

N° 5181

CHAMBRE DES DEPUTES

Session ordinaire 2002-2003

PROJET DE LOI

- relatif aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques,
- portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle, et
- portant modification de la loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel

* * *

*(Dépôt: le 11.7.2003)***SOMMAIRE:**

	<i>page</i>
1) Arrêté Grand-Ducal de dépôt (30.6.2003)	1
2) Texte du projet de loi	2
3) Exposé des motifs et commentaire des articles	11

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre délégué aux Communications et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.— Notre Ministre délégué aux Communications est autorisé à déposer en Notre nom à la Chambre des Députés

- le projet de loi sur les réseaux et les services de communications électroniques;
- le projet de loi portant organisation de la gestion des ondes radioélectriques;
- le projet de loi portant réorganisation de l'Institut Luxembourgeois de Régulation;
- le projet de loi
 - relatif aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques,
 - portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle, et
 - portant modification de la loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel.

Palais de Luxembourg, le 30 juin 2003

Le Ministre délégué aux Communications,

François BILTGEN

HENRI

TEXTE DU PROJET DE LOI

Art. 1er.– *Champ d'application*

Sans préjudice de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et de la législation sur les réseaux et les services de communications électroniques; les dispositions spécifiques de la présente loi s'appliquent au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics.

Art. 2.– *Définitions*

Aux fins de la présente loi on entend par:

- (a) „abonné“: une personne physique ou morale partie à un contrat avec une entreprise offrant des services de communications électroniques accessibles au public, pour la fourniture de tels services;
- (b) „appel“: une connexion établie au moyen d'un service téléphonique accessible au public permettant une communication bidirectionnelle en temps réel;
- (c) „consentement“: toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle l'utilisateur ou l'abonné accepte que les données à caractère personnel fassent l'objet d'un traitement;
- (d) „communication“: toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public à l'exception des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques sauf si et dans la mesure où un lien peut être établi entre l'information et l'abonné ou l'utilisateur identifiable qui la reçoit;
- (e) „courrier électronique“: tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau de communications public, qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère;
- (f) „données relatives au trafic“: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;
- (g) „données de localisation“: toutes les données traitées dans un réseau de communications électroniques qui comportent des indications sur la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;
- (h) „réseau de communications électroniques“: les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;
- (i) „réseau de communications public“: un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public. Le fournisseur du réseau de communications public est dénommé ci-après „opérateur“;
- (j) „service de communications électroniques“: un service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur les réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus; il ne comprend pas les services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques. Le fournisseur de services de communications électroniques est dénommé ci-après „fournisseur de services“;
- (k) „service à valeur ajoutée“: tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation;

- (l) „utilisateur“: une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public;
- (m) „utilisateur final“ un utilisateur qui ne fournit pas de réseaux de communications publics ou de services de communications électroniques accessibles au public.

Art. 3.– Sécurité

(1) Le fournisseur de services prend les mesures techniques et d'organisation appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec l'opérateur en ce qui concerne la sécurité du réseau. En cas d'atteinte ou de risque d'atteinte grave à la sécurité du réseau et/ou des services, le fournisseur de services et le cas échéant l'opérateur prend les mesures appropriées pour y remédier, les frais étant à sa seule charge.

(2) Sous réserve de ce qui précède, le fournisseur de services et le cas échéant l'opérateur informe ses abonnés de tout risque imminent d'atteinte à la sécurité du réseau et/ou des services mettant en cause la confidentialité des communications ainsi que du moyen éventuel pour y remédier, y compris du coût probable que cela implique.

Art. 4.– Confidentialité des communications

(1) Tout fournisseur de services et/ou opérateur assure la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes.

(2) 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.

(3) Le paragraphe (2):

- (a) n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité;
- (b) ne s'applique pas aux autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle conformément aux législations en vigueur pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales;
- (c) ne s'applique pas aux communications et aux données relatives au trafic y afférentes, effectuées à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut dans le seul but de permettre (a) la réécoute de messages lors de problèmes de compréhension ou d'ambiguïté entre l'appelant et l'appelé, (b) la documentation de fausses alertes, de menaces et d'appels abusifs et (c) la production de preuves lors de contestation sur le déroulement d'actions de secours.

Les données relatives au trafic y afférentes dont les données de localisation sont à effacer une fois le secours apporté. Le contenu des communications est à effacer après un délai de 6 mois,

- (d) 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. Dans pareil cas, les parties aux communications doivent 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 de conservation de l'enregistrement. La communication enregistrée est effacée dès que la finalité est atteinte, et en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction;
- (e) ne s'applique pas lorsque les moyens de communications électroniques servent à stocker des informations ou à accéder à des informations stockées dans l'équipement terminal d'un abonné, d'un utilisateur ou d'un utilisateur final moyennant utilisation de témoins de connexion („cookies“) ou de dispositifs analogues à condition que ceux-ci soient utilisés à des fins légitimes et que le responsable du traitement qui les expédie ou qui permet à un tiers de les expédier fournisse à l'abonné,

l'utilisateur ou l'utilisateur final des informations claires, précises et complètes au sens de l'article 26 la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel dont sur la ou les finalité(s) du traitement en question nonobstant le droit de ce dernier de s'opposer gratuitement, sans indication de motif et à tout moment à un tel traitement. Cette disposition ne fait pas obstacle à un stockage ou un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné, l'utilisateur ou l'utilisateur final.

(4) Quiconque contrevient aux dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 5.– Données relatives au trafic

- (1) (a) Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services et/ou opérateur qui traite des données relatives au trafic est tenu de conserver ces données pendant une période de 12 mois. La Commission nationale pour la protection des données peut, après consultation de l'Institut, des autorités judiciaires et des autorités compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle, désigner les catégories de données non susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite des infractions pénales.
- (b) Après la période de conservation prévue sub (a), le fournisseur de services et/ou l'opérateur est obligé d'effacer les données relatives au trafic concernant les abonnés, les utilisateurs et les utilisateurs finals, ou de les rendre anonymes.

(2) Tout fournisseur de services et/ou tout opérateur qui traite des données relatives au trafic concernant les abonnés, les utilisateurs et les utilisateurs finals, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication et/ou aux traitements prévus par les dispositions sub (3) et (4), à l'exception des accès qui sont:

- ordonnées par les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle conformément aux législations en vigueur pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales; ou
- demandées par les organes compétents conformément à la législation en vigueur dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation.

(3) Les données relatives au trafic qui sont nécessaires en vue d'établir les factures des abonnés et aux fins des paiements d'interconnexion peuvent être traitées. Un tel traitement n'est possible que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

(4) Les données relatives au trafic peuvent être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services pour autant que le fournisseur d'un service de communications électroniques et/ou l'opérateur informe préalablement l'abonné, l'utilisateur ou l'utilisateur final concerné des types de données relatives au trafic traitées, de la finalité et de la durée du traitement et que celui-ci ait donné son consentement nonobstant son droit de pouvoir s'opposer à tout moment à un tel traitement.

(5) Le traitement des données relatives au trafic effectué dans le cas des activités visées aux paragraphes (1) (b); (3) et (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services

et/ou de l'opérateur qui sont chargées d'assurer la facturation et/ou la gestion du trafic, répondre aux demandes de clientèle, détecter les fraudes, commercialiser les services de communications électroniques ou pour fournir un service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(6) Quiconque contrevient aux dispositions des paragraphes (1), (2), (4), (5) du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 6.– Facturation détaillée

(1) Tout abonné a le droit de recevoir une facture non détaillée.

