Avis sur le projet de loi n° 5181 relatif aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification de la loi du 2 août 2002

Délibération n° 3/2004 du 20 février 2004

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la Commission nationale pour la protection des données a entre autres pour mission d'« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».

C'est dans cette optique, et faisant suite à la demande lui adressée par courrier du 3 novembre 2003 de Monsieur le Ministre délégué aux Communications, que la Commission nationale entend présenter ci-après plusieurs observations, réflexions et commentaires au sujet des dispositions spécifiques du projet de loi 5181 relatives à la protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (PARTIE I) et sur les dispositions portant modification de la loi du 2 août 2002 (PARTIE II). Elle a choisi de limiter ses observations aux questions ayant une incidence directe sur la protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel et notamment celle de la vie privée des personnes physiques .

PARTIE I. Avis relatif aux dispositions spécifiques de protection des personnes à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques

A. Conformité de la transposition

1) Champ d'application et définitions

Article 2

1) La distinction faite entre utilisateur et utilisateur final, introduite dans le projet de loi par égard à la législation sur les réseaux et les services de communications électroniques, n'a pas réellement lieu d'être dans le contexte de la protection de la vie privée. Il serait dès lors peut-être plus clair de n'utiliser que les notions d'utilisateur et d'abonné et de rayer en conséquence toutes les occurrences des termes « **utilisateur final** » du projet de loi.

2) Etant donné que la directive 2002/58/CE renvoie à la directive 95/46/CE pour définir le consentement, la Commission nationale renvoie de même quant à la notion de « **consentement** » (article 2 lettre c) du projet sous avis (calquée sur celle de la loi du 2 août 2002) à ses remarques formulées au niveau des modifications proposées à la loi du 2 août 2002 (ayant transposé la directive 95/46/CE) , telles que reprises sous la partie II, point 1) ci-après.

3) Il faudrait préciser que le terme d' **« interconnexion »** employé dans le projet sous avis, notamment à l' article 5, n'est pas à confondre avec la notion d'interconnexion visée à l'article 16 de la loi du 2 août 2002.

La présente notion d'interconnexion est celle est d'ores et déjà employée en matière de réseau de communications électroniques et en particulier, dans le nouveau paquet réglementaire communications électroniques.

Dans ce paquet, la directive 2002/19/CE du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « accès ») définit, en son article 2, l'interconnexion de la façon suivante :

« b) interconnexion : la liaison physique et logique des réseaux de communications publics utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre, ou bien d'accéder aux services fournis par une autre entreprise. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'accès mis en ouvre entre opérateurs de réseaux publics; »

On peut relever d'importantes différences entre ces deux utilisations d'une même terminologie :

- la directive 2002/19/CE parle d'interconnexion des réseaux et donc des moyens de communication quant la loi du 2 août 2002 parle de corrélation de données et donc de contenus ;
- la directive 2002/19/CE a comme champ les réseaux de communication publics quand la loi du 2 août 2002 couvre tant les réseaux publics que privés ;

Ainsi, ces utilisations de la terminologie d'interconnexion semblent être éloignées. En effet, a priori, l'une parle des moyens de communications quant l'autre parle de contenus corrélés (données à caractère personnel).

Cette distance n'est toutefois pas aussi marquée car la définition de la directive 2002/19/CE pose la question du contenu (qu'il s'agisse d'information à caractère personnel ou non).

En effet, la directive 2002/19/CE explique, après avoir défini l'interconnexion comme la mise en place physique de moyens permettant de communiquer entre deux réseaux auparavant distincts, qu'il peut également s'agir « d'accéder aux services fournis par une autre entreprise » et poursuit en disant que « Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. ».

Ainsi, la directive 2002/19/CE, tout en parlant de liaison physique et logique, définit certains objectifs fonctionnels et en rapport au contenu (données à caractère personnel ou non).

Ces objectifs recoupent, pour les utilisateurs, la possibilité :

- de communiquer entre eux ;
- d'avoir accès à des services (contenus) pouvant, le cas échéant, être fournis par d'autres personnes que les opérateurs de réseau (par des prestataires de service) ;

Ces éléments fonctionnels nous rapprochent de la définition de la loi du 2 août 2002 qui, si elle concerne le contenu à caractère personnel, définit également l'interconnexion sous un aspect fonctionnel, c'est à dire celui d'une corrélation de données à caractère personnel.

De plus, une autre analogie peut-être faite. Les deux définitions permettent de qualifier d'interconnexion :

- concernant la directive 2002/19/CE, une opération concernant deux parties de réseaux d'un même opérateur
- ou encore, concernant la loi du 2 août 2002, deux traitements mis en œuvre par deux personnes responsables des deux traitements (qui en forment un troisième, à savoir, celui d'interconnexion).

De façon générale et introductive, il semble souhaitable de coordonner, lorsque c'est possible, les terminologies en provenance de diverses sources. Ceci est d'autant plus d'actualité que la réglementation des réseaux applique le principe de neutralité technologique et que la frontière contenu-contenant est de plus en plus ténue.

2) Sécurité : article 3

L'intitulé de l'article 3 du projet de loi pourrait préciser qu'il s'agit de la « Sécurité des services et des réseaux ».

Les termes « Sous réserve de ce qui précède » peuvent porter à confusion. En effet, il est difficile de déterminer si les fournisseurs de services et/ou les opérateurs ont l'obligation d'informer les abonnés quant aux mesures qu'ils peuvent prendre afin de rendre leurs communications sécurisées, en toutes circonstances ou uniquement lorsque les mesures qu'ils prennent eux-mêmes ne sont pas suffisantes.

Si la volonté du législateur est de limiter cette obligation au second cas, ce qui semble être l'orientation de la directive, il convient de remplacer « Sous réserve de ce qui précède » par « Si ces mesures ne sont pas suffisantes afin de remédier à l'atteinte à la sécurité ou pour en écarter le risque ».

3) Confidentialité des communications : article 4

L'article 4 du projet de loi transpose l'article 5 de la directive.

Article 4 paragraphe (2)

A noter que l'article 4 paragraphe (2) de la loi est cependant moins protecteur pour la personne concernée que l'article 5 paragraphe (1) de la directive.

La directive dispose que « en particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. »

En revanche, le projet sous avis prévoit qu' « il est interdit à toute personne autre que l'abonné, l'utilisateur ou l'utilisateur final concerné d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement de l'abonné, de l'utilisateur ou de l'utilisateur final concerné. »

Selon la formulation actuelle de l'article 4 paragraphe (2), il paraît donc possible que la confidentialité de la communication ne soit pas assurée entre l'abonné, l'utilisateur et l'utilisateur final dans la mesure où il s'agit de personnes différentes.

Si l'abonnée est une entreprise et l'utilisateur est son salarié, le projet sous avis laisse entrevoir la licéité d'une mesure de surveillance (écoute ou enregistrement) opérée par l'abonnée sur son salarié, qui est contraire à la confidentialité des communications prescrite par l'article 5 de la directive, et qui serait par ailleurs contraire tant à la loi du 11 août 1982 concernant la protection de la vie privée, qu'au régime d'autorisation institué par les articles 10, 11 et 14 de la loi du 2 août 2002.

Dans un souci de transposition fidèle de la directive, il faudrait supprimer les termes « abonné » et « utilisateur final », notions non prévues par la directive, laquelle définit à l'article 2 lettre a) le terme « utilisateur » comme étant *« toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ».*

Article 4 paragraphe (3) lettre (c)

Aussi, les exceptions mentionnées à l'article 4 paragraphe (3) du projet de loi semblent bien appropriées, notamment eu égard au contenu des articles 10 et 15 paragraphe (1) de la directive. Quelques remarques importantes s'imposent malgré tout.

Il est fait mention de l'Institut à l'article 4 paragraphe (3) (c) et à d'autres endroits du projet de loi[1]. Il s'agit sans doute de l'Institut Luxembourgeois de Régulation (« ILR »), mais cela ne ressort pas clairement du texte du projet de loi. Peut-être faudrait-il définir l'Institut à l'article 2.

De plus, ce même article 4 paragraphe (3) (c) du projet de loi prévoit de permettre la réécoute de messages, la documentation de fausses alertes et la production de preuves. Or, ni le considérant 36, ni l'article 10 de la directive, ne visent le contenu des communications. Seules les données d'identification et de localisation de la ligne appelante sont visées et peuvent être utilisées dans le but précis de permettre aux services d'urgences d'intervenir le plus efficacement possible. S'il est concevable que la réécoute de communications en cas d'ambiguïté est néanmoins de nature à permettre une intervention plus efficace des services concernés et donc la défense et la sécurité publique au sens de l'article 15 de la directive, il n'en va pas de même en relation avec la production de preuves (puisque, par définition, l'intervention aurait déjà dû avoir lieu au moment de la production de ces preuves). Il n'est donc pas certain que cette dernière hypothèse soit couverte par la directive (à moins que l'on considère que les preuves recherchées le soient pour sauvegarder la sécurité nationale ou la

[1] Voir aussi les articles 5 (1) (a), 7 (5) et 9 (1) (a).

poursuite d'infractions pénales, auquel cas l'article 15 de la directive trouverait également à s'appliquer).

La question des appels malveillants (fausses alertes, menaces et appels abusifs) est soulevée quand à elle par le considérant 36 de la directive qui ne mentionne cependant pour de tels appels que les données d'identification et non les données de localisation.

Le dernier alinéa de l'article 4 paragraphe (3) (c) du projet de loi n'est pas clair. Il mentionne les « données relatives au trafic y afférentes », sans qu'il soit fait référence à quoi ces données sont afférentes. Il conviendrait de remplacer cette phrase par « Les données relatives au trafic afférentes aux communications visées ci-dessus, y compris les données de localisation, doivent être effacées après l'intervention du service concerné (…) ». Cette formulation est au demeurant plus large et permet de viser tous les cas urgent, pas seulement les « secours » (notion qui n'est pas définie et donc source d'équivoque potentielle).

Enfin, en ce qui concerne la conservation du contenu des communications, et sous les réserves formulées ci-dessus à leur sujet, il conviendrait peut-être de préciser que le contenu des communications est à effacer après un délai de 6 mois « au plus », à moins que la volonté du législateur soit précisément de mettre à charge des opérateurs une obligation de conserver ces données pendant une durée fixée à 6 mois (auquel cas cela devrait être précisé).

Au même article 4 paragraphe (3) (c), deuxième alinéa, il conviendrait de mettre la proposition « dont les données de localisation » entre virgules.

