes luxembourgeois existants et susceptibles de s'appliquer aux services de la société de l'information s'appliquent toujours. Par ailleurs le projet relatif à la transposition de la future directive relative aux services financiers à distance contiendra aussi des dispositions sur l'obligation d'information en cette matière.

§ 1er: Usant de la faculté laissée aux Etats membres d'offrir si nécessaire aux consommateurs une protection plus étendue que celle qui résulterait d'une transposition stricte de la norme communautaire, la liste proposée à l'article 64 précise ou complète parfois le contenu de l'obligation d'information, dont le principe et les contours d'application ont été fixés par la directive communautaire relative aux ventes à distance.

Certaines dispositions visent précisément à répondre aux particularités du commerce électronique, et aux attentes légitimes de ses acteurs, spécialement en matière de sécurité des transactions. Ainsi, le prestataire qui dispose d'un certificat délivré par un prestataire de service de certification accrédité doit en informer le consommateur, cette indication renforçant à la fois la notoriété et la crédibilité de l'offreur, mais aussi la confiance du consommateur désireux de contracter. De la même manière, et pour des raisons analogues, le prestataire est tenu de communiquer son adresse en tout état de cause, et non plus seulement lorsqu'un paiement anticipé est effectué ainsi que le prévoit la directive ventes à distance.

Au-delà de l'obligation d'information relative à l'identité du prestataire, le présent article renforce la protection du consommateur en ce qu'il développe l'information préalable obligatoire portant sur le contenu de l'offre commerciale et sur les conditions contractuelles proposées.

Considérant que la connaissance du contenu des garanties commerciales éventuellement proposées peut être de nature à influer sur la décision du consommateur de contracter, ou au contraire de rechercher une solution alternative plus attractive, le présent article fait obligation au prestataire de diffuser les informations concernant notamment les conditions afférentes à la mise en oeuvre des garanties commerciales et du service après-vente proposés.

En ce qui concerne l'information préalable portant sur les conditions contractuelles, le présent article en renforce légèrement le contenu en faisant obligation au prestataire d'informer le consommateur d'une part de l'absence de confirmation des conditions de la transaction lorsque l'opération est réalisée au moyen d'un service de la société de l'information, et d'autre part de l'existence mais aussi de l'absence du droit de rétractation selon les cas prévus par le présent chapitre.

L'information préalable et obligatoire du consommateur est enfin étendue aux modes de remboursement des sommes éventuellement versées par le consommateur avant la fin de la période de rétractation. Une telle mesure devrait inciter les entreprises à une plus grande clarté dans leurs politiques de remboursement, favorisant ainsi l'émergence de mécanismes contractuels de remboursement plus efficaces et plus rapides.

S'agissant de la présentation de l'ensemble de ces informations, le prestataire ne doit pas utiliser de techniques visant à attirer l'attention du consommateur sur une partie seulement de l'écran de façon à mettre en évidence certaines informations au détriment d'autres: toutes les informations délivrées doivent être suffisamment lisibles. En toute hypothèse, les règles de droit commun interdisant la publicité trompeuse ou de nature à induire en erreur s'appliquent au commerce électronique, et sont susceptibles de sanctionner aussi bien une inexactitude affectant le contenu de l'information diffusée que la présentation de cette information.

Les informations préalables doivent être fournies au consommateur „en temps utile avant la conclusion du contrat". Cette rédaction est issue de l'article 4 § 1 de la directive 97/7/CE.

§ 2: Afin de tirer pleinement avantage des possibilités offertes par les techniques de communication modernes, il est prévu d'obliger le prestataire à garantir au consommateur un accès en ligne aux informations à tout stade de la transaction (par le biais par exemple d'un lien hypertexte).

Le dialogue direct entre le consommateur et le prestataire est également encouragé, dans la mesure toutefois où les moyens nécessaires pour établir ce dialogue sont à la portée du prestataire. Nous avons supprimé le terme interactif car un service de la société de l'information est interactif puisqu'il est à la demande du destinataire du service qui est actif.

§ 3: Dans les hypothèses où le consommateur ne bénéficie pas du droit de rétractation certaines informations additionnelles sont exigées, afin de permettre au consommateur de se rendre compte si notamment le produit acheté ou le service demandé est compatible avec les installations techniques dont il dispose, et d'évaluer le temps et le coût approximatif de téléchargement d'un produit ou d'un service, par exemple, téléchargement d'un logiciel ou d'un CD.

Art. 65.– ***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 a accès, la confirmation des informations mentionnées à l'article 64 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.

§ 1: Conformément à l'article 5 de la directive 97/7, le texte pose le principe d'une confirmation obligatoire des informations données par le professionnel, nous ne visons ici que le prestataire de services de la société de l'information car sinon on pourrait entraîner une confusion et croire que l'on vise aussi le destinataire de services puisque celui-ci peut aussi être un professionnel(utilisateur).

Dans un souci de simplification, cette confirmation porte exactement sur les mêmes informations que celles qui doivent être fournies avant la conclusion du contrat (articles 62 et 64), outre l'indication des conditions d'exercice du droit de rétractation.

La confirmation suppose une démarche positive de la part du prestataire. Il n'appartient pas au consommateur de prendre l'initiative de télécharger ou imprimer les informations qui s'affichent sur son écran, c'est bien le prestataire qui doit s'en charger et présenter l'ensemble des informations requises sur un support durable, directement accessible et à la disposition du consommateur.

