

N° 4735⁹

CHAMBRE DES DEPUTES

Session ordinaire 2001-2002

PROJET DE LOI**relatif à la protection des personnes à l'égard du traitement
des données à caractère personnel**

* * *

AVIS DE LA CHAMBRE DE COMMERCE**DEPECHE DU MINISTRE AUX RELATIONS AVEC LE PARLEMENT
AU PRESIDENT DE LA CHAMBRE DES DEPUTES**

(19.6.2002)

Monsieur le Président,

A la demande du Ministre délégué aux Communications, j'ai l'honneur de vous faire parvenir en annexe *l'avis de la Chambre de Commerce* sur le projet de loi sous rubrique.

Veuillez agréer, Monsieur le Président, l'assurance de ma haute considération.

*Pour le Ministre aux Relations
avec le Parlement,*

Daniel ANDRICH

Conseiller de Gouvernement 1re classe

*

AVIS DE LA CHAMBRE DE COMMERCE

(13.2.2002)

Par sa lettre du 15 décembre 2000, Monsieur le Ministre délégué aux Communications a bien voulu saisir la Chambre de Commerce pour avis du projet de loi sous rubrique.

Le présent projet de loi a pour objet de transposer la directive 95/46/CE du Parlement européen et du Conseil 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 est amené à remplacer l'actuelle loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, telle que modifiée. Il est à noter que les Etats membres avaient jusqu'au 24 octobre 1998 pour transposer ladite directive. Le Luxembourg a été condamné par la Cour de Justice des Communautés Européennes par un arrêt du 4 octobre 2001, suite à un recours en manquement introduit en décembre 2000. Il y a donc urgence à adopter une nouvelle loi en matière de protection des données, non seulement pour se conformer au droit communautaire, mais également du fait que la loi du 31 mars 1979 est devenue largement obsolète.

1. Considérations générales et introductives

Le développement de l'économie numérique va de pair avec une croissance des mouvements et échanges internationaux de données de toutes sortes, dont notamment les données à caractère personnel. Standards ouverts et le caractère global des réseaux permettent et facilitent la transmission des données en les mettant ainsi à la disposition de tout le monde. Il y a aujourd'hui un consensus général à considé-

rer que la croissance et le développement de la société de l'information, et avec elle du commerce électronique, est largement tributaire du niveau de protection réservé aux données en circulation. Une réglementation au niveau mondial s'impose dès lors au vu de la mondialisation des réseaux et de la libre circulation des données.

Alors que la protection des données à caractère personnel faisait traditionnellement l'objet d'une réglementation juridique afin de protéger la sphère de l'intimité de l'individu, les données à caractère personnel ont aujourd'hui tendance à être considérées comme étant une marchandise et revêtant une certaine valeur marchande. Cette tendance est nettement plus exprimée de l'autre côté de l'Atlantique et s'imposera au fur et à mesure de la mondialisation des échanges commerciaux par les réseaux. Dès lors, toute réglementation en la matière constituera nécessairement une tentative de conciliation entre le respect des droits et libertés fondamentaux des individus d'une part, et les intérêts commerciaux internationaux d'autre part.

A première vue, la directive 95/46/CE, et avec elle le projet de loi No 4735, semblent ainsi être en opposition à l'atmosphère générale du monde développé qui tend vers plus de transparence, d'ouverture et de communication et où s'établit une culture du tout-connaître, voire du tout-publier.

Ce climat de transparence est très largement influencé par la mentalité anglo-saxonne qui se veut plus ouverte et qui considère que celui qui n'a rien à se reprocher n'a rien non plus à cacher. Les moyens informatiques modernes ont donné aux adeptes de la transparence les moyens techniques de leur ambition. Que ce soient les Etats, que ce soient les médias, que ce soit le monde commercial, tous entendent profiter de ce climat de transparence pour y établir leurs intérêts de pouvoir et d'argent. A cet égard, le secteur financier luxembourgeois, par exemple, est bien placé pour constater que le droit fondamental à la discrétion et au secret est attaqué de toutes parts. Le droit au secret, le droit à l'intimité privée, le droit de se taire sont des droits qui s'apprêtent à céder le pas.

Dans la discussion publique des objectifs contradictoires se distinguent:

- la transparence serait une vertu en soi; l'individu aurait à céder devant une multitude de causes, comme:
 - la liberté de la presse dans un univers médiatisé à l'extrême, le droit à l'information, le droit d'être informé,
 - la lutte contre le crime international et organisé, plus généralement, la sécurité des hommes et des biens qui appelle une internationalisation de la justice et des moyens d'enquête,
 - l'égalité du citoyen devant l'impôt,
 - la gestion informatique du service public,
 - plus généralement le traitement de masse de tous les bienfaits d'une société de consommation.
- Parallèlement, la protection de la vie privée et des droits de l'homme en général, la protection des données nominatives ou encore la protection des droits de l'individu en face d'une administration toute-puissante sont des sujets d'actualité. Il est admis qu'un Etat de droit digne de ce qualificatif doit une protection renforcée à l'individu devant la curiosité publique. La directive prétend répondre à cette aspiration.