(2) Les appels gratuits y compris ceux aux services d'urgence et d'alerte ne sont pas indiqués sur la facture détaillée indépendamment de son degré de détail. En outre la facture détaillée ne contient aucune indication permettant d'identifier l'appelé.

Art. 7.– Identification de la ligne appelante et de la ligne connectée

(1) Dans le cas où la présentation de l'identification de la ligne appelante est offerte en tant que service, le fournisseur du service permet à l'abonné et à l'utilisateur appelant d'empêcher, par un moyen simple et gratuit, la présentation de l'identification de la ligne appelante, et ce appel par appel. L'abonné appelant dispose de cette possibilité de manière permanente pour chaque ligne.

(2) Dans le cas où la présentation de l'identification de la ligne appelante est offerte en tant que service, l'abonné appelé doit pouvoir empêcher, par un moyen simple et gratuit pour un usage raisonnable de cette fonction, la présentation de l'identification de la ligne pour les appels entrants.

(3) Dans le cas où la présentation de l'identification de la ligne appelante est offerte en tant que service et où l'identification de la ligne appelante est présentée avant l'établissement de l'appel; l'abonné appelé doit pouvoir, par un moyen simple et gratuit, refuser les appels entrants lorsque l'utilisateur ou l'abonné appelant a empêché la présentation de l'identification de la ligne appelante.

(4) Dans le cas où la présentation de l'identification de la ligne connectée est offerte, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, empêcher la présentation de l'identification de la ligne connectée auprès de la personne qui appelle.

(5) Pour les appels effectués à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut, l'identification de la ligne appelante est toujours présentée même lorsque l'appelant l'a empêché.

(6) Les dispositions du paragraphe 1e s'appliquent également aux appels provenant de l'Union européenne à destination de pays tiers. Les dispositions des paragraphes (2), (3) et (4) s'appliquent également aux appels entrants provenant de pays tiers.

(7) Le fournisseur du service informe le public, par des moyens appropriés et au plus tard lors de la conclusion d'un contrat des possibilités susénoncées.

(8) L'abonné appelé prétendant être victime d'appels anonymes à contenu malveillant peut obtenir l'identification de la ligne appelante ou connectée, des appels répétés ou intempestifs, déclarés comme étant malveillants, lesquels ont été effectués ou repérés sur base d'un même numéro d'appel ou d'un même raccordement.

Un règlement grand-ducal fixera les modalités à respecter par le fournisseur du service et/ou l'opérateur ainsi que par les abonnés prétendant être victime d'appels anonymes à contenu malveillant. Il précisera également les caractéristiques d'un appel à contenu malveillant et déterminera l'utilisation de l'identification de la ligne appelante même si sa présentation est empêchée.

(9) Quiconque contrevient aux dispositions du présent article 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. La juridiction

saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 8.– Renvoi automatique d'appels

Dans le cas où le renvoi automatique d'appels (ou déviation) est offert en tant que service, le fournisseur du service confère à tout abonné la possibilité de mettre fin, par un moyen simple et gratuit, au renvoi automatique d'appels par un tiers vers son appareil terminal lorsque le fournisseur du service peut identifier l'origine des appels renvoyés. Le cas échéant, cette identification se fait en collaboration avec d'autres fournisseurs de services concernés.

Art. 9.– Données de localisation autres que les données relatives au trafic

(1) (a) Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services et/ou opérateur qui traite des données de localisation autres que des données relatives au trafic est tenu de conserver ces données pendant une période de 12 mois. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou par appel. La Commission nationale pour la protection des données peut, après consultation de l'Institut des autorités judiciaires et des autorités compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle, désigner les catégories de données non susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite des infractions pénales.

Les données de localisation autres que les données relatives au trafic sont également communiquées au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut.

(b) Après la période de conservation prévue sub (a), le fournisseur de services et/ou l'opérateur est obligé d'effacer les données de localisation autres que les données relatives au trafic concernant les abonnés, les utilisateurs et les utilisateurs finals, ou de les rendre anonymes.

(2) Tout fournisseur de services et/ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés, les utilisateurs et les utilisateurs finals, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données, à l'exception des accès qui sont ordonnés par les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle conformément aux législations en vigueur pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales.

(3) Tout fournisseur de services et/ou opérateur ne peut traiter des données de localisation, autres que les données relatives au trafic, concernant les abonnés, utilisateurs et les utilisateurs finals, que si celles-ci ont été rendues anonymes ou moyennant le consentement exprès de l'abonné, de l'utilisateur ou de l'utilisateur final, dans la mesure et pour la durée nécessaire à la fourniture d'un service à valeur ajoutée sous réserve des dispositions (2), (4) et (5).

(4) Le fournisseur du service et le cas échéant l'opérateur informe préalablement l'abonné, l'utilisateur ou l'utilisateur final sur les types de données de localisation traitées, autres que les données relatives au trafic, sur la ou les finalité(s) et la durée de ce traitement ainsi que sur la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée et que l'abonné, l'utilisateur ou de l'utilisateur final doit avoir donné son consentement et nonobstant son droit de s'opposer gratuitement, sans indication de motif et à tout moment à un tel traitement.

Dans le cas du traitement de données de localisation, autres que les données relatives au trafic, l'abonné, l'utilisateur ou l'utilisateur final doit avoir la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

(5) Le traitement effectué des données de localisation, autres que les données relatives au trafic, dans le cas des activités visées aux paragraphes (1)(b), (3) et (4) est restreint aux personnes agissant sous

l'autorité du fournisseur de services et/ou de l'opérateur ou du tiers qui fournit le service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(7) Quiconque contrevient aux dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 10.– *Annuaire d'abonnés*

(1) L'abonné, doit être informé gratuitement et au plus tard lors de la souscription de l'abonnement, des fins auxquelles sont établis des annuaires d'abonnés imprimés ou électroniques accessibles au public (ci-après „les annuaires“) ou consultables par l'intermédiaire de services de renseignements, dans lesquels les données le concernant peuvent figurer, ainsi que de toute autre possibilité d'utilisation reposant sur des fonctions de recherche intégrées dans les versions électroniques des annuaires.

(2) (a) L'abonné doit avoir la possibilité d'indiquer clairement, lors de la souscription de l'abonnement ou à tout autre moment lors de nouvelles éditions de mises à jour ou d'annuaires, si les données à caractère personnel le concernant, et lesquelles de ces données doivent figurer dans un annuaire public, dans la mesure où ces données sont pertinentes par rapport à la fonction de l'annuaire en question telle qu'elle a été établie par le fournisseur de l'annuaire.

(b) L'abonné doit pouvoir vérifier, corriger ou supprimer ces données. La non-inscription dans un annuaire public d'abonnés, la vérification, la correction ou la suppression de données à caractère personnel dans un tel annuaire est gratuite.

(3) Le traitement de données à des fins d'annuaire autres que la simple recherche des coordonnées d'un abonné sur la base de son nom et, au besoin, d'un nombre limité d'autres paramètres n'est possible que si l'abonné a donné son consentement préalable nonobstant son droit de s'opposer gratuitement, sans indication de motif et à tout moment à un tel traitement.

(4) Le présent article s'applique aux personnes physiques ainsi qu'aux personnes morales dans le respect de leurs intérêts légalement protégés.