Article 4 paragraphe (3) lettre (d)

L'article 4 paragraphe (3) (d) du projet de loi, qui constitue une exception au principe d'interdiction prévu à son article 4 paragraphe 2, devrait peut-être mentionner que l'abonné ou l'utilisateur concerné (et si cette distinction est maintenue, l'utilisateur final) est en droit de refuser le traitement envisagé, comme cela est prévu par la directive. Dans ce cas, par analogie avec la Directive 95/46/CE, il parait également indiqué de prévoir que le fournisseur de service ou l'opérateur doit avertir l'abonné concerné des conséquences d'un tel refus, notamment si le refus implique l'impossibilité de fournir le service demandé.

D'autre part, la Commission nationale salue l'initiative gouvernementale ayant libellé l'article 4 paragraphe (3) (d) du projet de loi de façon plus restrictive que la directive, car il ne mentionne que la possibilité d'effectuer des enregistrements pour fournir la preuve « d'une transaction commerciale » et écarte la fin de cette phrase « ou de toute autre communication commerciale », tel que prévu à l'article 5 paragraphe 2 de la directive.

La Commission nationale ne peut que partager cette approche prudente, puisque dans le cas contraire, en accordant aux responsables des traitements la possibilité supplémentaire d'effectuer des enregistrements pour fournir la preuve « à toute autre communication commerciale », le risque d'atteinte à la sphère privée se trouverait sensiblement aggravé pour la personne concernée (que ce soit le client ou le salarié de l'entreprise).

Quant à la dispense du « consentement »

L'article 4 paragraphe 3 point d) permet l'enregistrement d'une communication sans avoir obtenu le consentement des personnes concernées. Il constitue une exception au principe d'interdiction édicté à l'article 4 paragraphe 2.

En dépit du fait que la dispense du consentement est expressément consacrée à l'article 4 paragraphe 3 point d) du projet sous avis, la Commission nationale est d'avis que l'article 4 paragraphe 3 point d) reste en contradiction avec la loi du 11 août 1982 concernant la protection de la vie privée, en particulier avec son article 2 qui requiert le consentement de la personne enregistrée pour lever le voile de la confidentialité des communications privées.

Aux termes de l'article 2 de la loi précitée du 11 août 1982 :

« Est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 euros à 5.000 euros, ou d'une de ces peines seulement, quiconque a volontairement porté atteinte à l'intimité de la vie privée d'autrui.
*1° en écoutant ou en faisant écouter, en enregistrant ou en faisant enregistrer, en transmettant ou en faisant transmettre, au moyen d'un appareil quelconque, des paroles prononcées **en privé** par une personne, **sans le consentement** de celle-ci;*
2° en observant ou en faisant observer, au moyen d'un appareil quelconque, une personne se trouvant dans un lieu non accessible au public, sans le consentement de celle-ci, en fixant ou en faisant fixer, en transmettant ou en faisant transmettre dans les mêmes conditions l'image de cette personne.
Lorsque les actes énoncés au présent article ont été accomplis au cours d'une réunion au vu et au su de ses participants, le consentement de ceux-ci est présumé;
3° en ouvrant sans l'accord de la personne à laquelle il est adressé ou de celle dont il émane, un message expédié ou transmis sous pli fermé, ou, en prenant connaissance, par un appareil quelconque, du contenu d'un tel message ou en supprimant un tel message.
Les dispositions du No 1 du présent article ne s'appliquent pas à celui qui, chargé de l'entretien ou de la surveillance d'un réseau téléphonique public ou privé, écoute dans l'exercice de ses fonctions une communication pour s'assurer du bon fonctionnement de la liaison.
Est puni des peines prévues au présent article celui qui ne respecte pas le secret de la communication ainsi écoutée. »

Si l'intention du législateur était celle de déroger à la loi précitée de 1982 en ce qui concerne les communications effectuées au moyen d'un réseau de communication public et de services de communications électroniques accessibles au public, il parait préférable dans un souci de sécurité juridique de le mentionner expressis verbis dans le projet sous avis, à moins que le législateur ne retienne qu'une telle précision soit superflue au regard du principe général de droit que la loi postérieure (le projet sous avis) déroge implicitement à la loi antérieure (loi de 1982).

Cette conclusion s'impose davantage dans la mesure où l'article 1er du présent projet précise que les dispositions sont des dispositions spécifiques de « protection des données » applicables en matière de communications électroniques accessibles au public et qu'en dehors du champ d'application du présent projet, les dispositions générales de la loi du 2 août 2002 s'appliquent (document parlementaire 5181/00, p.12). Ceci est parfaitement en ligne

avec l'article 1er paragraphe 2 de la directive 2002/58/CE qui dispose que « *les dispositions de la présente directive précisent et complètent la directive 95/46/CE »*. En revanche, rien n'est dit dans le projet sous avis quant à la loi de 1982, de sorte qu'il faut présumer que la volonté du législateur est celle de la laisser intacte.

Quant aux enregistrements à des fins de preuve des transactions commerciales, l'ABBL écrit dans son avis du 5 novembre 2003 que *« l'article 4 du projet de loi pose le principe de la confidentialité des communications. Il s'agit d'un texte spécial par rapport à la loi générale du 11 août 1982 concernant la protection de la vie privée qui, notamment, interdit l'écoute et l'enregistrement de communications sans le consentement des personnes concernées. Si la loi du 11 août 1982 sur la vie privée pose un tel principe, c'est parce qu'elle vise à protéger les interlocuteurs d'une communication contre l'enregistrement clandestin par des tiers. Elle ne dit rien cependant sur la situation d'une personne qui enregistre la communication téléphonique qu'elle entretient elle-même avec une autre personne. Il était donc urgent que cette situation soit clarifiée. »*

La Commission nationale ne saurait partager l'analyse de l'ABBL reprise à son compte par la Chambre de Commerce consistant à dire que la loi de 1982 ne préciserait pas si l'interdiction d'écouter, d'enregistrer ou d'intercepter les paroles prononcées en privé, au moyen d'un appareil quelconque, vise uniquement les tiers ou si cette prohibition doit être entendue comme s'appliquant également aux parties entre lesquelles les paroles prononcées en privé sont échangées.

En effet, en employant les termes de « *écoutant ou en faisant écouter, en enregistrant ou en faisant enregistrer »* la loi de 1982 fait envisage aussi bien le fait d'écouter ou d'enregistrer soi-même que le fait de « faire écouter ou enregistrer » par un tiers la conversation téléphonique. Quelle serait l'utilité et la signification de la distinction opérée si les parties à la conversation échappaient à la prescription légale?

Admettre que l'interdiction édictée à l'article 2 point 1 ne vise que les tiers revient à interpréter de la même façon le fait d'écouter/enregistrer ou de faire écouter/enregistrer, étant donné que dans cette logique « écouter/enregistrer » vise un premier tiers et « faire écouter/enregistrer » un deuxième tiers mandaté par le premier tiers. Or ces deux personnes sont des tiers par rapport à l'entretien téléphonique, de sorte qu'en visant à la fois deux personnes tierces différentes la distinction opérée par le texte légal en question ne donnerait aucun sens et ne serait qu'en réalité une redite superflue.

De même, en employant le terme « quiconque » la loi vise indistinctement le tiers à la communication privée et la partie concernée (partenaire de la conversation téléphonique) elle-même. Dans le cas contraire, le législateur aurait pris soin de préciser que la loi de 1982 vise uniquement les tiers et non aussi les partenaires à la conversation téléphonique. Or, tel n'est pas le cas.

En outre, cette interprétation de la loi de 1982 s'impose davantage à la lecture de la seconde phrase de l'article 2, point 2 : *« Lorsque les actes énoncés au présent article ont été accomplis au cours d'une réunion au vu et au su de ses participants, le consentement de ceux-ci est présumé; ».*

Est visée en l'occurrence la situation d'une réunion (d'affaires) où un enregistrement est effectué et les participants ayant été dûment informés. Dans cette hypothèse, si un participant

à la réunion souhaite enregistrer la discussion, le consentement des autres participants est présumé lorsqu'il procède à l'enregistrement au vu et au su des autres.

La Commission nationale juge également opportun de rappeler ce qu'est une communication privée.

Dans le commentaire des articles relatif à la loi de 1982, l'on peut lire que « *Il n'est pas nécessaire que ces paroles (*prononcées par une personne en privé*) aient été prononcées dans un lieu privé, même prononcée en un lieu public mais destinée à n'être entendue que par une personne déterminée, l'écoute de la conversation constitue une infraction* » (doc. parl. 2177/00, p.1683).

Ceci rejoint l'approche du législateur belge, dont la loi luxembourgeoise de 1982 s'est inspirée.

D'après les travaux préparatoires de la loi belge, une communication professionnelle, mais non destinée à être entendue par d'autres personnes que les partenaires à la conversation est une communication privée au sens de la loi. Une communication est privée dans la mesure où elle n'est pas publique, et non pas dans le sens où elle ne serait pas professionnelle.

Contrairement à l'avis de l'ABBL du 5 novembre 2003 et de l'avis de la Chambre de commerce du 29 janvier 2003 (reprenant littéralement l'avis de l'ABBL sur ce point), la Commission nationale estime dès lors que l'employeur est à considérer comme étant tiers à la conversation téléphonique tenue entre son salarié et un client de l'entreprise, de sorte que le consentement et du salarié et du client est requise au titre de la loi de 1982, à moins que l'intention du législateur ne consiste à déroger à cette disposition d'ordre général en le précisant expressément dans le présent projet de loi.

Quant à la notion de « légalement autorisé »

La Chambre de Commerce a souligné dans son avis du 29 janvier 2004 que la « législation luxembourgeoise ne prévoit pas d'autorisation légale pour l'enregistrement des communications électroniques à des fins commerciales ».

Pour bien cerner la signification des termes « légalement autorisé », il y a lieu de rappeler la directive à cet égard :

Le considérant 23 de la directive 2002/58/CE prévoit que

« La confidentialité des communications devrait également être assurée dans les transactions commerciales licites. Au besoin et sous réserve d'une autorisation légale, les communications peuvent être enregistrées pour servir de preuve d'une transaction commerciale. La directive 95/ 46/CE est applicable en pareil cas. Les parties aux communications devraient être informées de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée du stockage de l'enregistrement. La communication enregistrée devrait être effacée dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction. »

L'article 5 paragraphe 2 de la directive dispose que :

« Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale. »

Il en découle qu'une autorisation par une disposition légale est nécessaire pour que l'exception au principe d'interdiction visée à l'article 4 paragraphe (3) (d) du projet sous avis puisse devenir efficace et trouver application.

Cette analyse de la directive 2002/58/CE est confirmée par l'autorité de contrôle belge en matière de protection des données.

« *C'est cette intervention légale qui permettra de circonscrire les limites de l'exception au principe de confidentialité des données. Tant que l'exception prévue par la directive n'aura pas été explicitement transposée en droit belge, les responsables du secteur bancaire sont donc tenus d'obtenir le consentement des parties à la communication* » (cf. avis n° 1/2002 du 22 août 2002 intitulé *« Enregistrement des télécommunications effectuées dans le cadre des services bancaires »,* rendu par la Commission belge pour la protection de la vie privée).