Dans le souci de bien faire, les législateurs européens ont une nette tendance à prendre résolument les deux directions à la fois. De plus en plus, le monde politique demande de la transparence; de plus en plus aussi il tente également de protéger l'individu. Cette contradiction peut se retrouver parfois dans un seul et même texte de loi. Le secteur financier en constitue un exemple flagrant:

- Les données secrètes des clients de banques sont accessibles aux autorités de contrôle ou à d'autres organismes investis d'une mission publique, mais ceux-ci sont alors soumis à un même secret. Ces autorités peuvent quelquefois partager les données recueillies avec leurs homologues étrangers, là encore sous la condition que ceux-ci soient soumis à un secret équivalent, et ainsi de suite. En fin de compte, on se demande si on n'aboutit pas dans un système où tout le monde a le droit de tout savoir à condition de le tenir secret.
- On demande aux banques d'indiquer à chaque paiement toutes les données permettant une identification des donneurs d'ordres et des bénéficiaires concernés. La Commission européenne de son côté veut imposer aux banques une protection accrue de ses mêmes données tout en exigeant par ailleurs une accélération des paiements des virements transfrontaliers.

- L'Europe s'apprête à collecter les données sur les intérêts de l'épargne de centaines de millions de citoyens, à les traiter par ordinateur, à les envoyer vers d'autres ordinateurs, pour contrôler, enquêter, interconnecter.

Les défenseurs d'une idée de protection de la vie privée et aussi de protection du traitement des données nominatives semblent bien perdus dans ce climat. Par la directive 95/46/CE, les décideurs politiques européens ont voulu donner l'impression d'attacher encore une importance à cette idée. Ils ne sont cependant pas crédibles dans leur démarche alors qu'ils font tout par ailleurs pour organiser la transmission de données au-delà des frontières et au-delà des organisations. Ainsi, la directive apparaît comme l'alibi politique en face d'un droit qui disparaît, et non pas comme une tentative d'endiguer la tendance. Que ceux qui voudraient croire que la future législation sur le traitement des données va donner au citoyen des garanties se détrompent. Elle va au contraire rendre impossible d'opposer aux autorités des Etats qui réclament des données toutes considérations de protection fondées sur le droit national.

En cas de doute, la crainte diffuse devant ces orientations est combattue par les Etats avec une nette tendance des Etats à se faire confiance tout en se méfiant des opérateurs privés et commerciaux. Le même phénomène se manifeste dans le projet de loi sous avis qui admet des exceptions, p. ex. au droit à l'information des personnes concernées, en faveur de la poursuite des infractions, de la sûreté de l'Etat, de la défense et de la sécurité publique. En d'autres termes, l'Etat se considère au-dessus des soupçons qui lui semblent néanmoins justifiés vis-à-vis des entreprises. Si le texte prend garde de ne jamais s'appliquer lorsque les domaines sensibles de l'Etat et donc les libertés publiques sont concernés, il établit par contre une foule de chicanes pour les organisations privées. Une charge administrative considérable attend les entreprises dont on soupçonne l'abus permanent et systématique lorsqu'ils traitent les données personnelles dont ils disposent. Des peines pénales excessives viennent frapper ceux qui négligent la moindre des innombrables procédures prescrites. Si on doit comprendre la nécessité objective des traitements de données par l'Etat dans certains domaines sensibles, on doit tout de même regretter que ce pragmatisme fasse défaut par ailleurs. Ceci d'autant plus que le danger informatique, s'il existe, ne vient pas des opérateurs privés. Ils sont certes en mesure de causer un dommage par l'utilisation et la propagation de données fausses ou simplement privées, ils ne représentent pas pour autant une menace pour les libertés publiques.

Il serait illusoire de penser que le Luxembourg puisse renverser les tendances à cet égard. Les commentaires de la Chambre de Commerce qui suivent se veulent dès lors de rester constructifs dans une matière qui est largement technique et qui est de toute façon dictée par le droit européen. Il convient cependant de ne pas se voiler la face sur la direction que prennent les choses et de rappeler que cette loi se lira plus utilement en gardant à l'esprit les domaines de la vie privée qui s'effritent et que ce texte ne peut ni ne veut protéger.

2. Une transposition tardive et incomplète des directives communautaires

Il est à noter que la directive 97/66/CE du 15 décembre 1997, qui est venue compléter les dispositions de la directive 95/46/CE en ce qui concerne plus particulièrement le secteur des télécommunications, aurait dû être transposée avant le 24 octobre 1998. Le présent projet de loi aurait pu être l'occasion de transposer les deux directives communautaires. Par ailleurs, le contenu de la proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques aurait de même pu être pris en considération dans la mesure où ce texte reprend les dispositions de la directive 97/66/CE en les appliquant au secteur des communications électroniques.

Alors que le Luxembourg entend se présenter comme une plate-forme internationale en matière de commerce électronique et s'est doté à cette fin d'une loi-cadre en ce domaine, aucune disposition du projet de loi ne vise spécifiquement la protection des données personnelles dans le cadre de l'utilisation de techniques de communications électroniques. Il est à noter à cet égard que l'avant-projet de loi sur le commerce électronique comportait un chapitre spécifique à la protection des données personnelles qui visait notamment à transposer certaines dispositions de la directive 97/66/CE en droit luxembourgeois dans ses aspects liés au commerce électronique. La Chambre de Commerce a dû assister au démantèlement de cet avant-projet de loi et en particulier au retrait du chapitre relatif à la protection des données. Pourtant, les auteurs de ce projet de loi se proposaient de traiter cette partie du texte dans la future loi relative à la protection des données personnelles. Il s'avère toutefois qu'il n'en est rien. Le Conseil