(5) Quiconque contrevient aux dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 11.– *Communications non sollicitées*

(1) L'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe n'est possible que si l'abonné a donné son consentement préalable.

(2) Sans préjudice du paragraphe (1er) le fournisseur, qui dans le cadre d'une vente d'un produit ou d'un service, a obtenu directement de son client les coordonnées électroniques de celui-ci en vue d'un courrier électronique, peut exploiter ces coordonnées à des fins de prospection directe pour offrir des produits ou services analogues que lui-même fournit pour autant que ledit client soit clairement informé sur l'exploitation de ses coordonnées et nonobstant son droit de s'opposer par un moyen simple et gratuit à une telle exploitation au moment de la collecte de ses coordonnées et lors de chaque message, au cas où le client n'aurait pas d'emblée refusé une telle exploitation.

(3) L'envoi de communications non sollicitées à des fins de prospection directe par d'autres moyens que ceux visés aux paragraphes (1) et (2) n'est possible que si l'abonné concerné a donné son consentement préalable.

(4) Il est interdit d'émettre des messages électroniques à des fins de prospection directe en déguisant, dissimulant ou en dénaturant l'identité de l'émetteur au nom duquel la communication est faite, ou sans

indication d'adresse valable à laquelle le destinataire peut transmettre une demande de cesser ces communications.

(5) Le présent article s'applique aux personnes physiques et aux personnes morales dans le respect de leurs intérêts légalement protégés.

(6) Quiconque contrevient aux dispositions du présent article 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. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 12.– Dispositions transitoires et finales

(1) La Commission nationale pour la protection des données est chargée du respect des dispositions de la présente loi dans le cadre de ses missions et pouvoirs qui lui sont attribués en vertu de l'article 32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

(2) Le fournisseur offrant un annuaire „de recherche inverse“ au sens de l'article 10 paragraphe (3) avant l'entrée en vigueur de la présente loi informe l'abonné, par un moyen approprié et gratuit, de la finalité du traitement de ses données. L'abonné qui ne s'y oppose pas dans un délai de 2 mois est censé avoir consenti à ce que ses données soient traitées à des fins de recherche inverse.

(3) *Les articles suivants du code d'instruction criminelle sont modifiés comme suit:*

(a) *Art. 88-2: Les alinéas 1, 2, 3 et 5 de l'article 88-2 du Code d'Instruction criminelle sont modifiés comme suit:*

al 1: Les décisions par lesquelles le juge d'instruction ou le président de la chambre du conseil de la Cour d'appel auront ordonné la surveillance et le contrôle de télécommunications ainsi que de correspondances confiées à la poste seront notifiées aux opérateurs des postes ou télécommunications qui feront sans retard procéder à leur exécution.

al 2: Ces décisions et les suites qui leur auront été données seront inscrites sur un registre spécial tenu par chaque opérateur des postes ou télécommunications.

al 3: Les télécommunications enregistrées et les correspondances ainsi que les données ou renseignements obtenus par d'autres moyens techniques de surveillance et de contrôle sur la base de l'article 88-1 seront remis sous scellés et contre récépissé au juge d'instruction qui dressera procès-verbal de leur remise. Il fera copier les correspondances pouvant servir à conviction ou à décharge et versera ces copies, les enregistrements ainsi que tous autres données et renseignements reçus au dossier. Il renverra les écrits qu'il ne juge pas nécessaire de saisir aux opérateurs des postes qui les remettront sans délai au destinataire.

al 5: Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction.

(b) *Art 88-4: Les alinéas 1 et 4 de l'article 88-4 sont modifiés comme suit:*

al 1: Les décisions par lesquelles le Président du Gouvernement aura ordonné la surveillance et le contrôle de télécommunications ainsi que de correspondances seront notifiées aux opérateurs des postes ou télécommunications qui feront procéder sans retard à leur exécution.

al 4: Les correspondances seront remises sous scellés et contre récépissé au service de renseignements. Le chef du service fera photocopier les correspondances pouvant servir à charge ou à décharge et renverra les écrits qu'il ne juge pas nécessaire de retenir aux opérateurs des postes qui les feront remettre au destinataire.

(4) La loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel est modifiée comme suit:

Art. 3.– Champ d'application

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

- au traitement de données concernant une personne morale et dont la publication au Mémorial est prescrite par une loi ou un règlement grand-ducal.

Art. 11.– Traitement à des fins de surveillance sur le lieu du travail

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

- (a) pour les besoins de sécurité et de santé des travailleurs, ou
- (b) pour les besoins de protection des biens quelque soit le statut, public ou privé, de l'employeur, ou
- (c) pour le contrôle du processus de production portant uniquement sur les machines, ou
- (d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou
- (e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.
- (f) pour assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur quelque soit son statut, public ou privé, de l'Etat ou des collectivités publiques.

Art. 12.– Notification préalable à la Commission nationale

(2) Pour les traitements des données dont la mise en oeuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée.

Ces directives précisent:

- a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;
- b) la ou les catégories de données traitées;
- c) la ou les catégories de personnes concernées;
- d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;
- e) la durée de conservation.

En dehors de ces directives, la notification simplifiée comprend les informations prévues aux points (a) et (b) de l'article 13 paragraphe (1).

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale par support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique.

(3) Est exempté de l'obligation de notification:

- (b) le traitement ayant pour seul objet la tenue d'un registre qui en vertu d'une loi ou d'un règlement grand-ducal est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;

Art. 13.– Contenu et forme de la notification

(3) La notification se fait auprès de la Commission nationale moyennant support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique suivant un schéma à établir par elle. Il est accusé réception de la notification.

Art. 14.– Autorisation préalable de la Commission nationale

Nouveau paragraphe (3): „Toute modification affectant les informations visées au paragraphe (2) doit être autorisée par la Commission nationale préalablement à la mise en oeuvre du traitement.“

L'actuel paragraphe (3) devient le paragraphe (4). Le texte reste inchangé.

Nouveau paragraphe (5): „Un règlement grand-ducal fixera le montant et les modalités de paiement d’une redevance à percevoir lors de toute autorisation et de toute modification d’autorisation.“

Nouveau paragraphe (6): „L’autorisation se fait auprès de la Commission nationale moyennant support papier accompagné, le cas échéant, d’un support informatique ou d’une transmission par voie électronique. Il est accusé réception de l’autorisation.“

L’actuel paragraphe (4) devient le paragraphe (7). Le texte reste inchangé.

Art. 15.– Publicité des traitements

(2) Figurent dans ce registre:

- (a) les traitements notifiés à la Commission nationale en vertu de l’article 12, paragraphes (1) et (2)

Art. 27.– Exceptions au droit à l’information de la personne concernée

(1) L’article 26 paragraphes (1) et (2) ne s’applique pas lorsque le traitement est nécessaire pour sauvegarder :

- (g) une mission de contrôle, d’inspection ou de réglementation relevant, même à titre occasionnel, de l’exercice de l’autorité publique, dans les cas visés aux points (c), (d) et (e)

Art. 34.– Composition de la Commission nationale

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d’origine à un emploi correspondant au traitement qu’il a touché précédemment, augmenté des échelons et majorations de l’indice se rapportant aux années de service passées comme président ou membre effectif jusqu’à concurrence du dernier échelon du grade. (alinéa 6)

Toutefois, si l’autorité investie du pouvoir de nomination estime que la nature du travail accompli et l’expérience acquise par l’intéressé au sein de la Commission nationale justifient sa nomination à une fonction supérieure à celle visée ci-dessus, elle peut procéder à une telle nomination sans que le bénéficiaire ne puisse, de ce fait, accéder à une fonction ou obtenir un rang plus élevé que les fonctionnaires de la même carrière entrés au service de l’Etat en même temps que lui ou avant lui (nouvel alinéa 7)

A défaut de vacance, il peut être créé un emploi hors cadre correspondant à ce traitement; cet emploi est supprimé de plein droit à la première vacance qui se produit dans une fonction appropriée du cadre normal. (l’alinéa 7 devient l’alinéa 8)

Art. 41.– Dispositions spécifiques

(1) dernier alinéa: La centrale des secours d’urgence 112, les centres d’appels d’urgence de la police grand-ducale et la centrale du service d’incendie et de sauvetage de la Ville de Luxembourg accèdent dans les mêmes conditions et modalités que les autorités visées à l’alinéa précédent aux seules données concernant l’identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.