Se pose la question de savoir si le législateur n'a pas d'ores et déjà créé cette « autorisation légale » en ayant introduit les articles 10 et 11 dans la loi du 2 août 2002 qui prévoient la possibilité une surveillance –notamment des conversations téléphoniques professionnelles- dans certaines conditions qu'ils ont pour objet de préciser. Il ressort d'ailleurs clairement des travaux préparatoires que l'hypothèse en question a été expressément envisagée.

« Relèvent également de la protection des biens de l'entreprise…(Art. 11 paragraphe (1) lettre b) *... On peut encore y ajouter les écoutes téléphoniques effectuées par des établissements de crédit et autres professionnels du secteur financier aux fins d'enregistrer les ordres des clients passés par téléphone à condition toutefois que tant le client ait donné son accord à un tel enregistrement et que le salarié ait été informé que les conversations téléphoniques passées par ce téléphone seront enregistrées.* (document parlementaire 4735/13, p. 21).

- Si tel est cas, l'enregistrement « légalement autorisé » vise donc l'article 10 paragraphe 1er lettre a) de la loi du 2 août 2002 prévoyant la possibilité d'enregistrement des conversations téléphoniques professionnelles moyennant le consentement (du client de la banque) et l'article 11 paragraphe 1er lettre b) de la loi du 2 août 2002 prévoyant cette possibilité pour la protection des biens de l'entreprise dans l'hypothèse où un salarié (de la banque) est partie à la conversation surveillée, l'autorisation préalable de la Commission nationale pour la protection des données étant requise par ailleurs en vue d'assurer le respect d'un juste équilibre entre les intérêts en cause.

La Commission nationale rappelle dans ce contexte le rapport final de la commission des médias et des communications au niveau du projet de loi n° 4735 (ayant conduit à la loi du 2 août 2002) qui prévoit que : « *Il se peut qu'un même traitement tombe dans le champ d'application soit de l'article 10 soit de l'article 11 en fonction de la personne concernée. Par exemple, une caméra dans une grande surface tombe sous le coup de l'article 10 si la personne concernée est un client, même potentiel, du magasin et sous*

celui de l'article 11 si la personne concernée est un salarié employé par le propriétaire de ce magasin.» (document parlementaire 4735/13, p. 17).

L'article 4 (2) du projet sous avis parle de « moyen d'interception ou de surveillance », de sorte que les articles 10, 11 et 14 de la loi du 2 août 2002 sont applicables au cas de figure de l'article 4 (3) sous avis.

Ainsi les paragraphes 2 et 3 de l'article 4 relatif à la confidentialité des communications sont parfaitement cohérents : une mesure de surveillance consistant dans l'enregistrement de communications n'est pas interdite dans le cadre des usages professionnels licites pour prouver une transaction commerciale, pourvu qu'une autorisation pour ce genre de traitements ait été octroyée au responsable du traitement par la Commission nationale en application des 10 et 11 de la loi.

Pour s'en tenir au libellé de l'article 4 paragraphe (3) (d) du projet sous avis : en raison de l'autorisation émise par la Commission nationale sur base de la loi du 2 août 2002 l'enregistrement a été « légalement autorisé ».

Dans cet ordre d'idées, la proportionnalité de la mesure de surveillance projetée sera appréciée au cas par cas par la Commission nationale.

- Dans le cas contraire, c'est-à-dire si l'on considère que les articles 10 et 11 de la loi du 2 août 2002 n'équivalent pas à l'autorisation légale requise au titre de la directive 2002/58/CE, la Chambre de Commerce relève à juste titre l'absence de texte légal mettant à profit l'exception prévue par la directive, de sorte qu'il incombe au législateur - bien évidemment s'il entend en faire bénéficier les milieux professionnels concernés - d'insérer dans le projet sous avis une disposition légale qui circonscrit précisément les limites de l'exception au principe de confidentialité des données en veillant à y appliquer les principes de transparence, de finalité, de nécessité et de proportionnalité ancrés dans la loi du 2 août 2002.

Finalement, la Commission nationale salue l'initiative gouvernementale consistant à réaffirmer dans l'article 4 § 3 lettre d) le principe du droit à l'information d'ores et déjà inscrit dans l'article 26 de la loi du 2 août 2002 et repris du considérant 23 précité.

Article 4 paragraphe (3) (e)

Pour éviter tout problème d'interprétation, la Commission nationale recommande de reprendre la teneur de la directive qui emploie le terme de « refuser » au lieu de « s'opposer » au niveau de l'article 4 paragraphe 3 lettre e).

Etant donné la collecte directe des données auprès de la personne concernée, la Commission nationale souligne que :

- les informations précises et complètes doivent être fournies au moment de la connexion, au moyen d'une communication selon la technique du « pop up » par exemple. Les méthodes retenues pour communiquer des informations doivent offrir un droit de refus ou solliciter le consentement (mais le consentement doit-il être exprès et non équivoque ?) ;
- les personnes concernées sont l'abonné, l'utilisateur ou l'utilisateur final. Cependant si

l'accès a des terminaux appartient à des personnes morales abonnées, et lorsque plusieurs utilisateurs utilisent le service d'un même abonné, ou lorsqu'on est simplement en présence d'un abonné (tel un employeur) et d'un autre l'utilisateur (tel un employé), il est difficile à mettre en œuvre l'obligation d'informer et d'offrir le droit d'opposition requis. A titre d'exemple, il y a lieu de citer le problème de l'utilisation d'un équipement terminal par plusieurs utilisateurs, si un utilisateur accepte un cookie, celui-ci pourra être utilisé lors des sessions ultérieures initiées par d'autres utilisateurs.

Article 4 paragraphe (4)

Les sanctions prévues par l'article 4 paragraphe (4) du projet de loi semblent appropriées, notamment eu égard à l'article 24 de la directive 95/46/CE.

4) Données relatives au trafic : article 5

L'article 5 du projet de loi met en oeuvre les possibilités offertes par les articles 6 et 15 de la directive de limiter la confidentialité des communications ou des données y afférentes.

Il semble que les critères et limitations de l'usage qui peut être fait des données soient appropriés par rapport aux conditions imposées par la directive. En effet, la conservation des données est limitée quant à son objet et quant à sa durée.

En ce qui concerne la durée de conservation, cette question est traitée séparément sous le point B du présent avis.

Article 5 paragraphe (1)

Peut-être faudrait-il préciser, à l'article 5 paragraphe (1) (b) du projet de loi que, à défaut d'être effacées, les données doivent être rendues anonymes « au sens de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel », c'est-à-dire de sorte à ne plus pouvoir identifier les personnes concernées.

Quant à l'article 5 paragraphe 1 lettre e), la Commission nationale relève que dans le domaine de la sécurité nationale, la défense et la sécurité publique ou dans le domaine de la prévention, recherche et poursuite d'infractions pénales la faculté pour les Etats-membres de déroger dans leur législation nationale au principe de finalité est contenu dans la directive 95/46/CE au niveau de l'article 13 qui permet de limiter la portée de l'article 6 paragraphe 1, lorsqu'une telle mesure s'avère nécessaire et est proportionnée au but recherché.

Article 5 paragraphe (2)

Il pourrait être utile, pour une simple question de langage, de remplacer « nécessaires à ce que de telles » par « nécessaires pour que de telles » et « de manière telle qu'il est impossible » par « de manière telle qu'il soit impossible ».

Article 5 paragraphe (3)

L'article 6 paragraphe (5) de la directive vise non seulement les traitements aux fins visées à l'article 6 paragraphe (3) de la directive (commercialisation de services et fourniture de services à valeur ajoutée) mais aussi les traitements aux fins visées à l'article 6

paragraphe (2) de la directive (facturation). Or, cela n'est pas prévu par l'article 5 paragraphe (3) du projet de loi.

Il serait par conséquent utile d'ajouter après la première phrase de l'article 5 paragraphe (3) du projet de loi que « L'abonné doit être informé des types de données relatives au trafic qui sont traitées [éventuellement ajouter aussi, par souci de cohérence avec le paragraphe suivant : « , de la finalité »] et de la durée du traitement ».

Par ailleurs, il serait peut-être avantageux de limiter la durée du stockage autorisé de données relatives au trafic à des fins de facturation ou de paiement pour interconnexion en fixant une limite maximale qu'il ne faudrait pas dépasser, sauf en cas de litige, les données n'étant plus nécessaires aux fournisseur de services ou à l'opérateur.

Dans ce cas, il conviendrait d'ajouter encore à la fin de l'article 5 (3), conformément à l'Avis 1/2003 sur le stockage des données relatives au trafic à des fins de facturation[2] du Groupe de protection des données institué par l'article 29 de la Directive 95/46/CE (le « Groupe Article 29 ») : « (…) et ne peut en tout état de cause dépasser 6 mois lorsque la facture à été payée et n'a pas fait l'objet de litige ou de contestation ».

Article 5 paragraphe (4)

Il serait peut-être plus clair de remplacer « nonobstant son droit de pouvoir s'opposer à tout moment à un tel traitement » par « sans préjudice de son droit de retirer à tout moment sont consentement pour un tel traitement ».

Article 5 paragraphe (5)

Il faudrait peut-être viser le paragraphe (1) dans son ensemble plutôt que le paragraphe (1) (b) seul.

Article 5 paragraphe (6)

Les sanctions prévues par l'article 4 paragraphe (4) du projet de loi semblent appropriées. Malgré tout, il faudrait peut-être également viser le paragraphe (3), particulièrement si l'ajout suggéré plus haut est retenu. Dans ce cas, il faudrait simplement retirer les mots « des paragraphes (1), (2), (4), (5) ».

5) Facturation détaillée

Il serait peut-être utile de faire référence, dans l'article 6 paragraphe (2) du projet de loi, à une liste de numéros qui ne devraient pas figurer sur les factures détaillées. En effet, l'article 6 (2) du Projet de Loi est limité aux appels gratuits et ceux aux services d'urgence et d'alerte. Or, d'autres numéros peuvent révéler des informations sensibles sur les personnes, comme par exemple les appels vers les services Aide aux femmes (12344), Aide aux victimes de la criminalité (40 20 40), Femmes battues (44 81 81), Info-viol (49 58 54). Une telle liste pourrait être maintenue à jour mise à la disposition des opérateurs par l'ILR.

[2] Voir < http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp69_fr.pdf >.

6) Identification de la ligne appelante et de la ligne connectée

Article 7 paragraphe (1)

Outre la réserve émise ci-dessus quant à la distinction entre utilisateur et utilisateur final (voir point **I. A. 1) Champ d'application et définitions**) il faut remarquer que la dernière phrase de l'article 7 paragraphe (1) du projet de loi ne mentionne que l'abonné. Il faudrait ajouter la notion d'utilisateur (et d'utilisateur final si la distinction est maintenue).