d'Etat, dans son avis du 2 mai 2000 (Doc. parl. No 4641¹, pp. 2-3), avait néanmoins insisté pour que les lacunes de la loi relative au commerce électronique soient comblées le plus rapidement possible. Il est à souligner que les violations de la vie privée sont la crainte majeure des utilisateurs d'Internet et que cette crainte constitue un important obstacle au développement du commerce électronique. Bien que l'exposé des motifs précise que le projet de loi vient compléter la loi sur le commerce électronique et ainsi parfaire le „dispositif de sécurisation juridique“ du commerce électronique, le présent texte ne contient aucune disposition relative à la confidentialité des communications ou aux obligations des fournisseurs de service de communication électronique lors de la transmission de données. Il est précisé dans l'exposé des motifs (Doc. parl. No 4735, p. 86) que ces aspects essentiels en matière de commerce électronique devront faire l'objet d'un règlement grand-ducal. La Chambre de Commerce estime que des dispositions aussi fondamentales auraient leur place dans une loi plutôt que dans un règlement grand-ducal et que la loi adéquate reste celle relative au commerce électronique.

3. Un champ d'application imprécis

Il est indéniable que l'évolution de l'utilisation des ordinateurs dans les années 90 n'était en rien prévue lors de la rédaction de la loi de 1979. Les dispositions de cette loi sont aujourd'hui devenues difficilement applicables et largement inappliquées. Le décalage actuel de la loi de 1979 par rapport à la réalité est à garder en mémoire afin d'éviter, dans un nouveau texte, de renouveler les mêmes erreurs. Or le projet, du fait de son champ d'application extrêmement large qui tend à couvrir toutes les situations de traitement possibles, risque d'être tout aussi difficilement applicable que le texte actuel. De plus, il semble aux yeux de la Chambre de Commerce qu'un certain nombre de dispositions soit difficilement compatible avec certaines activités du secteur financier notamment.

3.1. Des définitions trop extensives

Le champ d'application du projet de loi est déterminé en son article 3, qui est repris de l'article 3 de la directive communautaire. Ce dernier est à lire en relation avec l'exposé des motifs de la directive qui précise que les traitements portant sur des données relatives aux personnes physiques ne sont couverts par la directive „que s'ils sont automatisés ou si les données sur lesquels ils portent sont contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause“. Même si le traitement manuel des données personnelles y est visé, il est précisé que „les dossiers ou ensembles de dossiers qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application“ de la directive. Cette précision est à mettre en rapport avec le champ d'application du projet de loi tel qu'il ressort des définitions qui figurent à l'article 2. Si la définition du concept de „traitement de données à caractère personnel“ est strictement repris de la directive 95/46/CE, il n'en est pas de même de la notion de „fichier de données à caractère personnel“ qui est défini comme „tout ensemble structuré ou non de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique“. Une telle définition tend notamment à s'appliquer à tout dossier ouvert et tenu par une entreprise en contact avec son client. Il en est de même pour les dossiers ouverts pour chaque salarié et tenus dans les départements des ressources humaines et services de personnel des entreprises. Il serait en effet inconcevable qu'un salarié ait accès par exemple à des notes confidentielles contenues dans son dossier, et encore moins qu'il ait un droit de rectification concernant de telles notes. Le caractère excessif de cet écart par rapport à la directive vient surtout du fait que le champ d'application du texte dépasse les applications purement informatiques, contrairement à la loi luxembourgeoise actuelle.

La combinaison de la définition de la notion de „fichier“ avec l'obligation d'autorisation préalable pour ce qui est du traitement concernant le crédit et la solvabilité des personnes concernées, visé à l'article 14 du projet de loi, conduit à ce que l'une des activités principales du banquier soit soumise à l'autorisation préalable de la Commission Nationale pour la Protection des Données. Cela ne peut pas être la volonté du législateur. Il est permis d'ajouter à ce sujet qu'une telle autorisation préalable, s'appliquant aux établissements de crédit, est incompatible avec le principe, énoncé tant dans la directive 95/46/CE qu'à l'article 5 du projet de loi, selon lequel le traitement de données à caractère personnel est légitime, en particulier lorsqu'il est nécessaire à la conclusion ou à l'exécution d'un contrat liant la personne concernée. Or la légitimité, précise l'exposé des motifs du projet de loi, „est ce qui fonde un

responsable de traitement à agir en tant que tel“. Dès lors que le traitement est légitime, aucune autorisation préalable ne devrait en toute logique être requise.

En conséquence, la Chambre de Commerce demande instamment à ce que, d'une part, la définition du terme „*fichier*“ ne couvre que les „*ensembles structurés de données*“ et que soient donc supprimés les mots „*ou non*“ de cette définition, de telle sorte que la constitution de simples dossiers soit exclue du champ d'application du texte, conformément à la directive 95/46/CE, et que, d'autre part, l'obligation d'autorisation préalable pour ce qui est du traitement concernant le crédit et la solvabilité des personnes concernées, visé à l'article 14 du projet de loi, ne concerne que les personnes dont le métier n'est pas d'octroyer des crédits.

Par ailleurs, le commentaire des articles parle de traitements concernant spécialement le crédit et la solvabilité, quelle que soit la profession en cause (banque, assurances ou autres professionnels du secteur financier). Selon les auteurs du projet de loi, de tels traitements conditionnent l'accès au contrat et devront donc être soumis à autorisation préalable.

En ce qui concerne les traitements en matière d'assurance, la Chambre de Commerce comprend mal quels traitements seraient visés (alors que l'assureur ne s'intéresse normalement pas au crédit et à la solvabilité des clients). La Chambre de Commerce demande par conséquent que la référence à l'assurance soit supprimée dans le commentaire afférent à l'article précité.