(3) L’accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d’instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l’article 40 du Code d’instruction criminelle et aux mesures particulières de secours d’urgence dans le cadre des activités de la centrale des secours d’urgence 112, des centres d’appels d’urgence de la police grand-ducale et de la centrale du service d’incendie et de sauvetage de la Ville de Luxembourg.

Art. 13.– Entrée en vigueur

La présente loi entre en vigueur le premier jour du mois qui suit sa publication au Mémorial.

EXPOSE DES MOTIFS ET COMMENTAIRE DES ARTICLES

- *Historique*

Les nouvelles technologies numériques avancées posent actuellement des exigences spécifiques à la protection de la vie privée des utilisateurs ainsi qu'au traitement de leurs données à caractère personnel. Le développement de la société de l'information se caractérise notamment par la mise en œuvre de nouveaux services de communications électroniques. L'Internet offre certes de nouvelles possibilités aux utilisateurs mais présente également de nouveaux dangers aux utilisateurs en ce qui concerne leurs données à caractère personnel et leur vie privée. L'accès aux réseaux mobiles numériques est ouvert à un large public à des conditions de plus en plus abordables. Ces réseaux numériques offrent de grandes capacités et de vastes possibilités pour le traitement des données à caractère personnel. Le succès du développement transfrontalier des services de communications dépendra donc en grande partie de la certitude qu'auront les utilisateurs que ces services ne porteront pas atteinte à leur vie privée.

Conscients de ces dangers le Conseil, dans sa résolution du 18 juillet 1989, ainsi que le Parlement européen avaient souligné l'importance de la protection des données à caractère personnel et de la vie privée eu égard notamment à l'introduction des réseaux numériques à intégration de services (RNIS). Des dispositions adéquates furent ainsi adoptées dans la *directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JOCE No L 281/31 du 23.11.1995)*.

- *But et objectifs de la Directive 97/66/CE*

La directive 97/66/CE a pour but d'harmoniser les dispositions nationales de „protection des données“ afin d'éviter de créer des obstacles au marché intérieur des télécommunications conformément à l'objectif énoncé à l'article 7A du traité (considérant 8 de la directive).

Elle tend à traduire les principes définis dans la directive 95/46/CE (transposée en droit national par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) en règles spécifiques applicables au secteur des télécommunications en renforçant d'une part la confidentialité des communications; principe garanti en conformité des instruments internationaux relatifs aux droits de l'homme dont notamment la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les constitutions des Etats membres et d'autre part les dispositions relatives au stockage et au traitement automatisés de données relatives aux abonnés et aux utilisateurs.

De ce fait la directive 97/66/CE est une réglementation sectorielle eu égard à la réglementation générale qu'est la directive 95/46/CE. De sorte que dans le secteur des télécommunications voire des communications électroniques la directive 95/46/CE est applicable à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la directive 97/66/CE.

- *La directive 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques dénommée directive „vie privée et communications électroniques“.*

Afin de tenir compte de l'évolution des marchés et des technologies des services de communications électroniques, la directive 2002/58/CE est destinée à remplacer la directive 97/66/CE.

La directive „vie privée et communications électroniques“ ne vise pas à modifier profondément le contenu de la directive actuellement en vigueur, mais à adapter et à actualiser ses dispositions pour tenir compte des évolutions récentes et prévisibles dans le domaine des services et des technologies des communications électroniques. De ce fait elle reprend les principes de base de la directive existante moyennant des modifications rédactionnelles et l'ajout de dispositions nouvelles plus adaptées à l'environnement actuel.

Son but consiste entre autres à adopter, conformément au cadre réglementaire posé, des règles qui sont neutres sur le plan technologique c'est-à-dire des règles qui n'imposent ni ne favorisent l'utilisation d'un type de technologie particulier ce qui implique que le consommateur voire l'utilisateur jouit d'un même niveau de protection quelle que soit la technologie mise en œuvre pour la fourniture d'un service donné.

• *Etat de transposition au Luxembourg*

Vu le vide juridique total en la matière dû au retard qu'a pris le Luxembourg dans la transposition de la directive 97/66/CE (cf. arrêt de la Cour du 6 mars 2003 condamnant le Grand-Duché de Luxembourg pour non-transposition de la directive 97/66/CE) et compte tenu de l'adoption de la directive „vie privée et communications électroniques“, le présent projet de loi se propose donc de transposer à la fois les principes de base de la directive 97/66/CE (incorporés dans la directive 2002/58/CE) et les dispositions nouvelles de la directive „vie privée et communications électroniques“.

Pourquoi l'avoir fait maintenant et non pas lors du dépôt du projet de loi No 4735?

La réponse est simple puisqu'il fallait attendre à ce que le texte communautaire se stabilise, suite à des discussions souvent difficiles au niveau communautaire aux sujets tels que la durée de conservation des données et les communications non sollicitées qui a suscité de vives discussions quant au choix du régime de l'opt in et de l'opt out.

Commentaire des articles

Article 1er.– Champ d'application

L'article 1er paragraphe 1er précise que les dispositions de la présente loi sont des dispositions spécifiques de „protection des données“ applicables en matière de communications électroniques accessibles au public. En dehors du champ d'application de la présente loi, les dispositions générales de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel s'appliquent.

La présente loi s'applique donc à la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications électroniques publics.

L'article 1er reprend l'article 3 de la directive 97/66 dont le texte a été actualisé par la directive „vie privée et communications électroniques“ qui remplace les „services de télécommunications“ par ceux de „services de communications électroniques“ et qui supprime la référence au RNIS et aux réseaux numériques mobiles par souci de neutralité technologique.

La référence à la „future“ législation sur les réseaux et les services de communications électroniques (paragraphe 1er) s'explique par le fait que la directive 2002/58/CE a initialement fait partie des directives du „paquet réglementaire des communications électroniques“¹ dont elle emprunte les concepts de base.

Article 2.– Définitions

La directive „vie privée et communications électroniques“ a remplacé les définitions existantes des „services et réseaux de télécommunications“ figurant dans la directive 97/66 par celles de „services et réseaux de communications électroniques“ afin d'aligner la terminologie sur la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (ci-après directive „cadre“). Une actualisation de ces définitions s'imposait pour faire en sorte que les différents types de services de communications électroniques soient couverts indépendamment de la technologie utilisée.

Il résulte de l'article 2 de la directive 97/66/CE ainsi que du texte de la directive „vie privée et communications électroniques“ (article 2) que les 2 textes sont complémentaires à la directive 96/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (loi du 2 août 2002 précitée) et à la directive „cadre“ (mentionnée ci-dessus) de sorte que leurs définitions s'appliquent également.