§ 2: Par exception, les informations délivrées ne sont soumises à aucune confirmation obligatoire lorsque le contrat porte sur un service dont l'exécution elle-même est réalisée au moyen d'un service de la société de l'information, à condition que le service soit fourni en une seule fois, et qu'il soit facturé par le prestataire. Toutefois, on trouve une obligation d'information à ce sujet au stade des informations préalables: le prestataire doit informer le consommateur de l'absence de confirmation des informations pour ce type de services (article 64 § 1, 11ème tiret).

Cette obligation d'information, destinée à compenser l'absence de confirmation ultérieure n'est pas imposée par la directive communautaire. Il s'agit donc d'une obligation supplémentaire insérée dans le projet de loi luxembourgeois.

§ 3: A des fins probatoires, le consommateur doit être en mesure d'obtenir un enregistrement exhaustif des éléments sur lesquels il a donné son accord, et qui font l'objet de la transaction. La précision de la date et de l'heure de la transaction revêtent une importance indiscutable en terme de preuve mais aussi en terme de sécurité juridique, à la fois pour le consommateur et aussi pour le prestataire.

Art. 66.– ***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 65, 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 quatorze 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 rétraction de quatorze 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;

h) les contrats dont l'exécution est entièrement terminée avant que le consommateur n'exerce son droit de rétractation.

§ 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.

Les modalités d'exercice du droit de rétractation sont directement inspirées de l'article 6 de la directive 97/7. Cependant, un effort de simplification a été entrepris, les dispositions communautaires ne paraissant pas sur ce point d'une clarté suffisante. Si le dispositif proposé est conforme à l'esprit de la directive, le texte proposé ne reprend pas la lettre de l'article 6 précité.

§§ 1 et 2: Le texte proposé envisage deux hypothèses:

– *un régime de droit commun (délai de rétractation de 7 jours) applicable lorsque l'obligation de confirmation des informations a été remplie.*

– *un délai de rétractation de 3 mois applicable lorsque l'obligation de confirmation n'a pas été remplie avec toutefois la possibilité de revenir au délai de 7 jours si la confirmation des informations intervient tardivement.*

§ 3: Le consommateur exerce son droit de rétractation sur tout support durable, notion définie par l'article 60 de la présente loi.

§ 4: Ce paragraphe vise les cas dans lesquels le droit de rétractation ne s'exerce pas.

L'alinéa f) du § 4: L'exercice de la faculté de rétractation est exclu pour deux types de contrats : les contrats portant sur des produits financiers dont le prix dépend des fluctuations du marché que le prestataire n'est pas en mesure de contrôler, les contrats portant sur les assurances de moins d'un mois.

La première exclusion vise à empêcher des manœuvres spéculatives sur de tels produits. Dans le second cas, la survenance rapide du terme permet au consommateur de se tourner presque aussitôt vers un autre prestataire, sans qu'il soit besoin de lui accorder un délai pour se rétracter.

§ 5: Ce texte entend régler le sort d'un crédit affecté à une opération particulière lorsque le consommateur exerce son droit de rétractation et renonce ainsi à l'opération ayant motivé la demande de crédit.

Art. 67.– ***Du paiement du service financier fourni avant la rétractation***

§ 1.– Quand le consommateur exerce son droit de rétractation conformément à l'article 66, il ne peut être tenu qu'au paiement de la partie du prix proportionnellement au service financier effectivement fourni par le prestataire.

Ce montant ne saurait être en aucun cas interprété comme une pénalité.

§ 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 64, 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 reçues de ce dernier en accord avec le contrat conclu, excepté le montant à payer au §1 du présent article.

Cette période débutera du jour où le prestataire a reçu la notification de la rétractation.

§ 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. Cette période débute du jour où le consommateur envoie la notification de la rétractation.

Ces dispositions sont inspirées de la proposition modifiée de directive relative aux contrats à distance de services financiers dans sa version du 19 novembre 1999[1].

§ 1 et § 2: Cette hypothèse permet de couvrir des situations où le service serait entièrement fourni avant la fin du délai de rétractation, situation dans laquelle le prestataire risque d'être dans l'impossibilité de remettre les choses en l'état. Dans ce cas, l'exécution du contrat est cependant soumise à l'acceptation expresse du consommateur.

§ 3: Le prestataire restitue au consommateur les sommes qu'il a reçues en exécution du contrat excepté le coût du service rendu par le prestataire entre le moment de la conclusion du contrat et la rétractation.

§ 4: Lorsque le consommateur exerce son droit de rétractation, il peut être tenu de restituer le bien ou les sommes reçues prestataire entre le moment de conclusion du contrat et la rétractation.

Art. 68.– ***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.

Ce texte vise à empêcher les prestations de services imposées, par exemple, un consommateur souscrit un abonnement sur Internet et le prestataire en profite pour lui facturer des produits qu'il n'a pas demandés. Il met en œuvre les dispositions de l'article 9 de la directive 97/7. Le consommateur n'a ni l'obligation de payer le prix, ni l'obligation de retourner le produit.

Art. 69.– ***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 du 25 août 1983 relative à la protection juridique du consommateur.

La charge de la preuve des conditions de conclusion du contrat incombe au prestataire, en effet faire peser une telle charge sur le consommateur serait trop lourd. De plus, c'est le prestataire qui met en ligne ces informations sur Internet.