L'article 2 (a) définit les données à caractère personnel comme étant „*toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (...)*“. Toutefois, la notion de données à caractère personnel telle que définie dans la directive ne comprend ni le son, ni les images comme information concernant une personne. Il en va de même des dispositions concernant la surveillance, définie à l'article 2 (h) et réglementée à l'article 10 du projet de loi sous rubrique. La directive n'entend nullement régler l'activité de surveillance. La Chambre de Commerce est d'avis qu'une telle réglementation n'a pas non plus sa place dans un projet de loi destiné à constituer un cadre légal pour l'utilisation des données à caractère personnel.

Pour autant que le projet de loi sous analyse devrait continuer à régir ces activités de surveillance, la Chambre de Commerce voudrait remarquer qu'elle s'oppose à ce qu'un traitement à des fins de surveillance sur le lieu de travail, tel que prévu à l'article 11 du projet de loi, soit soumis à une autorisation préalable de la Commission (article 14 (1) du projet de loi) et que cette autorisation soit subordonnée à l'avis préalable de l'Inspection du Travail et des Mines (article 14 (2) du projet de loi). On tente ici de réintroduire en catimini le système de l'autorisation préalable, système qui a pourtant fait la preuve de ses faiblesses. La Chambre de Commerce est en effet d'avis qu'une telle surveillance, plutôt que de restreindre un prétendu droit à la vie privée sur le lieu de travail, permet aux entreprises d'honorer pleinement les obligations qui leur incombent sur base de la législation sur la sécurité et la santé au lieu de travail et ceci surtout lorsqu'il s'agit de postes de travail individuels et à haut risque. Il s'y ajoute que, compte tenu du fait de la propagation des nouvelles technologies de l'information et de la communication au sein des entreprises et de leur usage facile, la tentation d'utiliser ces technologies à des fins privées est un risque réel pour l'entreprise. La submersion du poste de travail du salarié par un flot de courriers électroniques privés se traduit évidemment par une perte de la capacité de stockage du matériel informatique qui est d'autant plus importante que les courriers en question contiennent souvent des annexes exubérantes en *bits* et, en conséquence, gourmandes d'espace de mémoire. Toutefois, et c'est là le problème majeur, la consultation des courriers électroniques reçus et l'envoi de tels courriers par le salarié prend un certain temps qui va évidemment au dépens de l'employeur, alors qu'il s'agit de temps de travail rémunéré. Finalement, il ne faut pas oublier que l'envoi de courrier électronique génère des coûts téléphoniques. La Chambre de Commerce est dès lors d'avis qu'il convient de mettre les employeurs en mesure de recourir à des techniques de surveillance, sans qu'ils aient besoin pour cela d'avoir l'accord préalable du salarié, ni d'une quelconque autre instance ou autorité. Aux yeux de la Chambre de Commerce, une simple information à cet égard à l'adresse du salarié devrait suffire.

3.2. Des situations ambiguës

L'article 11 prévoit la surveillance sur le lieu de travail. Aux termes dudit article un tel contrôle n'est autorisé que s'il est temporaire (article 11 point 1 du projet de loi). A cet égard, la Chambre de Commerce s'interroge si cette condition est compatible avec le contrôle effectué dans le cadre d'un système d'horaire mobile.

4. La spécificité de certains types de données

4.1. La spécificité de certaines informations traitées par les banques

La Chambre de Commerce souhaite attirer l'attention des auteurs du projet de loi sur la spécificité de certaines informations traitées par les banques. Dans le cadre de la lutte contre le blanchiment, les banques sont tenues, en vertu de l'article 39 (2) et (4) de la loi du 5 avril 1993 sur le secteur financier, d'identifier non seulement leurs clients mais également les personnes avec lesquelles elles effectuent des transactions à titre occasionnel dès lors qu'il existe un soupçon de blanchiment. Les banques sont tenues de conserver les données relatives à ces personnes pendant une durée de cinq années à compter de l'exécution de la transaction. Quand bien même la banque se serait abstenue d'effectuer une transaction en raison de soupçons de blanchiment, il est plus qu'opportun qu'elle retienne les données relatives à ces personnes sans que celles-ci soient obligatoirement informées du traitement dont elles font l'objet.

Une logique similaire opère au regard de la lutte contre la corruption et le détournement de fonds publics, au titre de laquelle la Commission de surveillance du secteur financier, dans sa circulaire No 2000/21, impose aux banques „d'instaurer des procédures de contrôle particulières, afin de s'entourer de toutes les garanties nécessaires“ dans leurs relations „avec des personnes exerçant des fonctions publiques importantes dans un Etat ou des personnes et sociétés qui, de manière reconnaissable, leur sont proches ou leur sont liées“. Il est parfaitement légitime, sinon légalement requis, que les banques constituent, pour ce faire, des fichiers de personnes à risque, voire indésirables. Ces fichiers peuvent aussi bien contenir les noms de personnes avec lesquelles la banque a pu être en contact que ceux de personnes avec lesquelles elle ne souhaite pas ou n'est pas en droit d'établir de relations. Il peut par exemple s'agir des personnes à l'encontre desquelles il existe des mesures restrictives ou d'autres personnes faisant l'objet de sanctions au titre de la politique étrangère et de sécurité commune de l'Union européenne.

L'existence même de ces fichiers, indispensables au bon fonctionnement des établissements de crédit, ne doit pas être mise en péril par le droit, prévu à l'article 26 du projet de loi, des personnes concernées à être informées. Au regard de la lutte contre le blanchiment, y compris la corruption, la Chambre de Commerce considère que la collecte des données entre logiquement dans le champ d'application des exceptions au droit à l'information prévues à l'article 27 (1) du projet de loi sous examen, au titre de „la prévention, la recherche, la constatation et la poursuite d'infractions pénales“.