Article 7 paragraphe (6)

Une erreur de frappe devrait être corrigée. A la place de « Les dispositions du paragraphe 1e s'appliquent », il faudrait lire « Les dispositions du paragraphe 1er s'appliquent ».

Article 7 paragraphe (8)

Il serait préférable de ne pas mentionner que l'abonné appelé prétendant être victime d'appel anonymes peut *obtenir* l'identification de la ligne appelante ou connectée. En effet, cela peut laisser supposer que la victime prétendue pourra dans tous les cas prendre connaissance de l'identification de la ligne appelante. Or, il est à supposer que, dans certains cas, il sera préférable que seuls les services de police ou les autorités compétentes concernées soient aptes à obtenir de telles données, notamment pour vérifier les assertions de victimes prétendues ou encore pour éviter qu'une victime n'utilise à son tour ledit numéro à mauvais escient. Il vaudrait donc mieux utiliser l'expression « peut demander l'identification » en lieu et place de « peut obtenir l'identification ».

A cet égard, il faudrait peut-être distinguer les cas d'appels réellement malveillants et ceux d'appels simplement dérangeants.

En tout état de cause, la disposition telle qu'elle est rédigée actuellement serait mieux compréhensible si les virgules avant et après l'expression « des appels répétés ou intempestifs » étaient retirées. Il faut encore remarquer que l'utilisateur (et l'utilisateur final) n'est pas visé par l'alinéa premier de cet article.

Pour plus de clarté, le deuxième alinéa de l'article 7 paragraphe (8) pourrait être modifié comme suit : « Un règlement grand-ducal fixera les modalités que devront respecter le fournisseur du service et/ou l'opérateur ainsi que l'abonné prétendant être victime d'appels anonymes à contenu malveillant. Il précisera également les caractéristiques d'un appel à contenu malveillant et déterminera les conséquences possibles de l'obtention par l'abonné ou les autorités compétentes de l'identification de la ligne appelante alors même que la présentation de cette identification avait été empêchée par l'abonné ou l'utilisateur appelant ».

7) Renvoi automatique d'appel

Peut-être faudrait-il aussi mentionner l'opérateur qui sera parfois le seul apte à fournir les données nécessaires pour faire cesser une déviation d'appel.

8) Données de localisation autres que les données relatives au trafic

Article 9 paragraphe (1)

La Commission nationale renvoie à ses commentaires faites sous le point B relatif à la durée de conservation.

Article 9 paragraphe (2)

Mêmes suggestions de modification que pour l'article 5 paragraphe (2).

Article 9 paragraphe (3)

La fin de ce paragraphe devrait être formulée comme suit : « (…) et sous réserve des dispositions des paragraphes (2), (4) et (5) ».

Par analogie avec l'article 5 paragraphe (4), il faudrait ajouter ensuite : « En ce qui concerne les traitements effectués avec des données qui ne sont pas rendues anonymes, l'abonné [seulement si cette distinction est maintenue : « , l'utilisateur »] ou l'utilisateur [« final »] peut à tout moment, gratuitement et sans indication de motif, retirer sont consentement ».

Relativement à des services à valeur ajoutée, il semble important de prévoir, à l'instar de l'article 9 de la directive, que, « En outre, l'abonné [seulement si cette distinction est maintenue : « , l'utilisateur »] ou l'utilisateur [« final »] doit être en mesure d'interdire temporairement, par un moyen simple et gratuit, le traitement des données de localisation autres que les données relatives au trafic le concernant ».

Article 9 paragraphe (4)

Ce paragraphe pourrait être reformulé de la manière suivante : **« Le fournisseur du service** et, le cas échéant, l'opérateur informent préalablement l'abonné, [seulement si cette distinction est maintenue : « , l'utilisateur »] ou l'utilisateur [« final »] des types de données de localisation autres que les données relatives au trafic qu'ils traitent, des finalités et de la durée de ce traitement ainsi que de la transmission éventuelle de ces données à des tiers en vue de la fourniture du service à valeur ajoutée. » La suite de la phrase devrait être supprimée, la question du consentement étant traitée au paragraphe précédent (voir ci-dessus, Article 9 (3)).

Article 9 paragraphe (5)

Même observation que pour l'article article 5 paragraphe (5) en ce qui concerne la référence au paragraphe (1) (b).

9) Annuaires d'abonnés

Voir plus particulièrement nos commentaires repris sous l'article 12 ci-après.

A l'article 10 paragraphe (1), la virgule qui suit « L'abonné » devrait être déplacée après « doit en être informé ».

10) Communications non sollicitées

Article 11 paragraphe (1)

L'article 11 paragraphe 1 transpose l'article 13 paragraphe 1 du texte de la directive 2002/58/CE.

L'envoi de courriers électroniques à des fins de prospection directe ne pourra intervenir que lorsque l'abonné aura préalablement consenti à cet envoi (consentement expresse et non équivoque).

Dans le cas où le responsable du traitement souhaite obtenir le consentement préalable de l'abonné par un des moyens visés par l'article 11 paragraphe 1er se pose indubitablement le problème de savoir si une telle demande en obtention du consentement préalable ne soit elle-même qualifiée de communication non sollicitée. Dans l'affirmative, le consentement doit être recueilli d'une autre manière.

Article 11 paragraphe (2)

Le début de l'article 11 paragraphe (2) devrait être ainsi libellé : « **Sans préjudice du paragraphe (1er), le fournisseur qui, dans le cadre d'une vente d'un produit ou d'un service, (…)** ».

Malgré tout, le terme fournisseur est vague puisqu'il n'est pas défini. De plus, il peut porter à confusion avec l'expression fournisseur de services qui, elle, est définie à l'article 2 du projet de loi et ne vise que les personnes qui fournissent des services de communications électroniques. Il conviendrait plutôt d'utiliser les termes « toute personne physique ou morale » proposés par la Directive et qui englobent aussi les personnes qui proposent des produits par le biais de services de communications électroniques.

Aussi, pour indiquer plus clairement que le fournisseur *doit* donner la possibilité à son client de refuser toute communication future, la formulation suivante serait indiquée : « (…) pour autant que ledit client soit clairement informé sur l'exploitation de ses coordonnées et se voit donner clairement et expressément la faculté de s'opposer par un moyen simple et gratuit à une telle exploitation (…) ». En effet, « nonobstant son droit de » indique simplement que le client à ce droit mais pas que le fournisseur doit le mettre *expressément* à sa disposition.

Enfin, même s'il est vrai que les termes « **courrier électronique** » sont ceux utilisés par la directive elle-même, il semble que les termes « **message électronique** » seraient plus appropriés car ils englobent également, sans équivoque, les services de messages courts (« SMS ») et de messages multimédias (« MMS »), seules les télécopies n'étant pas visées par cette disposition.

11) Dispositions transitoires et finales

Article 12 paragraphe (2)

Ici encore, le mot fournisseur est utilisé sans définition et peut porter à confusion avec la notion définie à l'article 2 du projet de loi de fournisseur de services.

Il faudrait en outre insérer l'idée que seuls sont visés les annuaires qui respectent les dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Cela pourrait être formulé comme suit : « **Le fournisseur offrant un annuaire licite de „recherche inverse" (…)** ». Sans cela, on pourrait penser que l'obtention éventuellement illicite de données serait validée par le silence de l'abonné.

La Commission nationale s'interroger sur la pertinence de cette disposition transitoire au regard des considérations suivantes.

Dans le commentaire des articles du projet de loi n° 5181, l'on peut lire sous l'article 10 que :

« Il convient que l'opérateur et/ou le fournisseur d'annuaires publics informent les abonnés figurant dans ces annuaires des fins auxquelles ceux-ci sont établis (paragraphe 1er) et de toute utilisation particulière qui peut être faite des versions électroniques des annuaires publics, notamment grâce aux fonctions de recherche intégrées dans le logiciel, telles que les fonctions de recherche inverse qui permettent aux utilisateurs d'un annuaire de trouver le nom et l'adresse d'un abonné à partir d'un numéro de téléphone. Dans ce cas, il s'agirait d'une nouvelle finalité qui ne serait pas compatible avec la finalité primaire, et de ce fait en principe illicite selon le régime général de la loi du 2 août 2002 à moins que la personne concernée n'ait expressément consenti au traitement de ses données à ces nouvelles fins (paragraphe 3). Ainsi, le consentement informé des personnes concernées à l'inclusion de leurs données dans des annuaires publics pour des recherches inversées est donc indispensable. » (document parlementaire 5181/00, p.18 et 19).

La Commission nationale partage cette analyse qui se fonde sur les dispositions de l'article 14, paragraphe 1er, lettre (e) de la loi du 2 août 2002.

L'annuaire inversé constitue au sens de la directive 2002/58/CE du 12 juillet 2002 une utilisation des données à une fin autre que celle pour laquelle elle a été collectée, de sorte qu'en application de l'article 14, paragraphe 1er, lettre (e) de la loi, ce traitement est soumis à l'autorisation préalable de la Commission nationale, d'une part, et ne peut être effectué que moyennant consentement préalable de la personne concernée, d'autre part.

Il s'ensuit qu'au stade actuel de la législation luxembourgeoise, **la situation visée par le second paragraphe de l'article 12 du projet sous avis qui réserve un « opt out » pour l'abonné (personne concernée) ne peut se rencontrer en pratique, alors qu'elle est d'ores et déjà contraire à la loi du 2 août 2002** en vigueur qui requiert le consentement exprès comme « opt in » pour utilisation des données pour une toute nouvelle finalité.

B. Durée de conservation des données

Le projet de loi fixe à 12 mois la durée pendant laquelle les fournisseurs de services et opérateurs sont tenus de conserver les données relatives au trafic et autres données de localisation.

Etant donné que la directive prévoit en son article 6 paragraphe (1), concernant la durée de conservation de les données relatives au trafic, que celles-ci « *doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaire à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1* ».

Que l'article 15 de la directive énonce que les Etats membres peuvent « *adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié* » pour la sauvegarde de la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et le poursuite d'infractions pénales.

Qu'en ce qui concerne les données de localisation autres que les données relatives au trafic, la directive dispose en son article 9 paragraphe (1) qu'elles ne peuvent être traitées « *qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée* ».

Qu'il n'est donc pas fait mention de l'article 15 de la directive comme à l'article 6 paragraphe (1) de la directive, mais l'article 15 de la directive lui-même permet de limiter la portée des droits et obligations de plusieurs dispositions, dont celles de l'article 9 de la directive.