Art. 70.– ***Exemptions***

Les articles 64, 65 et 66 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.

Ces dispositions sont directement inspirées de l'article 3.2 de la directive relative aux ventes à distance. Elles sont tout à fait applicables aux services de la société de l'information, en effet, on peut commander par exemple des pizzas sur Internet, réserver une chambre d'hôtel or il serait incohérent de soumettre ce genre de transactions à une obligation de confirmation (art. 65), à de nombreuses informations préalables (art. 64), au droit de rétractation (66).

*

1 Doc. No 12932/99 CONSOM 70 ECOFIN 238 CODEC 684.

TITRE VI

DE LA RESPONSABILITE DES PRESTATAIRES INTERMEDIAIRES

Ce titre V donne une sécurité juridique absolument indispensable aux opérateurs afin qu'ils ne craignent pas d'être poursuivis en permanence dès que des informations illicites circulent sur Internet. Si l'on posait le principe de responsabilité des intermédiaires, on ignorait le véritable problème, à savoir qui est à l'origine du contenu illicite et donc qui est réellement responsable.

Art. 71.– *Simple transport („mere conduit")*

§ 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) s'il sélectionne et modifie 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.

Ces dispositions sont directement inspirées de l'article 12 de la future position commune sur le commerce électronique. Elle réglemente la responsabilité des intermédiaires dans trois articles 12, 13 et 14. Elle cible des activités très précises et reste neutre technologiquement. Pour ces trois types d'activités bien précises, les prestataires de services sont, pour le simple transport et le caching, irresponsables, et pour l'hébergement, la responsabilité est limitée. Les conditions de cette exonération de responsabilité ou de sa limitation sont énumérées limitativement.

Dans les articles 71 à 73 du projet de loi, le principe est celui de l'irresponsabilité des intermédiaires uniquement quant à l'activité de transport et son corollaire le stockage éphémère. En effet, techniquement pour transporter des informations d'un point A à un point B il faut faire des copies techniques, ces copies sont automatiques et disparaissent rapidement. Mais le texte est très précis, il s'agit d'un stockage automatique, intermédiaire et transitoire. Ce stockage ne doit pas être confondu avec le caching visé à l'article suivant du projet de loi.

Pour bénéficier d'une exonération de responsabilité, trois conditions doivent être remplies cumulativement. Le fait qu'un prestataire procède automatiquement à une transmission à la demande d'un destinataire de son service ne doit pas avoir pour conséquence qu'il soit considéré comme à l'origine de la transmission par exemple.

Quant au stockage éphémère visé au paragraphe 2 du présent article, sont visées uniquement les activités de stockage permettant l'exécution de la transmission de l'information. Ces activités de stockage n'incluent pas les copies que fait le prestataire dans le but de mettre les informations à la disposition d'utilisateurs ultérieurs. Ces activités de stockage font l'objet de l'article 72.

Précisons que la durée du stockage des informations ne doit pas dépasser le temps raisonnablement nécessaire à la transmission.

Il est clair qu'un prestataire qui collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales va au-delà des activités de „simple transport" ou de „caching" et que, dès lors, il ne peut bénéficier des dérogations en matière de responsabilité prévues pour ce type d'activités.

Art. 72.– *Le „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'un tribunal ou une autorité administrative a ordonné le retrait de l'information ou interdit son accès.

Le caching fait en permanence des copies automatiques et temporaires selon un processus non surveillé donc sans accès au contenu.

Le caching est seul visé ici et il est important seulement parce qu'il rend plus efficace la transmission. Il y a stockage uniquement dans un but d'accélération de la transmission.

On entend dans l'alinéa b) par conditions d'accès à l'information tout ce qui a pour objectif de rendre l'accès conditionnel à un site par exemple. Il s'agit de systèmes techniques pour protéger l'intérêt économique de la personne qui a mis en place le service.

On vise dans l'alinéa c) les pratiques technologiques pour les mises à jour utilisées par les professionnels.

Dans l'alinéa d) il s'agit de protéger les accès conditionnels. Par exemple, il existe des technologies dans des sites qui permettent de savoir combien il y a de visiteurs par jour or l'intermédiaire qui fait du caching ne doit pas interférer dans ces techniques.

Dans l'alinéa e), on met comme condition de l'irresponsabilité le fait que le prestataire retire des sites miroirs (caching) les informations copiées automatiquement si elles ont été retirées d'un site ou rendues inaccessibles sur ce site. Si techniquement le prestataire ne les retire pas qu'il rende l'accès impossible à ces informations si cela a été fait pour le site „principal".

Pour pouvoir être exempté d'une responsabilité qui pourrait éventuellement lui être opposée pour ce type de stockage, le prestataire de service doit donc respecter certaines conditions.

Art. 73.– ***Hébergement***

§ 1.– 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 l'activité ou l'information sont vraisemblablement illicites; 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.

Cet article est directement inspiré de la future position commune sur le „commerce électronique", plus précisément l'article 14. Il instaure une limite de responsabilité en ce qui concerne l'activité de stockage des informations fournies par les destinataires du service, stockage effectué à leur demande (par exemple, fourniture d'un espace serveur pour le site web d'une entreprise ou d'un particulier, un forum …).

L'exonération de responsabilité concerne la responsabilité tant civile que pénale.