4.2. Les fichiers „fraude“ dans le secteur des assurances

Conformément aux dispositions de la Directive 95/46, l'article 5 du projet de loi prévoit différentes conditions, en application desquelles un traitement portant sur des données à caractère personnel est considéré comme légitime. Ces conditions viennent remplacer l'unique condition de licéité jadis retenue par la loi du 31 mars 1979, à savoir l'autorisation préalable de toute création et exploitation d'une banque de données.

La Chambre de Commerce est d'avis que la condition de licéité tenant à l'intérêt légitime devrait également pouvoir servir de base à la mise en place d'un fichier fraude. La lutte contre la fraude à l'assurance poursuit certainement un but légitime. La fraude a inévitablement des répercussions sur le niveau des primes d'assurance et pénalise ainsi la très grande majorité des assurés non fraudeurs.

La Chambre de Commerce rappelle à cet égard les inquiétudes du secteur des assurances au sujet des chiffres relatifs au phénomène de la fraude à l'assurance. Le Grand-Duché de Luxembourg est en retrait par rapport à ses voisins étrangers en ce qui concerne les moyens législatifs disponibles pour combattre de façon convenable ce problème.

En effet, la plupart de nos pays voisins (dont notamment la Belgique et l'Allemagne – pays pourtant bien connu pour ses susceptibilités en cette matière) ont mis en place des fichiers centraux performants, basés sur des informations nominatives, qui permettent de lutter efficacement contre le fléau de la fraude à l'assurance, coûtant en définitive très cher à la grande majorité des assurés.

Malheureusement, notre législation sur la protection des données nominatives ne permet pas, dans sa teneur actuelle, de recourir à de tels dispositifs informatiques. En l'absence d'adaptation de ladite législation, le secteur des assurances restera démuné face à la réalité de la fraude à l'assurance.

Il s'y ajoute que la fraude à l'assurance revêt une dimension de plus en plus internationale, notamment à travers le phénomène de la criminalité organisée sévissant dans plusieurs pays, ce qui rend indispensable une coopération internationale efficace à laquelle le secteur des assurances luxembourgeois doit malheureusement rester à l'écart du fait que le cadre légal ne permet pas la mise en place des applications informatiques appropriées.

4.3. Le défaut d'exclusion concernant les données à caractère public

Aux yeux de la Chambre de Commerce, le texte projeté comporte une lacune majeure dans la mesure où il omet de distinguer entre les données à caractère privé et celles à caractère public. Il est légitime que les premières soient protégées. En revanche, le caractère public des secondes devrait autoriser un traitement libre de celles-ci.

- Il peut s'agir de données manifestement publiques, telles que les informations connues de tous au sujet des personnalités célèbres. Ces données sont effectivement visées à l'article 6 (2) (e) du projet de loi qui prévoit une exception à l'interdiction du traitement de certaines catégories particulières de données.
- Il peut par ailleurs s'agir de données rendues publiques par la personne concernée elle-même. Ainsi les données figurant dans un annuaire téléphonique national devraient-elles légitimer la constitution de fichiers et la préparation de correspondance par les machines de traitement de texte.
- Il peut s'agir enfin des données rendues publiques par l'autorité publique. Il en est ainsi, à titre d'exemple, des listes de faillites ou des listes des établissements de crédit établies par la Commission de surveillance du secteur financier.

La Chambre de Commerce soutient vivement que de telles données publiques devraient être traitées différemment des données à caractère privé recueillies auprès de la personne concernée. Il est à noter à cet égard que la directive 95/46/CE vise uniquement la protection des données concernant les personnes physiques et n'impose donc aucune obligation relative au traitement des données concernant des personnes morales. Or, la protection des personnes morales par rapport aux traitements de données, prévue par le projet de loi, a pour corollaire un certain nombre d'obligations à charge des responsables de traitement. Ce sont précisément ces obligations qui sont en décalage par rapport au caractère public de certaines informations relatives aux personnes morales. C'est pour cette raison que la Chambre de Commerce plaide pour une exclusion des données publiques concernant des personnes morales du champ d'application du texte. Il est rendu attentif à cet égard à la définition très large du terme „*traitement*“ qui peut inclure des envois par télécopie ou l'utilisation de machines de traitement de texte.

4.4. L'extension du champ d'application aux activités relevant de l'Etat

Le champ d'application du texte s'étend également, selon les termes de l'article 3 (5) au traitement ayant pour objet la sécurité publique, la défense, les activités relatives à des domaines du droit pénal, la sûreté de l'Etat ou le bien-être économique de l'Etat lorsque celui-ci est lié à la sûreté de l'Etat. L'article 17 du projet de loi prévoit parallèlement que les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique feront l'objet d'un règlement grand-ducal.