On pourrait déduire de ces dispositions que les Etats membres ont toute latitude de prévoir une durée limitée pendant laquelle les fournisseurs de services ou les opérateurs seraient obligés de conserver toutes les données relatives au trafic et de localisation. C'est ce que fait le Projet de Loi en ses articles 5 paragraphe (1) (a) et 9 paragraphe (1) (a).

C'est la position qu'a adoptée la France dans la loi sur la sécurité quotidienne promulguée le 15 novembre 2001. Le principe d'effacement des données relatives à une communication y est inscrit, tempéré par deux exceptions : la conservation pour les besoins de facturation et la conservation à des fins de poursuite des infractions pénales, cette dernière ne pouvant dépasser un an. Des recommandations ont cependant été émises afin que la durée de conservation des données de communication soit réduite pour ce qui concerne la poursuite des infractions pénales.

A cet égard, l'annexe 2 du 9ème rapport sur la mise en œuvre de la réglementation de l'Union Européenne en matière de communications électroniques[3] présente un tableau qui donne un panorama des dispositions législatives nationales existantes sur le sujet en Europe (voir page 32 dudit rapport).

[3] COM(2003) 715 final ; voir
< http://www.europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/annualreports/9threport/annex2181103.pdf >.

Mais cette interprétation de la directive n'est pas la seule possible. En effet, d'aucuns considèrent que, dans l'état actuel des choses, les Etats membres ne peuvent pas prévoir *a priori* une durée de conservation généralisée des données relatives au trafic ou de localisation pour toutes les communications électroniques dont ils sont porteurs.

C'est notamment ce qui découle de la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications[4] : « *La protection des données de trafic dans les télécommunications est maintenant prévue dans la directive 2002/58/CE du Parlement européen et du Conseil concernant la vie privée et les communications électroniques (Journal Officiel L 201/37), qui précise que le traitement des données de trafic est en principe autorisé pour la facturation et le paiement des interconnexions. Après un très long et très explicite débat, il a été établi selon l'article 15 (1) de la directive que la conservation des données de trafic à des fins policières doit remplir des conditions strictes : dans chaque cas la conservation des données doit être prévue pour une période limitée et constituer une mesure nécessaire, appropriée et proportionnelle dans une société démocratique.*
Lorsque des données de trafic doivent être conservées, sa nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou tout autre forme d'abus.
La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable ».

Cette position a été entérinée par le Groupe Article 29. En effet, dans son Avis 5/2002 sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications, adopté le 11 octobre 2002, le Groupe Article 29 déclare qu'il « *souscrit en tout point aux termes de cette déclaration* ».

Ainsi, si de nombreuses controverses ont précédé le vote de la Directive sur le sujet sensible de la rétention des données relatives au trafic, il ne s'agit apparemment pas actuellement pour les Etats membres de prévoir une conservation systématique des données, mais plutôt de prévoir un système « au cas pas cas »[5].

Ce qui peut être prévu sans aucun doute, c'est la possibilité pour une autorité judiciaire nationale d'ordonner à un fournisseur de services ou à un opérateurs dans un cas particulier, par exemple dans le cadre d'une enquête judiciaire ouverte, de conserver exceptionnellement certaines données pendant une durée limitée, si cela est justifié par un motif énoncé à l'article 15 (1) de la Directive.

[4] Adoptée lors de la 24ème conférence internationale des commissaires européens à la protection des données personnelles qui s'est tenue à Cardiff au Pays de Galle du 9 au 11 septembre 2002) ; pour la déclaration complète, consulter < http://www.cnil.fr/thematic/docs/international/Cardiff_declaration.pdf >.

[5] D'aucuns considérant même qu'il en va « *de la défense des libertés fondamentales et constitutionnelles garanties également dans la Convention européenne des droits de l'homme* » (Marco CAPPATO, rapporteur sur la Directive) et du principe même de la démocratie

Ainsi, dans l'état actuel des choses, la Commission nationale estime que la règle devrait rester celle de l'interdiction de rétention des données de communications. Les exceptions doivent être verrouillées et permises uniquement dans un but précis, les mesures devant être nécessaires, appropriées, proportionnelles et prévues pour une durée limitée (la plus courte possible).

Un rapport sur la légalité de la rétention de données à l'égard des droits garantis par la Convention européenne des droits de l'homme confirme cette interprétation.

En effet, ce rapport expose que la notion de rétention systématique et généralisée de données à été rejetée expressément lors de l'adoption de la Directive.

Cependant, ce même rapport fait également état d'une décision-cadre, à l'étude au sein du Conseil de l'Union Européenne (Justice et Affaires Intérieures), qui imposerait aux Etats Membres de prendre des mesures législatives nationales pour obliger les fournisseurs de services et les opérateurs d'opérer une rétention de données pendant une durée allant de 12 à 24 mois pour les besoins éventuels d'enquêtes policières ou de poursuites judiciaires.

La rapport indique que de telles mesures seraient contraires aux dispositions de l'article 8 de la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales, garantissant le droit à la vie privée, et de la jurisprudence de la Cour européenne des droits de l'homme (il y est fait référence dans le considérant 11 de la Directive).

Il paraît indiqué de rappeler la teneur de l'article 8 de la Convention européenne des Droits de l'Homme :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Il en découle que la protection de la vie privée est la règle, et l'ingérence dans ce droit doit rester l'exception.

Plus récemment, le 9 janvier 2004, la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures du Parlement européen a publié un Projet de rapport sur le premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)[6] (voir à la page 7).

Quant aux exceptions aux lois relatives à la protection de la vie privée, ce projet de rapport indique que le Parlement européen « *estime que les législations nationales prévoyant à des fins judiciaires la conservation sur une grande échelle de données concernant les*

[6] Voir < http://www.europarl.eu.int/meetdocs/committees/libe/20040121/519419fr.pdf >.

communications entre citoyens ne sont pas pleinement conformes aux dispositions et à la jurisprudence de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, puisqu'elles instaurent un empiétement sur le droit à la vie privée qui n'est pas autorisé par le pouvoir judiciaire, au cas par cas et pour une durée limitée, qui ne distingue pas de catégories dans la population soumise à surveillance, qui ne respecte pas le secret des correspondances protégées (comme les communications de juriste à client), qui ne précise pas la nature des délits ni les circonstances qui justifieraient de tels empiétements, lesquels font naître en outre de sérieux doutes quant à leur nécessité pour une société démocratique ou à leur caractère approprié et proportionné – au sens de l'article 15 de la directive 2002/58/CE ».

Par ailleurs, le projet de rapport indique également que le Parlement européen « *demande à la Commission d'élaborer, sur la base de la convention européenne sur les droits de l'homme, de la jurisprudence qui en dérive et des directives sur la protection des données à caractère personnel, un document qui examine le droit à la vie privée et les exceptions légalement admises à ce droit et qui vérifie la conformité des mesures nationales de conservation des données personnelles ainsi que les lois nationales prévoyant des exceptions au principe général du droit à la protection de la vie privée pour des motifs comme l'ordre public, la défense nationale, la sûreté de l'État, ses intérêts économiques pourvu que des activités liées à la sûreté de l'État soient en jeu, la conduite de poursuites pénales, ou bien autorisant, pour les mêmes motifs, une interception de données à caractère personnel; invite les institutions européennes à lancer un débat ouvert et public au sujet dudit document* ».

Dans ce contexte ambigu et en attendant les résultats des travaux actuels de l'Union européenne, la question pourrait être réglée par une disposition de type : « Rien dans la présente loi ne doit être interprété comme empêchant les autorités judiciaires compétentes d'ordonner aux fournisseurs de services ou aux opérateurs de conserver, pendant la durée qui leur sera indiquée, les données relatives au trafic ou de localisation concernant les communications qui leur seront désignées ». Il faudrait alors adapter les articles 5 paragraphe (1) (a) et 9 paragraphe (1) (a) du projet de loi.

Si le législateur devait malgré tout privilégier une interprétation de la directive lui permettant de fixer une durée pendant laquelle les données relatives au trafic doivent être systématiquement stockées par les fournisseurs de services ou les opérateurs, la Commission nationale est d'avis que la durée prévue actuellement de 12 mois constitue en tout état de cause le maximum acceptable.

Enfin, il y a lieu de réitérer les réserves formulées ci-dessus au sujet de la conservation de l'enregistrement du contenu des communications avec les services d'urgence prévu à l'article 4 paragraphe (3) (c) et limité à une durée de 6 mois (voir point A) 3).

C. Lacunes potentielles

1) Article 14 de la Directive

Nous supposons qu'aucune mesure n'a été ou ne sera prise en vue d'imposer des exigences relatives à des caractéristiques techniques spécifiques aux terminaux ou autres équipements de communications électroniques et que cela n'est pas nécessaire pour les besoins de la transposition de la Directive.

2) Prospection directe – changement de régime – période de transition

Il est un point qui n'est pas traité par le Projet de Loi. En effet, on ne sait pas quel sera le sort des adresses de courrier électronique collectées licitement avant l'entrée en vigueur de la loi projetée.

Le système rendu obligatoire et retenu par le Projet de Loi en ce qui concerne la prospection directe par courrier électronique (médium le plus utilisé dans l'état actuel des choses) est celui du consentement préalable obligatoire (« *opt-in* »), avec possibilité permanente d'opposition (« *opt-out* »).

Est-ce à dire que les entreprises devront, suite à l'entrée en vigueur de la loi projetée, obtenir le consentement des personnes dont elles avaient déjà obtenu l'adresse électronique, par des investissements probablement très coûteux, et ce licitement sous l'empire de la loi 14 août 2002 relative au commerce électronique, amenée à être modifiée sur ce point par le projet de loi n° 5095 pour prévoir un système de *opt-in* ?

Il serait possible et peut-être raisonnable de prévoir une période de transition pour permettre aux fournisseurs de services disposant d'une base d'adresses de courrier électronique existante de contacter les personnes concernées afin de savoir si elles souhaitent ou non continuer à recevoir des courriers électroniques de prospection direct en provenance de ces fournisseurs de services.

II. DEUXIEME PARTIE : Avis sur les dispositions portant modification de la loi du 2 août 2002

A. Modifications prévues

Le projet de loi sous avis apporte à son article 12. – dispositions transitoires et finales sub (4) un certain nombre de modifications à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Ces modifications visent d'une part à apporter certaines clarifications susceptibles d'éviter des difficultés d'interprétation et d'application des dispositions existantes et de compléter ces dernières sur des points mineurs d'autre part.

Par ailleurs l'article 11 est modifiée à son paragraphe 1er au point b de façon à marquer à l'abri de tout doute que cette condition de légitimité d'un traitement à des fins de surveillance sur le lieu du travail s'applique bien à tous les employeurs quelque soit leur statut, public ou privé.
Une condition de légitimité supplémentaire est ensuite rajoutée sous f) visant à autoriser l'employeur à surveiller – dans le respect des principes de nécessité et proportionnalité s'entend– ses travailleurs pour assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur.