Le principe posé dans le paragraphe 1 est le suivant: dès que le prestataire a connaissance de faits illicites il doit agir vite et ainsi ne voit pas sa responsabilité engagée.

Donc en cas de connaissance effective le prestataire a sa responsabilité engagée s'il reste inactif mais cela se révélera parfois difficile à prouver. Dans tous les cas où l'activité est apparemment illicite il peut aussi voir sa responsabilité engagée car il aura eu suffisamment d'indices et n'aura pas averti les autorités, il aura commis une négligence. Ensuite c'est au droit commun de fixer les conditions de cette négligence (fautive ou responsabilité sans faute …).

Le prestataire doit donc prendre rapidement des mesures pour retirer les informations ou rendre l'accès à celles-ci impossible. Ce principe énoncé au b) du § 1 constitue une base sur laquelle les différentes parties intéressées peuvent effectivement mettre en place des procédures permettant de notifier au prestataire de services des informations qui est à l'origine d'une activité illicite, et obtenir le retrait de ces informations ou une interdiction d'accès (procédures parfois appelées „procédures de notification et

de retrait", „notice and take down procedures"). Néanmoins, ces procédures ne se substituent pas aux voies de recours judiciaires existantes.

Le paragraphe 2 vise les cas où le prestataire fournit plus que de l'hébergement donc il ne peut pas invoquer son irresponsabilité. Par exemple, un fournisseur d'hébergement ouvre un service de ragots et passe pour cela un contrat avec un journaliste. Si des propos diffamatoires sont rapportés par le journaliste le prestataire qui l'héberge ne pourra pas prétendre à l'irresponsabilité car il aura fait plus que de l'hébergement, il se sera rapproché d'une activité éditoriale.

Art. 74.– ***Absence d'obligation en matière de surveillance***

§ 1.– Pour la fourniture des services visés aux articles 71 à 73, 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.– Le paragraphe 1 du présent article est 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.

Cet article est inspiré de l'article 15 de la future position commune sur le commerce électronique.

Le principe est donc l'absence d'obligation générale de surveillance, néanmoins, les autorités judiciaires peuvent demander aux prestataires de les informer s'ils soupçonnent des activités illégales. Les cas où cette information est requise sont à la discrétion de ces autorités. Cependant le principe de non-surveillance demeure.

*

TITRE VII

DES PAIEMENTS ELECTRONIQUES

Les définitions de ce titre VI et son champ d'application sont inspirées de la recommandation de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire[1]*. Il était essentiel pour tous les acteurs du commerce électronique de créer un environnement juridique sécurisant.*

Cette sécurité passe tout d'abord, par les définitions du paiement électronique, de l'émetteur, du titulaire et du champ d'application. Ensuite, l'émetteur voit peser sur lui certaines obligations, et enfin le titulaire a certaines obligations juridiques notamment celle de notifier la perte ou le vol de son instrument de paiement. Enfin, le titulaire ne peut révoquer ses instructions de paiement car cela donnerait lieu à des contestations.

Art. 75.– ***Définitions***

Pour l'application du présent titre, il faut entendre par:

§ 1.– „*instrument de transfert électronique de fonds*": 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 rechargeable.

§ 2.– „*instrument rechargeable*": tout instrument de transfert électronique de fonds sur lequel des unités de valeur sont stockées électroniquement.

§ 3.– „*émetteur*": une personne, qui dans le cadre de son activité commerciale, met un instrument de transfert électronique de fonds à la disposition d'une autre personne conformément à un contrat conclu avec celle-ci.

§ 4.– „*titulaire*": une personne qui, en vertu d'un contrat qu'elle a conclu avec un émetteur, détient un instrument de transfert électronique de fonds.

---

1 JO No L 208 du 2 août 1997, pp. 52-58.

La définition de l'instrument de transfert électronique de fonds se veut plus simple que celle de la recommandation de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique qui comprend une définition du paiement électronique qui d'une part, renvoie au champ d'application (opérations visées) et d'autre part, contient une autre définition, celle d'instrument de paiement d'accès à distance. Or ces deux définitions (instrument de paiement électronique et instrument de paiement d'accès à distance) peuvent être regroupées.

L'instrument rechargeable représente la même chose que l'instrument de monnaie électronique issue de la recommandation mais nous avons voulu éviter la confusion avec d'autres textes qui définissent la monnaie électronique, notamment la position commune arrêtée par le Conseil le 29 novembre en vue de l'adoption de la directive concernant l'accès à l'activité des établissements de monnaie électronique et son exercice, ainsi que la surveillance prudentielle de ces établissements[1]*. De plus, en déterminant que l'instrument rechargeable est un instrument de transfert électronique de fonds cela sous-tend que l'instrument rechargeable permet de procéder aux opérations visées au § 1.*

Les instruments rechargeables sont par exemple des cartes prépayées ou une mémoire d'ordinateur sur lesquelles des unités de valeur sont stockées électroniquement, en Belgique par exemple la carte Proton. Au Luxembourg, le porte-monnaie électronique miniCASH émis par un certain nombre d'institutions financières et géré par le CETREL.

Art. 76.– ***Champ d'application***

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.

Ce que l'on cherche à protéger à travers l'instrument rechargeable c'est le compte en banque qui y est relié. De plus, certaines cartes sont rechargeables sans accès à un compte comme les cartes de photocopies par exemple. Par ailleurs, les cartes monoprestataires n'ont pas besoin d'être couvertes.