Si donc les dispositions impératives du texte s'imposent aussi à l'Etat, il est à observer que les multiples limitations et dérogations prévues laissent douter de la volonté des auteurs de réellement soumettre les services de l'Etat à l'ensemble des obligations prévues. L'application aux administrations étatiques semble faite pour leur permettre de légitimer certaines actions et non pas pour leur imposer de nouvelles obligations. Cette réalité est flagrante en ce qui concerne les droits les plus importants dont bénéficient les personnes concernées par un traitement. Ainsi la sauvegarde de la sûreté de l'Etat, de la défense ou de la sécurité publique justifient-elles des dérogations aux obligations relatives au droit à l'information de la personne concernée (article 27 du projet de loi) et au droit d'accès aux données la concernant (article 29 du projet de loi). De plus, la sauvegarde d'un „*intérêt économique ou financier important de l'Etat, en particulier dans les domaines monétaire, budgétaire et fiscal*“ justifie l'absence de droit d'information des personnes concernées. Sur cette base, l'Etat pourrait ainsi refuser tout droit d'information aux administrés en ce qui concerne les données collectées à des fins d'imposition. La Chambre de Commerce considère qu'une telle prérogative est exorbitante. Elle l'est d'autant plus que l'harmonisation européenne du traitement des données va rendre impossible d'opposer des arguments de protection de la vie privée à la curiosité transfrontalière d'autres Etats européens.

5. Des sanctions disproportionnées et trop nombreuses

Le champ d'application extrêmement large du projet de loi est à mettre en relation avec les sanctions qui sont attachées à tout manquement aux obligations qui y figurent. La grande sévérité des peines apparaît comme disproportionnée par rapport aux faits incriminés. Ainsi, le fait d'avoir omis d'informer une personne après avoir, par exemple, relevé son numéro de téléphone et son adresse est punissable d'une peine d'emprisonnement de un an et d'une amende de 5.000.000 LUF. Une telle disproportion entre la gravité des actes et la lourdeur des peines encourues est d'autant plus contestable que le projet de loi ne prend aucunement en compte l'élément moral de l'infraction. Ainsi, celui qui a omis de se conformer à la loi par simple négligence sera punissable comme celui qui s'est sciemment soustrait aux obligations qui y sont imposées. La Chambre de Commerce réclame que les peines soient revues à la baisse et adaptées à la gravité des faits et que le mot „*sciemment*“ soit ajouté à un certain nombre de dispositions d'ordre pénal qui figurent dans le projet de loi, en particulier aux articles 5 (2) et 26 (4). La Chambre de Commerce estime que, dans les hypothèses les moins graves, les sanctions administratives prévues à l'article 35 du projet de loi sous analyse sont suffisantes.

Dans ce contexte, la Chambre de Commerce voudrait également rendre attentif à l'article 23 (h) qui exige que les mesures relatives à la sécurité des traitements doivent „*empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée*“. On impose ici au responsable du traitement une obligation qui est hors de son rayon de contrôle et d'influence, obligation qui est pourtant sanctionnée par une disposition pénale.

Par ailleurs, la Chambre de Commerce est d'avis que le nombre de sanctions pénales est démesuré et que leur dispersion devrait faire l'objet d'un regroupement dans un chapitre intitulé „Dispositions pénales“.

Il est à remarquer que les montants devraient désormais être indiqués en euros et non plus en francs luxembourgeois.

6. L'interconnexion, un danger pour la vie privée

L'interconnexion est conçue par le projet de loi comme „*la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par d'autres responsables de traitement*“. La Chambre de Commerce se demande si le concept même „*d'interconnexion*“ tel que défini dans le projet est compatible avec les droits des personnes concernées. La directive 95/46/CE précise que „*les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine*“. L'exposé des motifs du projet de loi précise certes que le principe de finalité est le principe fondateur du texte et „*qu'il ne serait pas opportun d'ouvrir, par le biais de l'interconnexion, une brèche dans ce principe fondamental*“. Toutefois, à peine le principe de finalité réaffirmé, l'exposé des motifs s'empresse de l'écarter expressément puisqu'il est précisé que la notion d'interconnexion couvre „*la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité*“. L'interconnexion ainsi définie apparaît quelque peu contraire aux principes énoncés par la directive. Il est à rappeler à cet égard que l'article 6 (1) de la directive impose aux Etats membres de prévoir que les données à caractère personnel soient „*collectées pour des finalités déterminées, explicites et légitimes*“ et ne soient pas „*traitées ultérieurement de manière incompatible avec ces finalités*“.

Si l'article 16 soumet l'interconnexion à l'autorisation préalable de la Commission Nationale pour la Protection des Données, il est aussi fondamental que cette dernière vérifie la compatibilité des finalités des différents traitements. L'autorisation préalable ne doit pas être considérée comme une simple formalité.

Ainsi, l'interconnexion ne devrait être possible qu'à la condition que les finalités des différents fichiers soient compatibles entre elles. La Chambre de Commerce souhaite que le régime du secret professionnel auquel sont soumises certaines professions soit respecté et qu'ainsi il ne soit pas autorisé d'interconnecter des fichiers gérés par des personnes différentes, particulièrement lorsque celles-ci ne sont pas soumises au même régime de secret professionnel. Rien ne justifierait que les fichiers de l'administration fiscale et ceux de la sécurité sociale soient rapprochés. De même, il ne serait pas concevable que puissent être connectés les fichiers d'établissements de crédit différents. Il appartient, sinon à la loi, du moins à la Commission Nationale pour la Protection des Données d'y veiller.

Des raisonnements analogues doivent prévaloir en ce qui concerne la communication d'informations à des tiers.

Par ailleurs, en ce qui concerne la nécessité d'une autorisation préalable pour l'interconnexion de données à caractère personnel, la Chambre de Commerce rappelle que l'article 11 de la loi sur le contrat d'assurance relatif à l'obligation de déclaration, dispose que „*le preneur ne doit pas déclarer à l'assureur les circonstances déjà connues de celui-ci*“. Dans la pratique, afin de connaître les éléments déjà déclarés dans le cadre d'un autre contrat d'assurance auprès du même assureur, ce dernier sera obligé de procéder de façon quasi systématique à des interconnexions de fichiers (pour lesquelles il devra solliciter une autorisation).