L'article 2 a suivi cette démarche en reprenant les termes „appel“; „communication“; „données relatives au trafic“; „données de localisation“; „consentement“; „service à valeur ajoutée“ et „courrier électronique“ figurant dans le texte de la directive 2002/58/CE mais également ceux de „service de

¹ Directive 2002/19/CE „accès“
 Directive 2002/20/CE „autorisation“
 Directive 2002/21/CE „cadre“
 Directive 2002/22/CE „Service universel“

communications électroniques“, „réseau de communications électroniques“, „réseau de communication public“ et d’ „utilisateur final“ figurant dans la directive „cadre“ transposés en droit national par le projet de loi sur les réseaux et les services de communications électroniques.

L’article 2 (a) reprend, par souci de clarté, la définition de l’ „abonné“ telle que prévue par la directive 97/66CE, en l’adaptant à celle figurant dans le projet de loi sur les réseaux et les services de communications électroniques. La définition de l’abonné constitue une notion clé dans le corps du texte et se caractérise par la relation contractuelle entre l’abonné (personne physique ou morale) et l’entreprise offrant des services de communications électroniques accessibles au public laquelle peut prévoir un paiement périodique ou un versement unique pour le service fourni ou à fournir; les cartes de prépaiement constituent également un contrat.

Alors que l’article 2 (l) définit le terme „utilisateur“ par opposition à celui „d’abonné“ comme étant une personne qui utilise ou qui demande un service sans être „nécessairement abonnée à ce service“.

L’inclusion des définitions „utilisateur final“ (correspond à la définition (p)) de la directive 2002/21 „directive-cadre“ et „utilisateur“ a pour objet, eu égard à la législation sur les réseaux et les services de communications électroniques, de citer les catégories d’utilisateurs pouvant être affectés par les dispositions du présent projet de loi.

La définition (b) relative à „l’appel“ n’apporte pas de commentaire particulier. La définition (c) relative au „consentement“ est calquée sur celle de la loi du 2 août 2002 (article 2 (c)).

Il résulte du nouveau considérant 16 relatif à la définition de „communication“ (article 2 (d) du texte et article 2 (d) de la directive 2002/58/CE) que les informations diffusées par un service de radiodiffusion sur un réseau de communications public le sont à l’intention d’un nombre virtuellement illimité d’auditeurs/téléspectateurs et ne constituent pas une communication au sens de la directive. Par contre, lorsqu’il est possible d’identifier l’abonné ou utilisateur individuel qui reçoit ces informations, comme, par exemple, dans le cas de la fourniture de services vidéo à la demande, les informations acheminées s’inscrivent dans la définition de „communication“.

Le „courrier électronique“ (article 2 (e)) non prévu par la directive 97/66/CE, figure cependant dans le texte de la directive „vie privée et communications électroniques“ (article 2 (h)) afin de tenir compte de la diversité actuelle des services de communications électroniques. Cette définition vise avant tout les „e-mails“.

Les „données relatives au trafic“ (article 2 (f)) sont définies comme „toutes les données traitées en vue de l’acheminement d’une communication par un réseau de communications électroniques ou de sa facturation“. Il s’agit d’une nouvelle définition prévue par le texte de la directive 2002/58/CE permettant de poser le principe fondamental selon lequel toutes les données relatives au trafic générées durant une communication, qu’elles soient nécessaires ou non à l’établissement de la communication doivent être effacées ou rendues anonymes dès lors qu’elles ne sont plus nécessaires à la transmission d’une communication. Cette définition inclut les données de localisation générées durant l’exécution d’une communication et comprend également les „données de navigation“ comme par exemple les URL/ Unique Resource Locator.

Il résulte du nouveau considérant 15 du texte de la directive 2002/58/CE qu’ „une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui envoie la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d’effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d’une communication, le protocole de référence, l’emplacement des équipements terminaux de l’expéditeur ou du destinataire, le réseau de départ ou d’arrivée de la communication, ou encore le début, la fin ou la durée d’une connexion; elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau“.

Le moment exact où s’achève la transmission d’une communication, au-delà duquel les données relatives au trafic doivent être effacées sauf à des fins de facturation, peut dépendre du type de service de communications électroniques fourni. Ainsi, dans le cas d’un appel par téléphonie vocale, la transmission cesse dès que l’un ou l’autre des usagers interrompt la connexion et, dans le cas d’un courrier électronique, la transmission prend fin dès que le destinataire prend connaissance du message, généralement à partir du serveur de son fournisseur de service.

Par „*données de localisation*“ (article 2 (g) du texte et article 2 (c) de la directive 2002/58/CE) on entend la latitude, la longitude et l'altitude du lieu où est installé l'équipement terminal de l'utilisateur, la direction de l'acheminement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée.

La définition relative au „*service à valeur ajoutée*“ (article 2 (k)) vise par exemple les conseils sur les forfaits tarifaires les plus avantageux ou sur le guidage routier, des informations sur l'état de la circulation, des prévisions météorologiques ou des informations touristiques etc.

Les définitions relatives aux „*réseau de communications électroniques*“; „*réseau de communications public*“, „*service de communications électroniques*“ et à „l'utilisateur final“ ont été reprises de la directive 2002/21/CE du PE et du Conseil relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques („*directive-cadre*“); laquelle est transposée par le projet de loi sur les réseaux et les services de communications électroniques.. Elles sont complémentaires par rapport aux définitions de la présente loi et feront l'objet d'un commentaire détaillé au projet de loi précité. En outre les dénominations „opérateur“ et „fournisseur de services“ ont pour objet une lecture plus facile du texte.

Article 3.– Sécurité

L'article 3 reprend le texte de l'article 4 de la directive 97/66/CE tout en remplaçant „services et réseaux de télécommunications“ par „services et réseaux de communications électroniques accessibles au public“. La sécurité étant un élément primordial pour le fonctionnement des réseaux et la prestation des services de communications électroniques d'où l'article 3 retient en quelque sorte une responsabilité en cascade en précisant que la responsabilité repose „primairement“ sur le fournisseur de services (alinéa 1e) vis-à-vis de son client et celle-ci est le cas échéant partagée conjointement avec l'opérateur lorsque la sécurité du réseau est en cause. Le fournisseur de services et le cas échéant l'opérateur sont obligés à informer les abonnés des risques particuliers liés à une atteinte à la sécurité du réseau et/ou des services (alinéa 2). Il s'agit d'une obligation de moyens qui incombe.

De tels risques peuvent notamment toucher les services de communications électroniques fournis par l'intermédiaire d'un réseau ouvert de sorte qu'il appartient au fournisseur qui offre des services de communications électroniques accessibles au public sur Internet, d'informer les abonnés des mesures qu'il envisage de prendre pour sécuriser les communications, en recourant par exemple à des types spécifiques de logiciels ou de techniques de cryptage.

En revanche l'obligation d'information prévue à l'article 3 alinéa 2 ne dispense pas le fournisseur de services et le cas échéant l'opérateur en ce qui concerne la sécurité de son réseau, de prendre immédiatement les mesures appropriées pour remédier à l'atteinte ou au risque d'atteinte grave à la sécurité du réseau et de rétablir le niveau normal de sécurité du service; les frais étant à sa seule charge. Notons que l'information de l'abonné sur les risques en matière de sécurité devrait être gratuite, exceptés les frais nominaux qu'un abonné peut être amené à supporter lorsqu'il reçoit ou collecte des informations (ex. téléchargement d'un message reçu par courrier électronique).