Bien évidemment, seuls les transferts de fonds sont réalisés par chèque, non le chargement et le déchargement d'un instrument de paiement rechargeable.

Art. 77.– ***La preuve des paiements effectués***

L'émetteur doit conserver un relevé interne des opérations effectuées à l'aide d'un instrument de transfert électronique de fonds, pendant une période d'au moins cinq ans à compter de l'exécution des opérations.

Cette disposition est directement inspirée de l'article 7 c) de la recommandation de la Commission du 30 juillet 1997. Il est essentiel que les opérations effectuées au moyen d'instruments de transfert électronique de fonds fassent l'objet d'un enregistrement afin d'en garder la trace et de pouvoir rectifier les erreurs éventuelles.

Art. 78.– ***La charge de la preuve***

L'émetteur doit, en cas de contestation d'une opération effectuée à l'aide d'un instrument de transfert électronique de fonds, 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.

La charge de la preuve, lorsqu'il s'agit d'établir qu'une transaction a été dûment enregistrée et inscrite dans les comptes et n'a pas été affectée par un incident technique ou tout autre dysfonctionnement, doit incomber à l'émetteur. Cette disposition est inspirée de l'article 7 alinéa e) de la recommandation. Il est évident que la charge de la preuve ne saurait reposer sur le titulaire, en effet, c'est l'émetteur qui détient l'équipement technique qui permet d'utiliser l'instrument de transfert électronique de fonds.

Art. 79.– ***Des risques liés à l'utilisation d'un instrument de transfert électronique de fonds***

§ 1. Le titulaire d'un instrument de transfert électronique de fonds 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 rechargeable.

---

1 No 12004/2/99 REV 2 EF36, ECOFIn, 190, CODEC 577.

L'émetteur d'un instrument de transfert électronique de fonds doit mettre à la disposition du titulaire les moyens appropriés pour effectuer cette notification.

§ 2. Hormis le cas où il s'est rendu coupable d'une fraude ou de négligence grave, le titulaire d'un instrument de transfert électronique de fonds visé à l'article 75 § 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.

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 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 transfert électronique de fonds visé à l'article 75 § 1 a), b) et c) après la notification.

§ 3. En toute hypothèse, l'utilisation d'un instrument de transfert électronique de fonds sans présentation physique de celui-ci ou identification électronique, n'engage pas la responsabilité de son titulaire.

Le partage de responsabilité entre le titulaire et l'émetteur de l'instrument de transfert électronique de fonds repose sur la notification de sa perte, de son vol ou de son utilisation frauduleuse par un tiers. Ces dispositions ne s'appliquent pas à l'utilisation d'un instrument rechargeable c'est pourquoi l'on précise qu'il s'agit d'un instrument de transfert électronique de fonds visé à l'article 75 § 1 a), b) et c).

Jusqu'à la notification, le titulaire n'assume en principe les risques d'une utilisation frauduleuse de l'instrument de transfert électronique de fonds qu'à concurrence d'un montant déterminé par voie de règlement grand-ducal. Ce montant pourrait être différent selon que le titulaire s'est rendu coupable ou non d'une faute ou d'une négligence grave.

De même, la situation est différente en matière d'instrument rechargeable puisque même après notification l'émetteur n'est pas responsable de la valeur stockée sur l'instrument puisque cet instrument est sans relation avec le compte bancaire et que la valeur stockée sera d'un montant limité.

Après la notification, les risques sont entièrement supportés par l'émetteur.

Le dernier paragraphe vise en particulier les paiements effectués par simple transmission du numéro apparent d'une carte de crédit pour lesquels la responsabilité du titulaire se trouve dégagée. Autre précision, la seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire. En effet, rien ne prouve que le titulaire ait communiqué son code secret dans le cas de l'utilisation par un tiers non autorisé de l'instrument de transfert électronique de fonds avec le code secret.

Art. 80.– ***Irrévocabilité des instructions de paiement***

Le titulaire ne peut révoquer une instruction qu'il a donnée au moyen de son instrument de transfert électronique de fonds, à l'exception de celle dont le montant n'est pas connu au moment où l'instruction est donnée.

Cette disposition est inspirée de l'article 5 d) de la recommandation du 30 juillet 1997et du considérant No 10. Elle est essentielle afin d'éviter de nombreuses contestations.

*

TITRE VIII

DISPOSITIONS FINALES

Art. 81.– Le Ministre de l'Economie est autorisé à procéder à l'engagement pour les besoins de l'Autorité d'Accréditation et de Surveillance de deux 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 21 décembre 1998 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 1999.

Art. 82.– § 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.

*

PARTIE C

ANNEXES

REGLEMENT GRAND-DUCAL (CERTIFICAT QUALIFIE ET EXIGENCES POUR LES DISPOSITIFS SECURISES DE CREATION DE SIGNATURE ELECTRONIQUE)

du xx yy 2000 concernant l'exécution concernant de l'article (17) et de l'article 25 de la loi du xx yy 2000 relatif au commerce électronique modifiant le code civil, le nouveau code de procédure civile et le code de commerce, de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers et la directive 93/13/CEE concernant les clauses abusives dans les contrats conclus avec les consommateurs

Nous JEAN, par la grâce de Dieu, Grand-Duc de Luxembourg, Duc de Nassau;

Vu la loi du xx yy 2000 relatif au commerce électronique modifiant le Code civil, le Nouveau code de procédure civile et le Code de commerce et transposant certaines dispositions de la directive 97/7/CEE concernant la protection des consommateurs en matière de contrats à distance et de la directive 93/13/CEE concernant la protection des consommateurs en matière de contrats à distance, et notamment son article 38 § 2;

Vu l'avis de la Chambre de Commerce;

Notre Conseil d'Etat entendu;

Sur le rapport de notre Ministre de l'Economie et après délibération du Gouvernement en Conseil;

Arrêtons:

Art. 1.– ***Définitions***

„*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.