De cette façon, la formule dérogatoire de l'autorisation préalable deviendrait le droit commun en matière d'assurance contrairement à l'objectif poursuivi par le législateur qui consiste à simplifier et à alléger la procédure.

7. Des dispositions difficilement applicables

7.1. La sécurité dans le secteur financier

En ce qui concerne les traitements à des fins de surveillance, la Chambre de Commerce voudrait faire remarquer que les banques effectuent une surveillance systématique par caméra-vidéo de leurs agences et lieux de distribution de billets de banque. Cette surveillance est effectuée dans un but de protection des personnes concernées ainsi que de prévention des infractions. Le projet de loi adopte à cet égard une attitude tout à fait réaliste en autorisant le traitement à des fins de surveillance dans tous les lieux accessibles au public et en particulier dans les banques. Toutefois, les conditions dans lesquelles celui-ci doit être mis en oeuvre sont par contre tout à fait irréalistes. Si le fait d'apposer des panneaux de signalisation est praticable dans les agences bancaires, l'obligation d'information prévue à l'article 26 du projet de loi est difficile, voire impossible à respecter. En effet, il ne sera pas possible aux banques de communiquer à toutes les personnes qui fréquentent une agence bancaire ou plus encore un simple guichet de retrait d'espèces, qui ne sont pas toujours des clients de la banque en question, les informations requises par l'article 26 du projet de loi. Par conséquent, la Chambre de Commerce demande que les termes „*sans préjudice du droit à l'information prévu à l'article 26*“ soient biffés au paragraphe 2 de l'article 10 du projet de loi. Il en est de même du paragraphe 4 de ce même article, qui réitère l'obligation d'information de l'article 26 du projet de loi.

7.2. La notification à la Commission

En ce qui concerne l'obligation de notification, la Chambre de Commerce considère que le traitement qui est fait par les banques quant aux données relatives à leurs clients constitue un traitement unique et n'est donc soumis qu'à une seule notification, même si les données sont par la suite réparties entre les différents services de la banque. En effet, d'une part, la collecte est le plus souvent réalisée au moment de l'entrée en relations d'affaires, et, d'autre part, même si l'information est relayée à l'intérieur de l'établissement, d'un service à un autre, elle a été collectée dans un but unique qui est l'exécution du contrat général de fourniture de services qui lie le client à sa banque. Ceci correspond d'ailleurs à la définition du terme „*fichier*“ qui vise tout ensemble de données, peu importe que cet ensemble soit ou non centralisé.

7.3. L'obligation de rectification et/ou de suppression des données

L'article 28 (5) du projet de loi analysé prévoit l'obligation pour le responsable du traitement de procéder à la rectification, l'effacement ou le verrouillage des données en raison de leur caractère incomplet ou inexact. Aux yeux de la Chambre de Commerce, une interprétation stricte de cette disposition conduirait à une contradiction entre cette obligation de rectification et l'obligation qui résulte de l'article 1334 du Code civil et du règlement grand-ducal du 22 décembre 1986 selon lesquels une copie fidèle consiste en une reproduction indélébile de l'original, protégée contre toute altération. Pour se conformer à ces textes, beaucoup d'entreprises mettent en place des procédures de conservation de leurs archives rendant impossible l'effacement ou la modification des données conservées sur certains supports.

Pour cette raison, la Chambre de Commerce prône une interprétation plus souple permettant aux responsables de traitement de satisfaire aux obligations de l'article 28 (5) du projet de loi sous analyse au moyen d'un ajout réalisé selon une méthode d'archivage identique au traitement antérieur et retraceable lors de la consultation.

7.4. Le droit d'opposition

Le droit d'opposition de la personne concernée par un traitement, prévu par l'article 30, est limité dans les hypothèses où le traitement est imposé en vertu de dispositions légales. La Chambre de Commerce attire l'attention sur le fait qu'en pratique, la très grande majorité des traitements tient à une exigence légale (tenue de comptabilité, exigences du droit du travail ou du droit fiscal, ...). A défaut de base légale pour un traitement, notamment en ce qui concerne les associations sans but lucratif privées, le juge devra alors faire la difficile appréciation de ce qui est une „raison prépondérante et légitime“.

7.5. Le droit à l'information

Le droit à l'information (article 26 du projet de loi sous examen) concrétise le principe de la bonne foi ou de la transparence du traitement de données à caractère personnel.

En matière d'assurances, la Chambre de Commerce se demande si, p. ex. concernant la gestion de sinistres, l'assureur qui propose une couverture de la responsabilité civile en matière automobile et qui reçoit des données relatives à la victime par un autre assureur, auprès duquel la victime est assurée, doit informer cette victime qu'il a enregistré des données la concernant. Il faut savoir que, de toute façon, et conformément à l'article 26 paragraphe (1) du projet de loi cette victime est déjà informée, au moment de la collecte, par son propre assureur, notamment en ce qui concerne les tiers ou catégories de tiers auxquels les données sont susceptibles d'être communiquées.

L'article 26 paragraphe (3) du projet de loi prévoit que l'information de la personne concernée (dans l'hypothèse où la collecte des données ne s'est pas faite auprès d'elle) n'est pas nécessaire si celle-ci a déjà été informée.

Dans le cas de figure décrit ci-dessus, la Chambre de Commerce estime que l'information donnée par l'assureur de la personne concernée devrait être considérée comme suffisante.