Article 4.– Confidentialité des communications

L'article 4 pose le principe fondamental de la confidentialité des communications telle qu'énoncée à l'article 5 des directives 97/66/CE et 2002/58/CE. L'article 4 est une transposition „fidèle“ de l'article 5 de la directive 2002/58/CE „directive vie privée et communications électroniques“ du moins en ce qui concerne les paragraphes (1), (2), (3) a), d) et e). Les paragraphes (1) et (2) ont pour objet de préciser la responsabilité de l'opérateur.

Le paragraphe 1er transpose en droit national le paragraphe 1er de l'article 5 de la directive 2002/58/CE en établissant en termes généraux l'obligation de confidentialité dans le chef de l'opérateur et/ou des fournisseurs de services.

Le paragraphe 2 pose le principe des interdictions ayant trait à la violation de la confidentialité des communications.

Notons que l'inobservation des paragraphes 1er et 2 est soumise à la même sanction (paragraphe 4). Le texte suit ainsi la logique de la loi du 2 août 2002 qui sanctionne les traitements illégaux sans distinguer selon l'existence ou non d'une intention dolosive.

Reste la question de l'interdiction du tiers d'intercepter des données, de les stocker, de les détenir etc.; non expressément prévue par le texte de la directive. Une telle interdiction pourrait néanmoins être retenue et faire l'objet d'une sanction à inclure aux actuels articles 509-1 et suivants du Code pénal.

Le paragraphe 3 lettre (a) transpose la 2^e exception de l'article 5 paragraphe 1^{er} de la directive 2002/58/CE et n'apporte pas de commentaire particulier.

En revanche le paragraphe 3 lettre (b) est une mesure nationale qui a pour objet de déterminer les autorités légalement autorisées à déroger au principe de la confidentialité. La lettre (b) reprend la systématique de l'article 41 de la loi du 2 août 2002 afin d'établir une certaine cohérence entre les deux dispositions. La lettre (b) du paragraphe 3 est une disposition générale qui permet aux autorités légales de conserver a priori toutes les données du fait qu'il leur est impossible de déterminer à l'avance pour quelle finalité exacte ces données seront conservées. En revanche la loi du 21 novembre 2002 réglementant le repérage de télécommunications et portant modification du Code d'Instruction criminelle (article 67-1 Cic) énonce les conditions dans lesquelles le recours au repérage de télécommunications est possible. Si ces conditions sont remplies, les données conservées par application de l'article 4 paragraphe 3 lettre (b) de la présente loi peuvent être utilisées. La loi réglementant le repérage peut donc être considérée comme un texte spécifique par rapport à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et notamment au présent projet de loi.

La lettre (c) du paragraphe 3 est une mesure nationale qui constitue la base légale à un enregistrement des communications type appels d'urgence et d'alerte. Le paragraphe (3) c) énonce les cas limitatifs pour lesquels un enregistrement est permis. Vu la difficulté de regrouper voire de catégoriser la multitude de services offerts en matière d'urgence et d'alerte; il est jugé plus opportun de se limiter aux 112 et aux numéros d'urgence tels que déterminés par l'Institut dont on vise avant tout le „113“ lequel n'étant pas un numéro d'appel d'urgence officiel instauré au niveau européen par une décision communautaire comme le „112“. La référence au 113 étant nécessaire afin d'éviter toute limitation en matière de prestation de secours. En revanche un numéro unique national attribué au corps des sapeurs pompiers fait défaut pour l'instant faute de réglementation adéquate et de centrale commune. Un projet est actuellement élaboré par le Ministère de l'Intérieur qui prévoit que la centrale du 112 servirait également de centrale commune aux sapeurs pompiers.

Les données relatives au trafic y afférents dont les données de localisation collectées dans les cas susénoncés sont à effacer une fois le secours apporté excepté le contenu des communications dont la conservation est nécessaire en cas de problème de compréhension ou d'ambiguïté entre l'appelant et les services d'urgence. En pratique les contestations parviennent au „113“ 2 à 6 mois après l'appel. C'est pourquoi le délai de 6 mois est jugé appropriée.

Le paragraphe (3) lettre (d) prévoit que l'enregistrement effectué à titre de preuve d'une transaction commerciale ou de toute autre communication etc. tombe également sous le principe la confidentialité des communications. La lettre (d) reprend le texte de l'article 5(2) de la directive 2002/58/CE. En effet il est pratique courante que des communications commerciales sont enregistrées pour servir de preuve. Cette pratique est à considérer comme usage professionnel licite, tant que les parties à la communication en sont informées avant que l'enregistrement n'ait eu lieu, de la finalité de l'enregistrement et de la durée de stockage. Les communications enregistrées devraient être effacées dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction.

Le paragraphe 3 lettre (e) transpose le paragraphe 3 de l'article 5 de la directive 2002/58/CE. Il s'agit d'un nouveau paragraphe ne figurant pas dans la directive 97/66/CE. L'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné.

Il résulte du considérant 25 du texte de la directive 2002/58/CE que les „cookies“ peuvent constituer un outil légitime pour évaluer par exemple l'efficacité de la conception d'un site et de la publicité faite sur ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne. Lorsque les „cookies“ sont destinés à des fins légitimes et servent à faciliter la fourniture d'un service de la société de l'information, leur utilisation doit être autorisée pour autant que l'opérateur d'un site qui les expédie ou qui permet à un tiers de les expédier via son site fournisse des informations claires et précises sur la finalité du/des dispositif(s) en question. Encore faut-il que l'utilisateur puisse refuser qu'un „cookie“ ou un dispositif analogue soit greffé sur son équipement terminal. Finalement l'accès au contenu d'un site spécifique peut être subordonné au fait d'accepter, en pleine connaissance de cause,

l'installation d'un „cookie“ ou d'un dispositif analogue à condition que celui-ci soit de nouveau utilisé à des fins légitimes.

Le paragraphe 4 sanctionne l'inobservation des dispositions du présent article. Il reprend la même sanction que celle figurant dans la loi du 2 août 2002.

Article 5.– Données relatives au trafic

L'article 5 traduit le texte actualisé de l'article 6 de la directive 2002/58/CE. L'article 5 restreint l'utilisation par le fournisseur de services et/ou opérateur des données relatives au trafic aux seules fins de transmission de communications électroniques (au lieu des seuls appels téléphoniques prévus par la directive 97/66/CE); de facturation et de fourniture de services à valeur ajoutée moyennant le consentement de l'abonné/utilisateur et ce pour une durée limitée (paragraphe 2, 3 et 4).

Cependant, pour des raisons d'ordre pénal et pour des mesures spéciales de surveillance à constater en vertu des articles 88-1 à 88-4 Code d'instruction criminelle, les données relatives au trafic sont à conserver pendant une durée de 12 mois (paragraphe 1er point (a)); pour des raisons de protection des données, le fournisseur de services et/ou l'opérateur doit néanmoins tout mettre en œuvre à ce que ces données ne soient plus accessibles à d'autres fins, dès lors qu'elles ne sont plus nécessaires à la communication, à la facturation ou, le cas échéant, à la fourniture de services à valeur ajoutée (paragraphe 2).