Disposition directement issue de l'article 2.4 de la directive sur les signatures électroniques. Cette définition est technique, elle fait directement appel à la technique de la cryptographie c'est pourquoi nous l'avons placée dans un règlement. Ainsi le projet de loi reste-t-il neutre d'un point de vue technologique.

„*Dispositif de création de signature*", un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature.

Cette nouvelle définition est issue de la directive sur les signatures électroniques. Elle est plus simple et plus claire.

„*Dispositif sécurisé de création de signature*", dispositif de création de signature qui satisfait aux exigences prévues à l'article 3 du présent règlement grand-ducal.

Cette nouvelle définition est issue de l'annexe III de la directive sur les signatures électroniques. Les conditions posées à l'annexe III constituent un minimum , elles ne suffisent peut-être pas à la transmission de documents importants ou pour un montant important.

„*Données afférentes à la vérification de signature*", des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique.

De même que pour les données afférentes à la création de signature, la notion de données afférentes à la vérification de signature clarifie la question.

„*Dispositif de vérification de signature*“, un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature.

Cette définition, plus simple, est issue de la directive relative à un cadre communautaire pour les signatures électroniques.

*Les concepts de „**dispositif de création de signature**“, de „**dispositif sécurisé de signature**“ et de „**dispositif de vérification de signature**“ sont directement empruntés à la directive relative à un cadre communautaire pour les signatures électroniques. Bien qu'à l'heure actuelle seule la technologie de la cryptographie asymétrique paraît satisfaire aux conditions posées par le projet de loi, l'insertion de ces concepts dans un règlement permettra de les adapter à d'autres techniques ou de changer de concepts.*

Les codes ou clés utilisés par le signataire sont nécessairement uniques, de même qu'est unique la signature manuscrite d'une personne. Il incombera donc au prestataire de service de certification (voir définition ci-dessous) de vérifier que telle clé ou tel code n'a pas déjà été attribué. Il est évident que la fiabilité et la sécurité de la signature électronique supposent qu'à un dispositif de création donné ne corresponde qu'un seul dispositif de vérification. Toutefois ce dernier sera destiné à être rendu public et utilisé par chaque destinataire de message signé électroniquement.

„*certificat*“, une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne.

Cette définition est plus simple, elle est issue de la directive sur les signatures électroniques, dans l'article 2.9.

*La notion de „**certificat**“ est fondamentale dans le contexte de la certification électronique puisque celui-ci établit le lien entre une personne (c'est-à-dire son identité) et son dispositif de vérification de signature. Par l'émission du certificat, le prestataire de service de certification „certifie“, c'est-à-dire affirme publiquement l'exactitude des informations qu'il contient. Les informations seront sécurisées par la signature électronique du prestataire de service de certification qui l'émet. La directive „signatures électroniques“ emploie le terme électronique et non plus numérique.*

„*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 1 du règlement grand-ducal relatif aux exigences relatives aux prestataires émettant des certificats qualifiés.

Le certificat qualifié est essentiel car il constitue l'un des éléments nécessaires pour conférer des effets juridiques à la signature électronique. Il contient des garanties même si ces dernières sont minimales. Elles sont minimales dans un objectif de souplesse. Quant aux exigences propres à tout certificat qualifié il est important de noter qu'y figurent l'identification et la localisation du prestataire de service de certification ainsi que sa signature. Quant aux exigences propres aux prestataires délivrant les certificats elles sont aussi bien de nature technique telle que la fiabilité, la sécurité, que de nature financière et juridique telle que l'obligation d'information d'une personne demandant un certificat et l'obligation de stockage dans certaines conditions.

„*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.

Art. 2.– Tout certificat qualifié doit contenir les informations suivantes:

a) une mention spécifiant qu'il s'agit d'un certificat qualifié;

b) l'identification du prestataire de service de certification, ainsi que son lieu d'établissement;

c) les nom et prénom ou, sur demande, un pseudonyme ne prêtant pas à confusion et identifié comme tel de la personne physique, respectivement tout renseignement pertinent permettant d'identifier la personne morale titulaire du certificat;

d) le cas échéant, tout attribut spécifique et durable du titulaire, certifié à sa demande, tel que sa profession, son adresse, le fait d'être mandaté pour agir au nom d'une entreprise, sa solvabilité, l'existence d'une garantie bancaire, son numéro d'identification à la TVA ou d'identification fiscale, le fait d'être titulaire de permis ou de licences particuliers;

e) des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;

f) le dispositif de vérification de signature du titulaire correspondant au dispositif de création de signature utilisé par le titulaire pour la signature électronique certifiée;

g) la date d'émission et la date d'expiration du certificat;

h) le code d'identification unique du certificat;

i) la signature électronique du prestataire de service de certification qui délivre le certificat;

j) le cas échéant, l'étendue et les limites éventuelles à sa responsabilité; l'accréditation du prestataire de service de certification;

k) le cas échéant, les limites à l'utilisation du certificat, ainsi que la valeur des transactions pour lesquelles le certificat peut être utilisé.