Contrairement à ce que laisse entendre l'exposé des motifs. cette hypothèse s'appliquera aussi bien aux employeurs publics que privés et non seulement à l'Etat.

La Commission nationale s'interroge quant à la nécessité d'englober le terme « recherche» dans le libellé de ce point 11 §1f) nouveau alors que ceux de « prévention et détection » paraissent suffisants et mieux en harmonie avec les observations faites par le Conseil d'Etat au sujet de l'article 10 (document parlementaire 4735/3, p.15).

B. Réflexions supplémentaires

Pour le surplus elle marque son accord avec les modifications proposées. Elle exprime en outre ci-dessous un certain nombre de réflexions et soulève des questions rencontrées dans l'application de la loi qui pourrait le cas échéant conduire le gouvernement à envisager d'autres amendements à proposer.

1. Le consentement

La Commission nationale s'est d'abord posé la question de la conformité à la directive 95/46/CE (éventuel problème de transposition) de la notion de "consentement" telle que définie à l'article 2, lettre (c) de la loi qui s'écarte en partie de la rédaction de la définition contenue dans la directive.

Le législateur luxembourgeois a ajouté les adjectifs « expresse, non équivoque » à la notion de „consentement de la personne concernée" de l'article 2 lettre h) de la directive aux termes duquel le consentement est défini comme étant „toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement",

Si l'ajout du terme « non équivoque » peut encore s'expliquer au regard du terme « indubitablement » que l'on retrouve au niveau des articles 7 lettre a) et 26, paragraphe 1er lettre a) de la directive, il en va autrement du terme « expresse ». En effet, la directive emploie le terme « explicite » uniquement dans le contexte des traitements portant sur des catégories particulières de données (article 8 paragraphe 2 lettre a).

Il en découle que, contrairement à la directive, le législateur luxembourgeois ne permet pas au responsable du traitement de recourir à la condition de légitimité du consentement (article 5, paragraphe 1er, lettre f) de la loi) par une acceptation tacite, fût-elle non équivoque, des traitements qu'il entend mettre en œuvre portant sur des catégories particulières de données dans un contexte autre que celui où des traitements portent sur des catégories particulières de données.

Il va sans dire que les responsables des traitements souhaiteraient pouvoir faire état, du moins dans certaines hypothèses, d'un consentement implicite mais tacite comme critère de légitimation.

La loi nationale est donc sur ce point plus rigoureuse que la directive qu'elle entend transposer.

Par ailleurs, le législateur luxembourgeois ne fait pas de distinction entre le consentement requis en cas de données ordinaires et de données sensibles. Or, la directive opère une distinction sur ce point. Elle requiert le consentement explicite en ce qui concerne le traitement de catégories particulières de données, mais non pour les autres types de données à caractère personnel.

Pour se conformer pleinement à la directive, il nous semblerait préférable de supprimer le terme « expresse » au niveau de la définition du consentement et d'inclure le terme « explicite » à l'article 6, paragraphe 2 lettre a) de la loi du 2 août 2002 qui aurait dorénavant la teneur suivante :
« (a) la personne concernée a donné son consentement explicite à un tel traitement, sauf indisponibilité du corps humain et sauf le cas interdit par la loi, ou lorsque ».

Une telle adaptation de la loi nationale serait aussi de nature à rencontrer le souci exprimé par la Commission européenne dans son rapport publié le 15 mai 2003 sur la mise en œuvre de la directive 95/46/CE de voir réduire les divergences constatées dans les lois des Etats–membres, en particulier au niveau de la rédaction des définitions.

2. L'interconnexion

A) La notion d'"interconnexion" visée à l'article 2, lettre (j) de la loi devrait être clarifiée.

S'il est vrai que dans le projet de loi initial (cf. document parlementaire n°4735/00, page 2), l'interconnexion était définie comme étant "toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour une autre finalité par le même responsable du traitement ou par un ou d'autres responsables du traitement", il n'en reste pas moins que la Commission des Médias et des Communications a adopté le 4 juillet 2002 un amendement au sujet de la notion d'interconnexion (cf. document parlementaire n° 4735/11, page 2) en la redéfinissant comme étant "toute forme de traitement

qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement". C'est cette définition qui a été retenue en définitive par le législateur.

A la lecture du commentaire dudit document parlementaire, il appert qu' *"il s'agit d'une part d'assurer la consistance avec l'article 16 (3) qui vise des finalités identiques ou liées. D'autre part, comme la demande d'interconnexion doit émaner conjointement de* ***plusieurs*** *responsables de traitement,* ***la référence à l'article 2 (j) „au même responsable du traitement" a été supprimée.*** *En effet, en cas de traitements ayant des finalités liées ou identiques effectués par un seul responsable du traitement, une notification unique ou une autorisation unique sont déjà prévues."*

Il s'ensuit que l'on ne saurait parler d'interconnexion de données au niveau d'un seul et même responsable du traitement, alors qu'il convient de lire la définition visée sous l'article 2 lettre (j) comme étant toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par "un autre ou **plusieurs autres**" responsables du traitement.

A part le fait que la définition actuelle prête à confusion, la Commission nationale estime que cette définition est critiquable.

Un traitement issu de la corrélation, par une même personne, de données issues de deux autres traitements initiaux distincts devrait à notre avis être soumis au même régime qu'un traitement consistant en la corrélation, par deux personnes différentes.

Ces deux situations devraient être qualifiées l'une comme l'autre d'interconnexion au risque d'aboutir de façon injustifiée à deux régimes juridiques distincts, ceci, au détriment de la protection de la personne concernée et de façon discriminatoire.

De plus et en opportunité, les grandes sociétés et l'Etat, en tant que grands consommateurs de données à caractère personnel, sont particulièrement exposés à la tentation d'utilisation incompatible avec la finalité déterminée initiale. Or, le régime légal actuel libère bien trop souvent ces acteurs des règles applicables en cas d'interconnexion puisqu'ils pourront rattacher bon nombre de traitements au même responsable (le plus haut possible dans l'organigramme structurel) alors que s'ils considéraient chaque entité spécialisée comme responsable de ses traitements ils seraient bien souvent dans une hypothèse d'interconnexion. En revanche, les PME, professions libérales et individus n'ont pas la possibilité d'échapper à leur guise aux contraintes légales de l'interconnexion.

L'intérêt de la personne concernée ne saurait se satisfaire d'une solution discriminante offrant la protection adéquate seulement aux corrélations entre responsables distincts.

Le champ de l'interconnexion ne devrait pas donc être interprété comme excluant la corrélation de données issues de traitements ayant un seul et même responsable de traitement au risque de vider de son sens l'article 16 de la loi et de générer deux régimes a protection variable sans raison les justifiant.

En toute hypothèse, la CNPD devrait être attentive tant à la qualification de destinataire qu'à celle de responsable de traitement indiquée dans les dossiers de demande d'autorisation ou de notification.

En effet, de nombreux détournements de la loi semblent en perspective, surtout si le régime distinctif est appliqué. Les grandes institutions seront immanquablement tentées d'éviter l'article 16 en groupant tous leurs traitements sous un même chapeau de responsabilité or, selon l'article 2 (o) le responsable de traitement est : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales ».

La Commission nationale propose dès lors de reformuler la définition de l'interconnexion retenue à l'article 2 comme suit :

« (j) "interconnexion": toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité par un responsable du traitement avec des données traitées dans d'autres traitements opérés par le même responsable du traitement ou par d'autres responsables du traitement ».

Cette définition a également le mérite de régler un autre problème résultant du texte actuel. En ne visant que les traitements présentant entre eux des finalités identiques ou liées, la définition actuelle ne règle pas la situation d'une interconnexion de données traitées pour des finalités distinctes et non liées.

Si l'intention du législateur consistait à interdire en application de l'article 16 de la loi de telles interconnexions, il convient de ne pas les exclure de la définition retenue à l'article 2 lettre (j) de la loi et donc d'en biffer les termes « finalités identiques ou liées » .

C'est ainsi que l'article 16 paragraphe 3 de la loi trouvera pleinement application en posant comme condition *sine qua non* de licéité d'une interconnexion de données le respect de finalités identiques ou liées de fichiers. A contrario, sont prohibées au regard de l'article 16 paragraphe 3 les interconnexions des données traitées pour des finalités distinctes et non liées.

B) La Commission nationale relève par ailleurs qu'une interconnexion opérée par (le même ou) par différents responsables des traitements ne pourra être autorisée (par la loi ou la Commission nationale) que pour des traitements portant sur des finalités compatibles, tandis que le cas d'autorisation visé par l'article 14 paragraphe 1er lettre e) relatif à l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées permet d'utiliser ultérieurement des données pour des finalités incompatibles.

3. La notion d'activités domestiques

L'article 3, paragraphe 5, de la loi dispose que celle-ci ne s'applique pas « au traitement mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques ».

Qu'en est-il de la surveillance sur le lieu de travail (soumise à l'autorisation préalable de la Commission nationale en vertu des articles 11 et 14) appliquée au travailleur domestique ?

La ratio legis doit amener la Commission nationale à décider qu'un tel traitement tombe bel et bien sous le champ d'application de la loi, puisqu'il ne s'agit pas à proprement parler d'une activité domestique du responsable du traitement, mais la personne physique occupant une femme de charge à son domicile privée est employeur et en cette qualité il met en œuvre un traitement à des fins professionnelles sujet à autorisation.

A supposer qu'une telle autorisation soit accordée, un problème peut se poser au niveau de l'exécution des missions incombant à la Commission nationale.

Aux termes de l'article 32, paragraphe (11) de la loi *« Quiconque empêche ou entrave sciemment, de quelque manière que ce soit, l'accomplissement des missions incombant à la Commission nationale, est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. Est considéré comme empêchant ou entravant sciemment l'accomplissement des missions incombant à la Commission nationale, le refus opposé à ses membres de donner accès aux locaux autres que les locaux d'habitation, où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés ».*

Concrètement, il n'y a pas de délit d'entrave pour le responsable du traitement qui refuse de donner accès à ses locaux d'habitation aux données faisant l'objet d'un traitement à des fins de surveillance de l'ouvrier domestique qu'il occupe. Est-ce possible que dans ce cas la notion de « local d'habitation » cède le pas à la notion de « lieu de travail » ?

Comment la Commission peut-elle en pareil cas exécuter sa mission fondamentale consistant à contrôler et à vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de la présente loi et de ses règlements d'exécution ?

Il appartient au législateur de lever cette contradiction.