En outre le fournisseur de services et/ou l'opérateur est tenu d'effacer voire de rendre anonymes (paragraphe 1er lettre (b)) les données relatives au trafic après expiration du délai de conservation et en l'absence d'une mesure d'enquête prise dans le cadre de l'article 40 du Code d'Instruction Criminelle. Cependant le paragraphe 2 est assorti de deux exceptions reprenant les dispositions de l'article 6 paragraphe 6 de la directive 2002/58/CE.

Le délai de 12 mois est considéré au niveau communautaire comme étant le délai maximum pendant lequel les données de ce type peuvent être conservées. L'article 16 de la Convention sur la cybercriminalité du 23.11.2001 (<http://conventions.coe.int/Treaty>) prévoit une durée maximum de 90 jours. Notons que la période de 12 mois oblige chaque fournisseur de services et/ou opérateur de conserver a priori toutes les données relatives au trafic pendant une durée de 12 mois pour les raisons indiquées ci-dessus.

Quant au paragraphe 3, le groupe sur la protection des personnes à l'égard du traitement des données à caractère personnel („groupe article 29“ de la directive 95/46/CE) souligne dans sa recommandation 3/99 l'absence, au niveau communautaire, d'une harmonisation de la période durant laquelle la facture peut être légalement contestée. Le „groupe article 29“ recommande à la Commission européenne d'harmoniser cette période „afin de fixer une limite au stockage des données relatives au trafic pour les besoins précis de la facturation, en vue de renforcer le droit fondamental des citoyens au respect de la vie privée“; période qu'il souhaite aussi courte que possible.

En l'absence d'une telle harmonisation et il y a lieu de préciser que le délai de contestation en la matière est de 10 ans au Luxembourg.

Le paragraphe 4 traite des données pouvant être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée et contient des dispositions classiques de protection des données.

Le paragraphe 5 limite l'accès aux données relatives au trafic aux personnes agissant sous l'autorité du fournisseur de services et/ou de l'opérateur pour assurer la facturation et/ou la gestion du trafic.

Le paragraphe 6 prévoit les sanctions pénales en cas de non-respect du présent article. Il s'agit d'une sanction analogue à celle prévue dans la loi du 2 août 2002.

Article 6.– Facturation détaillée

L'article 6 transpose l'article 7 de la directive 97/66/CE dont le texte est inchangé par rapport à celui de la directive 2002/58/CE excepté l'ajout relatif au „renforcement du respect de la vie privée“.

Eu égard à l'article 51 du projet de loi sur les réseaux et les services de communications électroniques qui fixe le niveau minimum d'une facture détaillée; l'article 6 du présent projet a pour objet de conférer aux abonnés le droit à une facture non détaillée tout en prévoyant des modalités susceptibles d'assurer le respect de la vie privée eu égard à la facture détaillée.

Dans ce contexte le paragraphe 2 prévoit que les appels gratuits y compris ceux aux services d'urgence et d'alerte ne sont pas indiqués sur la facture ainsi que l'identification de l'appelé jugée comme non indispensable pour l'établissement d'une facture.

Article 7.– Identification de la ligne appelante et de la ligne connectée

L'article 7 transpose l'article 8 de la directive 97/66/CE dont le texte demeure identique à celui de la directive 2002/58/CE (article 8). L'article 7 offre aux abonnés et aux utilisateurs des garanties afin de protéger leur vie privée dans le cadre de l'utilisation des services d'identification des lignes appelantes et connectées.

Il résulte du considérant 34 de la directive 2002/58/CE (considérant 19 de la directive 97/66) „ qu'il est nécessaire, en ce qui concerne l'identification de la ligne appelante, de protéger le droit qu'a l'auteur d'un appel d'empêcher l'indication de l'identification de la ligne à partir de laquelle l'appel est effectué, ainsi que le droit de la personne appelée de refuser les appels provenant de lignes non identifiées; qu'il est justifié, dans des cas spécifiques, d'empêcher la suppression de l'indication de l'identification de la ligne appelante; que certains abonnés, en particulier les numéros de type „SOS“ et autres organisations similaires, ont intérêt à garantir l'anonymat de ceux qui les appellent; qu'il est nécessaire, en ce qui concerne l'identification de la ligne connectée, de protéger le droit et l'intérêt légitime qu'a la personne appelée d'empêcher l'indication de l'identification de la ligne à laquelle l'auteur de l'appel est effectivement connecté, en particulier dans le cas d'appels renvoyés; que les fournisseurs de services de communications électroniques accessibles au public doivent informer leurs abonnés de l'existence, sur le réseau, de l'identification des lignes appelantes et connectées, ainsi que de tous les services offerts sur la base de l'identification des lignes appelante et connectée et des possibilités offertes en matière de protection de la vie privée; que cela permettra aux abonnés de choisir en connaissance de cause, parmi les possibilités qui leur sont offertes en matière de protection de la vie privée, celles dont ils souhaiteraient faire usage; que les possibilités qui sont offertes en matière de protection de la vie privée pour chaque ligne ne doivent pas nécessairement être disponibles comme un service automatique du réseau, mais peuvent être obtenues sur simple demande auprès du fournisseur du service de communications électroniques accessible au public“.

L'article 7 paragraphe 5 transpose l'article 9 b) de la directive 97/66 (article 10 b) de la directive 2002/58/CE). Il constitue une dérogation au principe énoncé aux paragraphes précédents dans la mesure où il est indispensable, dans le cadre d'une prestation efficace de sauvegarde de la vie humaine, que les numéros d'appel d'urgence tels que le 112, mais également les sapeurs pompiers professionnels et le 113 (voir commentaire article 4 (3) c)), puissent répondre aux appels d'urgence et de ce fait identifier la ligne appelante même si l'appelant s'y est opposé².

Les paragraphes 6 et 7 n'apportent pas de commentaire particulier.

L'article 7 paragraphe 8 transpose l'article 9 a) de la directive 97/66/CE (article 10 a) de la directive 2002/58/CE). Il tend à résoudre le phénomène des appels à contenu malveillant ou dérangeant en déterminant les conditions dans lesquelles la victime d'un appel à contenu malveillant peut obtenir l'identification de l'auteur. En revanche compte tenu des modalités techniques assez complexes à respecter par l'opérateur et/ou le fournisseur de services en la matière, un règlement grand-ducal déterminant les modalités procédurales minimum est indispensable.

Notons que le paragraphe 8 n'entend point déroger à l'article 6 de la loi du 11 août 1982 – Loi concernant la protection de la vie privée – mais entend apporter des précisions quant aux aspects de „protection des données“ ainsi qu'à la procédure applicable en la matière.

Le paragraphe 9 incrimine les pratiques d'identification et de communication de ces informations contraires.

Article 8.– Renvoi automatique d'appels

L'article 8 transpose l'article 10 de la directive 97/66/CE dont le texte demeure inchangé à l'article 11 du texte de la directive 2002/58/CE.

L'article 8 confère à l'abonné le droit et les moyens de mettre fin au renvoi d'appels sur leur ligne. Le but est de protéger l'abonné contre toute gêne que pourrait causer le renvoi automatique d'appels par

² Voir commentaire quant aux 112 et 113 à l'article 4 §3 lettre c)

d'autres personnes et de donner à l'abonné les moyens de faire cesser le transfert des appels renvoyés sur son terminal et ceci sur simple demande adressée au fournisseur de ce service.