Exiger que le certificat comporte la signature électronique du prestataire de service de certification nous paraît être une exigence essentielle de crédibilité et de sécurité du dispositif de certification.

Art. 3.– ***Les dispositifs sécurisés de création de signature***

§ 1.– Les dispositifs sécurisés de création de signature doivent garantir, par les moyens techniques et procédures appropriés, que:

a) les données utilisées pour la création de la signature ne puissent se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée;

b) 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;

c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

§ 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.

Ce règlement est directement inspiré de l'annexe III de la directive sur les signatures électroniques. Doivent être sécurisés c'est-à-dire à l'abri de toute falsification, de toute usurpation, que leur confidentialité soit assurée; en effet, le dispositif de création de signature représente la clé privée du signataire que lui seul connaît.

Le paragraphe 2 signifie que le futur signataire voit ce qu'il signe.

La directive relative aux signatures électroniques contient une annexe IV contenant une liste de recommandations pour la vérification sécurisée de la signature.

Art. 4.– Notre Ministre de l'Economie est chargé de l'exécution du présent règlement qui sera publié au Mémorial.

Palais de Luxembourg, le xx yy 2000

Pour le Grand-Duc:
Son Lieutenant-Représentant
HENRI
Grand-Duc Héritier

Le Ministre de l'Economie,
Henri GRETHEN

*

REGLEMENT GRAND-DUCAL (EXIGENCES CONCERNANT LES PRESTATAIRES DE SERVICE DE CERTIFICATION DELIVRANT DES CERTIFICATS QUALIFIES ET LES PRESTATAIRES ACCREDITES)

du xx yy 2000 concernant l'exécution de l'article 25 et 32 de la loi du xx yy 2000 relatif au commerce électronique modifiant le code civil, le nouveau code de procédure civile et le code de commerce et transposant la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers et la directive 93/13/CEE concernant les clauses abusives dans les contrats conclus avec les consommateurs

Nous JEAN, par la grâce de Dieu, Grand-Duc de Luxembourg, Duc de Nassau;

Vu la loi du xx yy 2000 relatif au commerce électronique modifiant le Code civil, le Nouveau code de procédure civile et le Code de commerce et transposant certaines dispositions de la directive 97/7/CEE concernant la protection des consommateurs en matière de contrats à distance et de la directive 93/13/CEE concernant la protection des consommateurs en matière de contrats à distance, et notamment son article 38 § 2;

Vu l'avis de la Chambre de Commerce;

Notre Conseil d'Etat entendu;

Sur le rapport de notre Ministre de l'Economie et après délibération du Gouvernement en Conseil;

Arrêtons:

Art. 1.– ***Prestataires de service de certification***

Un prestataire de service de certification doit:

a) présenter des garanties d'intégrité, de disponibilité, de sécurité pour exercer ses activités de certification;

b) conformément à l'article 23 de la présente loi, conserver un annuaire électronique comprenant les certificats qu'il délivre et le moment de leur expiration. Le fonctionnement de ce service d'annuaire doit être rapide, sûr et accessible en permanence à toute personne par voie électronique;

c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminés avec précision;

d) vérifier, par des moyens appropriés et conformes au droit luxembourgeois, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;

e) employer du personnel ayant des 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;

f) 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;

g) 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;

h) 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, en pouvant contracter une assurance appropriée;

i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai de vingt 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;

j) 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;

k) cet annuaire est constitué par 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.

Cet article transpose fidèlement l'annexe II de la directive sur les signatures électroniques, elle se rapporte aux exigences concernant les prestataires de service de certification délivrant des certificats qualifiés.

Par exemple, le prestataire de service de certification a l'obligation de conserver un annuaire électronique qui énumère au moins:

– *les certificats délivrés (à l'exception de ceux pour lesquels le titulaire n'a pas accepté à la publication);*

– *le moment de leur expiration;*

– *le moment de leur suspension ou de leur révocation.*

Un prestataire de service de certification peut s'imposer des obligations plus strictes que les exigences légales. Dans ce cas, il inscrit sur le certificat qu'il atteste l'exactitude d'une ou plusieurs informations complémentaires. Le prestataire de service de certification engage alors sa responsabilité dans le cas où ces informations se révéleraient inexactes.

Art. 2.– ***Prestataires de service de certification accrédités***

Un prestataire de service de certification obtient et conserve l'accréditation aux conditions suivantes:

a) respecter les exigences fixées par ou en vertu de la présente loi et celles fixées par l'article 1er du présent règlement;

b) se conformer aux exigences de fiabilité technique arrêtées par règlement grand-ducal et précisées, le cas échéant par l'Autorité Nationale d'Accréditation;

c) présenter un plan de sécurité précis qui répond aux exigences fixées à l'alinéa b du présent règlement. Ce plan est examiné et vérifié par l'Autorité Nationale d'Accréditation;

d) se conformer aux conditions visant à assurer l'interopérabilité des systèmes de certification, en particulier l'interconnexion des registres de certificats; et à assurer l'échange de données indispensables entre les prestataires de certification accrédités;

e) disposer d'une gestion indépendante par rapport aux utilisateurs du service;

Cette disposition du e) est essentielle puisque le prestataire est le tiers qui garantit l'identité d'une personne, le titulaire du certificat.

f) souscrire une assurance couvrant sa responsabilité professionnelle;

g) respecter les normes minimales relatives à la confidentialité et à l'intégrité des informations procurées par le titulaire du certificat.