4. L'article 4, paragraphe (2) de la loi

Aux termes de l'article 4, paragraphe (2), les données traitées à des finalités déterminées peuvent être traitées ultérieurement à des fins historiques, statistiques ou scientifiques et sont soumises aux conditions prévues par le régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14.

Il serait utile d'intégrer dans ce paragraphe l'idée contenue dans le considérant 29 de la directive 95/46/CE qui énonce que « le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques n'est pas considéré en général comme incompatible avec les finalités pour lesquelles les données ont été auparavant collectées, dans la mesure où les États membres prévoient des garanties appropriées; que ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne ».

Voir également en ce sens l'article 6, paragraphe 1, lettre b, de la directive aux termes duquel *« ...Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ».*

La Commission nationale propose dès lors de donner la teneur suivante à l'article 4, paragraphe (2) de la loi :

« Un traitement ultérieur de données à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible avec les finalités déterminées pour lesquelles les données ont été auparavant collectées et est soumis aux conditions prévues par le régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14. »

5. Les articles 6 et 7

A) Suivant l'article 6 paragraphe 4, lettre a) de la loi « Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi ».

La Commission nationale émet les plus grandes réserves quant à l'opportunité de permettre - comme le prévoit le texte actuel - à tous les responsables des traitements visés à l'article 7 paragraphe 1 de la loi de traiter des données génétiques, étant donné que pour la majorité des instances y visées une telle faculté s'avère très dangereuse pour les « personnes concernées ».

En tout état de cause, la Commission nationale est d'avis que pour des raisons de non proportionnalité le traitement de données génétiques ne saurait se justifier dans le chef des entreprises d'assurances ou des sociétés gérant les fonds de pension. Il ne résulte d'ailleurs aucunement des travaux parlementaires pour quelles raisons ces acteurs économiques ont été ajoutés à la liste des « services de la santé » .

B) Suivant l'article 7, paragraphe (4) de la loi du 2 août 2002, sous réserve que leur traitement soit en lui-même licite au regard des articles 6 et 7, les données y visées peuvent être communiquées à des tiers ou utilisées à des fins de recherche, d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal.

Aux termes de l'article 28-1, paragraphes 4 et 5, de la loi du 30 septembre 1992 modifiant la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques :

« (4) Un règlement grand-ducal pris sur avis du Conseil d'Etat détermine:
— les modalités d'après lesquelles les banques de données médicales peuvent être créées et exploitées;
— les modalités d'après lesquelles les données médicales peuvent être collectées et traitées;
— les conditions à observer afin de garantir la sécurité technique et le caractère confidentiel des données médicales collectées et traitées;
— les modalités d'après lesquelles les données médicales peuvent être communiquées à un tiers;
— les modalités d'après lesquelles les données médicales peuvent être utilisées à des fins de recherche.
Ce règlement peut aussi compléter les dispositions prévues aux chapitres 2 à 6 de la présente loi.
(5) La communication de données relatives à des prestations médicales, faite par le fournisseur de soins à un organisme de sécurité sociale aux fins de remboursement des dépenses afférentes est autorisée.»

Quant aux dispositions transitoires arrêtées dans la loi du 2 août 2002, celles-ci prévoient que:

« Avec l'entrée en vigueur de la loi, la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est abrogée.

Cependant „pour autant qu'ils ne sont pas contraires aux dispositions de la présente loi, les règlements pris en exécution de la loi modifiée du 31 mars 1979 précitée resteront en vigueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions". Il s'agit de combler le vide juridique qui résulterait d'une abrogation expresse des règlements grand-ducaux pris en exécution de la loi modifiée du 31 mars 1979. Les règlements d'exécution, trouvant une base légale suffisante dans le nouveau texte, resteront en vigueur jusqu'à ce qu'il est pourvu à leur remplacement par de nouvelles dispositions » (document parlementaire 4735/13, p. 45)

Il en découle que le paragraphe 5 de l'article 28-1 de la loi modifiée du 31 mars 1979 ayant pour objet d'autoriser le système du tiers payant se trouve abrogé depuis le 1er décembre 2002, date d'entrée en vigueur de la nouvelle loi du 2 août 2002, sans qu'une nouvelle base légale n'ait été créée en échange.

Dans ces circonstances il paraît urgent de voir pallier à cette lacune. Le législateur entendait sans doute que ceci se ferait dans le cadre du règlement grand-ducal prévu à l'article 7 paragraphe (4) de la loi du 2 août 2002 appelé à déterminer les modalités et les conditions suivant lesquelles les données visées aux articles 6 et 7 peuvent être communiquées à des tiers ou utilisées à des fins de recherche, sous réserve que leur traitement soit en lui-même licite. Ce règlement n'est cependant pas encore intervenu. Il est vrai que l'article 44 paragraphe (2) dispose que les règlements d'exécution de l'ancienne loi trouvant une base légale suffisante dans le nouveau texte resteront en vigueur jusqu'à ce qu'il soit pourvu à leur remplacement par de nouvelles dispositions et a explicitement visé à ce titre le règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation de données nominatives médicales dans les traitements informatiques. Or ce règlement ne règle pas la communication de données relatives à la santé dans le cadre du système du tiers payant, puisque ceci faisait l'objet d'une disposition légale expresse.

Quant aux conditions générales pour la communication de données médicales à des tiers prévues au chapitre IV de ce règlement grand-ducal du 2 octobre 1992 réglementant l'utilisation de données nominatives médicales dans les traitements informatiques, elles donnent lieu à une difficulté supplémentaire. L'article 16 (2) prévoit en effet que « *le consentement écrit n'est pas requis lorsque l'intérêt direct du malade exige la communication et qu'il y a lieu de présumer le consentement »* Il apparaît douteux en effet que la notion de *consentement présumé »* soit compatible avec la définition du consentement de la loi du 2 août 2002. En outre l'hypothèse envisagée présuppose que la personne concernée puisse être considérée comme *« malade »* et a recours à la notion *d'intérêt direct* non définie par ailleurs et nettement plus large que celle de *« sauvegarde de l'intérêt vital » employée par la loi* du 2 août 2002 aux articles 5 paragraphe 1er lettre(e) et 6 paragraphe (2) lettre (c)

Une clarification semble donc s'imposer, soit par la voie d'un règlement grand-ducal à prendre conformément à l'article 7 paragraphe (4) de la loi du 2 août 2002 appelé à déterminer les modalités et les conditions suivant lesquelles les données visées aux articles 6

et 7 peuvent être communiquées à des tiers ou utilisées à des fins de recherche, soit par de nouvelles dispositions venant compléter la loi à ce sujet.

6. L'article 9 : liberté d'expression

Concernant les modifications proposées à l'article 9, la Commission nationale renvoie à son avis substantiel émis dans le cadre du projet de loi n° 4910 sur la liberté d'expression dans les médias (cf. document parlementaire n° 4910/09).

7. L'article 10

A) Aux termes de l'article 10, paragraphe 1er, lettre (a) le traitement à des fins de surveillance peut être autorisé si la personne concernée a donné son consentement.

Les travaux parlementaires ne donnent aucun exemple pour cette condition de légitimité.

Si cette condition de légitimité peut certes viser l'hypothèse du client donnant son accord pour l'enregistrement des conversations téléphoniques avec sa banque afin de permettre à cette dernière de prouver des transactions commerciales, elle cadre mal avec le cas du malade (inconscient) se trouvant dans l'incapacité physique de donner son consentement mais qui est mis sous (vidéo) surveillance continue, en particulier en cas de réanimation médicale.

Un autre cas visé pourrait être celui des personnes dangereuses placées sous vidéosurveillance par exemple en garde à vue dans un milieu neuro-psychiatrique ou pénitentiaire enfermées dans un cabanon (« *Gummizelle* »).

A notre sens, on devrait également reprendre au niveau de l'article 10 (1) lettre a) le cas de figure réglé à l'article 6 paragraphe 2 lettre c) qui couvre les hypothèses où des données relatives à la santé sont traitées en dehors du contexte de la surveillance. La Commission nationale propose donc à cet effet de rajouter au paragraphe 1^{ier} de l'article 10 un point d) libellé comme suit :

(d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

B) De l'avis de la Commission nationale, les notions de « sécurité des usagers » et « prévention des accidents » inscrites à l'article 10, paragraphe 1, lettre (b) **n'englobent pas le cas des actes de vandalisme (dans les bus ou dans les gares etc.) ou les vols de biens.**

Dans un souci de cohérence au niveau des articles 10 et 11 de la loi, il apparaît cependant que ces hypothèses peuvent constituer des causes légitimes de recours à des traitements à des fins de surveillance.

La Commission nationale propose dès lors de modifier le texte légal en conséquence en ajoutant « la protection des biens » sous l'article 10, paragraphe 1er lettre b), pour y inclure notamment les vols ou les actes de vandalisme, d'autant plus que cette situation est d'ores et déjà réglée sous la lettre b) du premier paragraphe de l'article 11 relatif aux traitements à des fins de surveillance sur le lieu de travail.

8. L'article 11

La Commission nationale estime en revanche qu'il convient de biffer les termes « de l'entreprise » au niveau de l'article 11 § 1 lettre b), au motif qu'il existe encore d'autres personnes intéressées que l'employeur dont les biens méritent une protection, protection qui pourrait constituer une condition de légitimité au titre de la surveillance envisagée sur le lieu de travail. (Cette observation vaut également pour le nouveau libellé prévu dans le projet de loi sous avis : *« quelque soit le statut, public ou privé, de l'employeur »).*

En effet, comme la condition de légitimité indiquée sous le point b) du premier paragraphe de l'article 11 couvre exclusivement un traitement à des fins de surveillance sur le lieu de travail « pour les besoins de protection des biens de l'entreprise », il en découle nécessairement « a contrario » que les biens appartenant aux autres salariés qui sont déposés dans leur vestiaire personnel ne sont pas couverts par cette condition de légitimité en cas de vol perpétré par un de leurs collègues de travail.

En pareil cas, l'employeur ne peut faire bénéficier son salarié, victime du vol, des preuves collectées par un appareil pour lequel il a obtenu une autorisation pour protéger ses propres biens.

9. L'article 14

Dans le cadre du projet de loi n° 5181, il conviendrait également prévoir pour les engagements formels de conformité (pris en application de l'article 14, paragraphe 3, de la loi) au niveau du nouveau paragraphe 5 du même article la perception d'une redevance à fixer par règlement grand-ducal.

Le tarif serait sans doute plus modeste pour tenir compte de l'article 37, paragraphe 4, de la loi aux termes duquel :

« La Commission nationale est autorisée à prélever la contrepartie de ses frais du personnel en service et de ses frais de fonctionnement par la redevance à percevoir telle que prévue à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat. »

10. L'article 15

Aux termes du premier paragraphe de l'article 19 de la directive 95/46/CE „les Etats membres précisent les informations qui doivent figurer dans la notification qui comprennent entre autres au minimum le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant.