La solution contraire serait à l'origine d'une surcharge de travail considérable pour l'assureur sans apporter une protection supplémentaire à la personne concernée en raison du devoir d'information incombant déjà à son propre assureur. Une information multiple, abstraction faite du coût, ne fera qu'accentuer la méfiance du public vis-à-vis du traitement de données personnelles.

8. Un texte maladroît

Aux yeux de la Chambre de Commerce le texte dans sa teneur et sa présentation actuelle est à revoir. En effet, le texte dans sa version actuelle est indigeste et laisse le lecteur mal à l'aise, qui, intimidé par le nombre impressionnant de sanctions pénales, a des difficultés à se retrouver parmi les différentes dispositions et à se situer dans le cadre qui le concerne personnellement. Les nombreux renvois ne contribuent guère à un éclaircissement du justiciable et sont contraires au principe de droit pénal qui veut que seuls des textes clairs et limpides prévoient des sanctions.

Certaines dispositions traitent de cas de figure apparemment similaires, mais sont sanctionnées par des peines pénales différentes et parfois illogiques. La Chambre de Commerce renvoie à cet égard à l'article 12 (3) et (4) du projet de loi et s'interroge sur le sens de cette différence. Au vu de ces textes, la Chambre de Commerce se demande si un responsable de traitement ne préférera pas ne pas notifier, plutôt que de se voir exposer au risque d'avoir sciemment fourni des informations incomplètes ou inexacts et de courir ainsi le risque d'une peine de prison.

La même remarque vaut en ce qui concerne l'article 13 (4) du projet de loi sous analyse qui punit le non-respect des paragraphes 1er et 2 du même article. L'article 13 (1) énumère un certain nombre d'informations que doit comprendre la notification et l'article 13 (2) prescrit la notification de toute modification d'une de ces informations. La Chambre de Commerce ne saisit pas la différence entre l'infraction sanctionnée par l'article 13 (4) et celle punie par l'article 12 (3), respectivement 12 (4).

Par ailleurs, le texte contient un certain nombre de doubles emplois. Plus particulièrement, la Chambre de Commerce attire l'attention des auteurs du projet de loi à cet égard sur les articles 7 (2) et 14 (1) (a), ainsi que sur les articles 14 (1) (c) et 16 (1).

En ce qui concerne le traitement à des fins de surveillance sur le lieu de travail (article 11 du projet de loi), la Chambre de Commerce voudrait faire remarquer que l'emploi du mot „légitime“ à l'article 11 (1) *in fine*, n'est pas correct. Il faudrait en effet remplacer le mot „légitime“ par le mot „licite“, alors que le traitement mis en oeuvre devra de toute façon être légitime et rentrer dans un des six cas prévus par l'article 5 du projet de loi.

Certaines questions restent encore ouvertes. Ainsi, par exemple, concernant l'article 18 du projet de loi sous examen, la Chambre de Commerce s'interroge sur les pouvoirs réels de la Commission nationale. En effet, aux termes de l'article 25.6, deuxième alinéa, de la directive 95/46/CE, les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission européenne lorsque celle-ci constate qu'un pays tiers assure un niveau de protection adéquat en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes. En d'autres termes, un tel constat de la part de la Commission européenne du niveau adéquat lie les Etats membres. Une telle obligation de la part des Etats membres ne ressort pas clairement du projet de loi et la Chambre de Commerce se pose en conséquence la question quelle est la marge de manoeuvre des commissions nationales.

En ce qui concerne ce même article 18, la Chambre de Commerce aimerait préciser qu'il y a lieu d'ajouter le bout de phrase „ou destinées à faire l'objet d'un traitement“ au paragraphe (1) après le début de phrase „Le transfert de données faisant l'objet d'un traitement ...“.

Finalement, il y a lieu de reformuler l'article 24 (3) du projet de loi comme suit: „Le prestataire de service de certification ne peut opposer à la Commission le secret professionnel auquel il est soumis conformément à l'article 19 de la loi du 14 août 2000 relative au commerce électronique“, terme consacré par l'article 72 de ladite loi.

9. Conclusion

Il est clair que les Etats européens n'ont qu'une faible marge de manoeuvre en ce qui concerne la transposition de la directive 95/46/CE. Le Luxembourg se doit de ce fait de respecter les principes de base de cette directive. En particulier, le principe de finalité est, dans l'optique communautaire, à la base de la protection des personnes à l'égard des traitements de données. La Chambre de Commerce se permet de souligner à cet égard que l'interconnexion des fichiers ne doit pas permettre d'introduire une brèche dans ce principe.

Une interprétation stricte des dispositions du projet de loi dans sa version actuelle conduit vers une situation telle que tout rassemblement de données quelconques, si anodines soient-elles, et tout traitement, si élémentaire soit-il, est soit soumis à autorisation, soit prohibé.

La Chambre de Commerce exprime son accord avec une meilleure protection de la vie privée. Toutefois, elle ne peut s'exprimer en faveur des multiples tracasseries administratives que suscite le projet de loi. A défaut d'assouplir la rigueur des exigences prévues, le texte projeté risque de n'être guère plus viable que la loi du 31 mars 1979 et de rester tout aussi largement ignoré, ceci d'autant plus que la présentation et la rédaction actuelle du projet de loi sont assez indigeste et maladroite.

*

La Chambre de Commerce, après consultation de ses ressortissants, ne peut donc approuver le projet de loi sous rubrique dans sa version actuelle.