Sont visés aussi bien les prestataires accrédités que non accrédités.

L'article 2 mentionne des exigences propres aux prestataires accrédités ce qui leur fournit un label de qualité.

Palais de Luxembourg, le xx yy 2000

Pour le Grand-Duc:
Son Lieutenant-Représentant
HENRI
Grand-Duc Héritier

Le Ministre de l'Economie,
Henri GRETHEN

*

REGLEMENT GRAND-DUCAL
(PROCEDURE, SUSPENSION ET RETRAIT DE L'ACCREDITATION)

Règlement grand-ducal du xx yy 2000 concernant l'exécution de l'article 31 de la loi du xx yy 2000 relatif au commerce électronique modifiant le code civil, le nouveau code de procédure civile et le code de commerce et transposant certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers et la directive 93/13/CEE concernant les clauses abusives dans les contrats conclus avec les consommateurs

Nous JEAN, par la grâce de Dieu, Grand-Duc de Luxembourg, Duc de Nassau;

Vu la loi du xx yy 2000 relatif au commerce électronique modifiant le Code civil, le Nouveau code de procédure civile et le Code de commerce et transposant certaines dispositions de la directive 97/7/CEE concernant la protection des consommateurs en matière de contrats à distance et de la directive 93/13/CEE concernant les clauses abusives et notamment son article 38 § 2,

Vu l'avis de la Chambre de Commerce;

Notre Conseil d'Etat entendu;

Sur le rapport de notre Ministre de l'Economie et après délibération du Gouvernement en Conseil;

Arrêtons:

Art. 1.– ***De la procédure d'accréditation***

L'accréditation est délivrée aux prestataires de service de certification sur demande écrite et après instructions portant sur les conditions exigées par la présente loi.

La durée de l'accréditation est de [2, 3, 5 … ans].

La demande de l'accréditation doit être accompagnée de tous les renseignements nécessaire à son appréciation.

Une accréditation est de même requise avant toute modification des services de certification offerts ou d'un élément de certificats délivrés.

La décision prise par l'Autorité Nationale d'Accréditation et de Surveillance sur une demande d'accréditation doit être motivée et notifiée au demandeur dans les (six) mois de la réception de la demande ou, si celle-ci est incomplète, dans les (six) mois de la réception des renseignements nécessaires à la décision. Il est en tout cas statué dans les (douze) mois de la réception des renseignements nécessaires à la demande, faute de quoi l'absence de décision équivaut à la notification d'une décision de refus. La décision peut être déférée, dans un délai d'(un) mois sous peine de forclusion, au tribunal administratif, qui statue comme juge de fond.

Art. 2.– ***De la suspension et du retrait de l'accréditation***

L'Autorité Nationale d'Accréditation et de Surveillance qui constate qu'un prestataire de service de certification accrédité ne se conforme pas aux conditions et obligations qui s'imposent à lui octroie un délai pour régulariser sa situation.

Si, au terme de ce délai, le prestataire de service de certification accrédité ne s'est pas conformée aux conditions et obligations prescrites, l'Autorité Nationale d'Accréditation et de Surveillance, procède à la suspension ou au retrait de l'accréditation.

Le prestataire de service de certification est tenu de mentionner, dans le registre qu'il tient, conformément à l'article 23, la suspension ou le retrait de son accréditation et d'en informer sans délais les titulaires de certificats délivrés par lui.

L'Autorité Nationale d'Accréditation et de Surveillance étant chargée de la surveillance des prestataires de service de certification accrédités, il est nécessaire de lui procurer les moyens d'agir dans les cas où elle constate le non-respect des conditions et obligations prescrites par ou en vertu de la loi.

Le cas échéant, elle commence par mettre en demeure le prestataire de service de certification de se conformer à ses obligations.

Si, au terme d'un délai, fixé discrétionnairement par l'Autorité Nationale d'Accréditation et de Surveillance en fonction du cas d'espèce, le prestataire de service de certification n'a pas rétabli sa situation, l'Autorité Nationale d'Accréditation et de Surveillance procède à la suspension ou au retrait de l'accréditation.

Dans ce cas, le prestataire de service de certification est tenu de mentionner, dans le registre électronique, la suspension ou le retrait de son accréditation et d'en informer sans délai les titulaires de certificats délivrés par lui.

Pour éviter tout préjudice aux titulaires de certificat, l'Autorité Nationale d'Accréditation et de Surveillance devrait pouvoir ordonner au prestataire de service de certification la suspension voire la révocation de certificats lorsque soit le processus de délivrance et de conservation des certificats ne satisfait pas à un niveau de sécurité adéquat soit la non-conformité par le prestataire de service de certification accrédité à ses obligations compromet la fiabilité des certificats.

Palais de Luxembourg, le xx yy 2000

Pour le Grand-Duc:
Son Lieutenant-Représentant
HENRI
Grand-Duc Héritier

Le Ministre de l'Economie,
Henri GRETHEN