L'article 13, paragraphe 1er de la loi du 2 août 2002 prévoit en outre l'indication du sous-traitant.

Comme les clients des experts-comptables et réviseurs d'entreprises par exemple devront indiquer ces professionnels dans leurs notifications comme sous-traitants, la publicité conférée de cette manière à ces informations par le biais du registre public des traitements en

ligne permettrait de reconstituer les bases de clientèle de chaque cabinet luxembourgeois de révision et d'expert-comptable.

Dans un souci de sauvegarder la confidentialité de la clientèle des professionnels en cause, nous suggérons donc de supprimer le bout de phrase relatif au sous-traitant au niveau du premier paragraphe.

11. L'article 26 : le droit à l'information de la personne concernée

Le « droit à l'information de la personne concernée » est réglementé par l'article 26 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel qui prévoit en son paragraphe 1er lettre c) (lorsque les données sont collectées directement auprès de la personne concernée):

« (c) toute autre information supplémentaire telle que:
– les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
– le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
– la durée de conservation des données. »

Le paragraphe 2 lettre c) (lorsque les données n'ont pas été collectées auprès de la personne concernée) du même article dispose :

« (c) toute information supplémentaire telle que:
– les catégories de données concernées;
– les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
– la durée de conservation des données. »

Le législateur luxembourgeois s'est inspiré de la rédaction de la directive 95/46 CE du Parlement Européen et du Conseil du 24 octobre 1995 en reprenant aux paragraphes (1) et (2) de l'article 26 presque textuellement les deux modalités d'information de la personne concernée visées aux articles 10 et 11 de la directive (doc. parl. 4735/13 p. 23). Les articles 10 et 11 règlent la question de l'information en cas de collecte de données de la manière suivante :

Article 10
Informations en cas de collecte de données auprès de la personne concernée
Les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:
a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
b) les finalités du traitement auquel les données sont destinées;
c) toute information supplémentaire telle que :
- les destinataires ou les catégories de destinataires des données,

- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,
dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Article 11
Informations lorsque les données n'ont pas été collectées auprès de la personne concernée
1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les États membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:
a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
b) les finalités du traitement;
c) toute information supplémentaire telle que:
- les catégories de données concernées,
- les destinataires ou les catégories de destinataires des données,
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,
dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2. Le paragraphe 1 ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées.

Quant à **l'étendue de l'obligation d'information**, il résulte clairement des articles 10 et 11 que les informations tombant dans la catégorie « toute information supplémentaire » ne doivent être fournies à la personne concernée que « dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ».

La directive pose ainsi le principe de nécessité applicable en la matière en fonction du traitement mis en œuvre par le responsable du traitement.

Force est de constater que la loi luxembourgeoise est moins flexible en ayant omis de transposer également le bout de phrase « *dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ».*

S'il est vrai que l'on peut et doit interpréter et appliquer l'article 26 à la lumière des articles 10 et 11 de la directive, toujours est-il qu'un ajout légal au texte actuel enlèverait un élément d'insécurité juridique quand à la lecture qu'il convient de faire de ce texte qui ne donnerait plus ainsi lieu à des critiques éventuelles.

D'ailleurs, il résulte des travaux parlementaires que l'intention du législateur était dictée par les mêmes considérations de souplesse que celles inscrites à la directive.

« Le responsable du traitement devra fournir toutes les informations supplémentaires nécessaires, compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière. La liste de ces informations supplémentaires n'est pas exhaustive. Ainsi, par exemple, si les données n'ont pas été fournies par la personne concernée, celle-ci peut, suivant les cas, être en droit de connaître l'identité de la personne ayant fourni des données la concernant. De même l'article 30, paragraphe (1) lettres (b) et (c), oblige le responsable du traitement à informer la personne concernée de l'existence d'un droit d'opposition en cas de traitement à des fins de prospection. » (document parlementaire 4735/13, p. 24).

Les lettres c) du paragraphe 1er et 2 de l'article 26 de la loi auraient dorénavant la teneur suivante :

Le paragraphe 1er lettre c) :

« (c) toute autre information supplémentaire telle que:
– les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
– le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
la durée de conservation des données,
dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. »

Le paragraphe 2 lettre c) :

« (c) toute information supplémentaire telle que:
– les catégories de données concernées;
– les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
la durée de conservation des données,
dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données»

12. L'article 32

Conformément à l'article 32, paragraphe 7, la Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle a accès aux données faisant l'objet du traitement en question.

Elle recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. A cette fin elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

La CNPD regrette cependant que cet article omet de préciser si les membres de la CNPD ont la qualité d'officiers de police judiciaire, ou si la CNPD peut requérir les forces de l'ordre pour l'assister dans l'accomplissement de ses missions légales.

Dans la négative, il faudrait l'ajouter à cet article, et ce indépendamment du fait que le délit d'entrave est visé à l'article 32 paragraphe 11 disposant que « Est considéré comme empêchant ou entravant sciemment l'accomplissement des missions incombant à la Commission nationale, le refus opposé à ses membres de donner accès aux locaux autres que les locaux d'habitation, où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés. »

Dans ce contexte, le législateur pourrait notamment s'inspirer de la loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes oeuvrant dans les domaines social, familial et thérapeutique qui dispose en son article 9 :

« Chaque ministre prévu à l'article 1er de la présente loi est chargé, pour les activités qui le concernent, de surveiller et de contrôler la conformité de ces activités avec les dispositions de la présente loi.
Dans le cadre de sa mission de surveillance et de contrôle chaque ministre désigne un ou plusieurs fonctionnaires de l'Etat, soit de la carrière supérieure soit de la carrière moyenne relevant du cadre fermé, avec la mission de rechercher et de constater des infractions à la présente loi et à ses règlements d'exécution, le tout sans préjudice des pouvoirs reconnus aux officiers et agents de police judiciaire de la gendarmerie et de la police.
Dans l'exercice de leurs fonctions relatives à la présente loi, les fonctionnaires visés ci-avant ont la qualité d'officier de police judiciaire. Ils constatent les infractions par des procès-verbaux faisant foi jusqu'à preuve contraire. Leur compétence s'étend sur tout le territoire du Grand-Duché.
Avant d'entrer en fonctions, ils prêtent devant le tribunal d'arrondissement de leur domicile le serment suivant: «Je jure de remplir mes fonctions avec intégrité, exactitude et impartialité.»
L'article 458 du code pénal leur est applicable.
Les fonctionnaires prévus ci-avant ont accès aux locaux, terrains et moyens de transport des personnes et organismes assujettis à la présente loi. Ils peuvent pénétrer même pendant la nuit, lorsqu'il existe des indices graves faisant présumer une infraction à la présente loi, dans les locaux, terrains et moyens de transport visés ci-dessus. Ils signalent leur présence au chef de l'organisme ou à celui qui le remplace. Celui-ci a le droit de les accompagner lors de la visite. »

Une autre alternative consisterait à intégrer la faculté pour la Commission nationale de requérir la force publique en cas de besoin, telle que prévue à l'article 13 de la loi du 4 avril 1974 portant réorganisation de l'Inspection du travail et des mines :

« S e c t i o n 1. - Pouvoirs du personnel
Art. 13. (1) Le personnel d'inspection et le personnel de contrôle muni de pièces justificatives de ses fonctions est autorisé :

a) à pénétrer librement sans avertissement préalable, à toute heure du jour et de la nuit dans tout établissement assujetti au contrôle de l'inspection du travail; le droit de libre accès s'étend à toutes les dépendances des entreprises;
b) à pénétrer le jour dans tous les locaux qu'il peut avoir un motif raisonnable de supposer être assujettis au contrôle de l'inspection du travail et des mines.
Les dispositions du présent paragraphe ne sont pas applicables aux locaux qui servent à l'habitation.
(2) Lorsque le personnel visé au paragraphe (1) qui précède rencontre des difficultés à l'occasion de ses visites, il peut requérir les chefs locaux de la gendarmerie et de la police qui lui prêteront main forte.
(3) A l'occasion de l'exercice des droits visés au paragraphe (1) qui précède, le personnel d'inspection et le personnel de contrôle est tenu d'informer l'employeur ou son représentant ainsi que le président de la délégation ouvrière et, le cas échéant, le président de la délégation des employés de l'entreprise de sa présence.
(4) Il n'en est pas ainsi toutefois lorsqu'il estime que l'information prévue à l'alinéa qui précède risque de porter préjudice à l'efficacité du contrôle; dans ce dernier cas, le directeur de l'inspection du travail, ou, en cas d'empêchement, «l'un des directeurs adjoints»1 devra en être informé préalablement. »

13. L'article 36

L'étendue des missions de la Commission nationale, en particulier celles comportant de vastes et complexes recherches juridiques, l'élaboration d'avis et de recommandations ainsi celles relatives aux mesures de sécurité à respecter par les responsables des traitements, le recrutement à un stade à déterminer d'un juriste et d'un informaticien (ingénieur diplômé ou ingénieur technicien) auprès de la Commission nationale sous le statut de fonctionnaire s'impose afin de garantir le bon fonctionnement de l'établissement public.

Par conséquent, le cadre du personnel de la Commission nationale doit être étendu aux fonctions et emplois suivants :

« a) dans la carrière supérieure de l'attaché de direction:
- des conseillers de direction 1ère classe ou
- des conseillers de direction ou
- des conseillers de direction adjoints ou
- des attachés de direction 1ers en rang ou
- des attachés de direction.
b) dans la carrière supérieure de l'ingénieur:
- des ingénieurs 1ère classe;
- des ingénieurs chef de division;
- des ingénieurs principaux ou ingénieurs-inspecteurs ou ingénieurs;»
c) dans la carrière moyenne de l'ingénieur technicien:
- des ingénieurs techniciens inspecteurs principaux premiers en rang;
- des ingénieurs techniciens inspecteurs principaux;
- des ingénieurs techniciens inspecteurs;
- des ingénieurs techniciens principaux;
- des ingénieurs techniciens. »

L'article 37 paragraphe 4

En raison du fait que le projet de loi (n° 5181) prévoit également la perception d'une redevance pour les demandes d'autorisation préalable à introduire auprès de la Commission nationale, il convient de mentionner l'article 14 à l'article 37 paragraphe 4 de la loi, paragraphe qui aurait dorénavant la teneur suivante :

«(4) La Commission nationale est autorisée à prélever la contrepartie de ses frais du personnel en service et de ses frais de fonctionnement par la redevance à percevoir telle que prévue aux articles 13 et 14 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat. »

Ainsi décidé à Esch-sur-Alzette en date du 20 février 2004

La Commission nationale pour la protection des données

Gérard Lommel	Edouard Delosch	Pierre Weimerskirch
Président	Membre effectif	Membre effectif