Article 9.– Données de localisation autres que les données relatives au trafic

L'article 9 transpose l'article 9 du texte de la directive 2002/58/CE. Il s'agit d'un nouveau texte ne figurant pas dans la directive 97/66/CE qui introduit des garanties de respect de la vie privée des abonnés ou utilisateurs en matière de fourniture de services d'informations fondés sur la localisation des mobiles.

Dans les réseaux de communications mobiles, les données de localisation comportant des indications sur la position géographique d'un équipement terminal de l'utilisateur mobile sont traitées afin de permettre la transmission des communications. Ces données sont des données relatives au trafic couvertes par l'article 5. Toutefois les réseaux numériques mobiles peuvent également traiter des données de localisation qui sont plus précises que ne l'exige la transmission des communications et qui sont utilisées pour la fourniture de services à valeur ajoutée tels que par exemple les services personnalisés d'informations sur la circulation et le guidage des conducteurs. Il s'agit alors de données de localisation autres que les données relatives au trafic couvertes par le présent article. Vu leur caractère sensible, le traitement en vue de la fourniture de services à valeur ajoutée n'est possible que lorsque l'abonné ou l'utilisateur a donné son consentement préalable et qu'il a été informé du type de données de localisation traitées (autres que les données relatives au trafic), de leur finalité, de la durée du traitement ainsi que de la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée (paragraphe 4). L'abonné ou l'utilisateur doit en outre disposer d'un moyen simple et gratuit pour interdire temporairement le traitement de ce type de données (paragraphe 4 alinéa 2).

Le paragraphe 3 pose le principe de la durée du traitement. Ainsi les données de localisation autres que les données relatives au trafic ne peuvent être traitées qu'„après les avoir rendues anonymes ou moyennant le consentement exprès de l'abonné ou de l'utilisateur, dans la mesure et pour la durée nécessaire à la fourniture d'un service à valeur ajoutée“.

Les paragraphes 1er et 2 étant le corollaire de l'article 5 et n'apportent pas de commentaire particulier ici. Cependant l'article 9 paragraphe 1er (a) précise que pour l'application du présent paragraphe „une seule information de localisation est requise par communication ou par appel“ et ceci afin de limiter le volume d'informations générées par les utilisateurs mobiles lesquels se trouvent en déplacement constant. La dernière phrase de l'article 9 paragraphe 1er (a) souligne que ces données doivent également être communiquées au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut afin de permettre la localisation d'une personne en détresse.

Le paragraphe 7 prévoit la même sanction qu'à l'article 5 paragraphe (7) et n'apporte pas de commentaire particulier.

Article 10.– Annuaire d'abonnés

L'article 10 transpose l'article 12 des directives 2002/58/CE et 97/66/CE tout en supprimant la possibilité de monnayer le droit de ne pas figurer dans un annuaire; disposition conforme à l'article 45 du projet de loi sur les réseaux et les services de communications électroniques. L'article 10 tient également compte des nouveaux services de communications électroniques et des nouveaux types de services d'annuaires.

Les annuaires d'abonnés aux services de communications électroniques sont librement commercialisés et largement diffusés et publiés. Pour protéger la vie privée des personnes physiques et l'intérêt légalement protégé des personnes morales, il importe que l'abonné soit à même de déterminer si les données à caractère personnel qui le concernent doivent être publiées dans un annuaire et, dans l'affirmative, lesquelles de ces données doivent être rendues publiques (paragraphe 2). 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.

Le paragraphe 4 précise le champ d'application du présent article. Le paragraphe 5 assortit l'inobservation du présent article d'une sanction.

Article 11.– Communications non sollicitées

L'article 11 transpose l'article 13 du texte de la directive 2002/58/CE dont les paragraphes 1er (à l'exception de l'intégration du „courrier électronique“ dans le système de l'opt in) et 3 demeurent inchangés par rapport à l'article 12 de la directive 97/66/CE.

Le paragraphe 1er intègre le courrier électronique dans le système „opt in“ prévu à l'article 13 paragraphe 1er de la directive 2002/58/CE. Il résulte du texte de la directive précitée que le marché unique exige actuellement une approche harmonisée selon laquelle les communications non sollicitées à des fins de prospection directe ne peuvent être envoyées que si l'expéditeur a obtenu le consentement préalable du destinataire („opt in“). Des discussions controversées ont eu lieu au niveau communautaire entre „l'opt out“ (envoi de communications non sollicitées à moins que l'abonné ait clairement refusé) et „l'opt in“ (envoi de communications non sollicitées que si l'abonné a donné son consentement préalable) et ont finalement fait pencher la balance en faveur de „l'opt in“. L'article 48 de la loi sur le commerce électronique, ayant initialement retenu le système de l'„opt out“ pour les communications *commerciales* non sollicitées; a du être modifié en conséquence (v. projet de loi No 5095 modifiant la loi du 14 août 2000 relative au commerce électronique).

Le paragraphe 2 reprend l'article 13 paragraphe 2 de la directive 2002/58/CE ne figurant pas à l'article 12 de la directive 97/66/CE. Le paragraphe 2 permet à un fournisseur qui vend des produits ou services à son client d'exploiter les coordonnées électroniques collectés auprès de celui-ci pour proposer à ce client des produits ou services analogues. Il s'agirait de ce fait de données collectées à une fin précise pouvant être réutilisées ultérieurement à cette même fin au seul profit de la personne concernée en vue de lui proposer des produits ou services analogues. Notons que le texte de l'article 48 paragraphe (3) du projet de loi modifiant la loi du 14 août 2000 relative au commerce électronique est aligné sur le texte du présent paragraphe.

Le paragraphe 3 (article 13 paragraphe 3 de la directive 2002/58/CE) soumet également à l'„opt in“ l'envoi de communications non sollicitées à des fins de prospection directe *par d'autres moyens* que ceux visés aux paragraphes 1 et 2 tels que par exemple les appels téléphoniques personnels ou les envois de publicité adressés par voie postale. Ce choix s'explique par un niveau de protection plus adéquat de la personne concernée dans la mesure où celle-ci doit donner son consentement préalable à un tel envoi et que l'émetteur a l'obligation d'informer le destinataire avant l'envoi. En cas de doute la charge de la preuve incombe donc à l'émetteur lequel doit prouver qu'il a informé le destinataire tandis que l'„opt out“ fait peser la charge de la preuve au destinataire lequel doit prouver qu'il ne souhaite pas recevoir ce type de communications respectivement qu'il figure sur un „registre d'opt out“.

Tandis que l'article 48 paragraphe (3) du projet de loi modifiant la loi du 14 août 2000 relative au commerce électronique retient actuellement le système de „l'opt in“ pour les seules communications *commerciales* non sollicitées; l'article 11 du présent projet de loi introduit le système de l'„opt in“ pour l'ensemble des communications électroniques non sollicitées donc celles à caractère commercial et celles n'ayant pas de caractère commercial.

Le paragraphe 4 transpose l'article 13 paragraphe 4 de la directive 2002/58/CE non prévu à l'article 12 de la directive 97/66/CE. Le paragraphe 4 énonce le principe selon lequel il est interdit d'émettre des messages non sollicités à des fins de prospection directe sous une fausse identité, une identité déguisée ou dissimulée, une fausse adresse de réponse ou une adresse de réponse déguisée ou un faux numéro. Il s'agit d'une précision utile apportée au phénomène du „spamming“.

Le paragraphe 5 précise que le présent article s'applique aux personnes physiques et morales.

Le paragraphe 6 ne mérite pas d'observation particulière.

Article 12.– Dispositions finales

L'article 12 paragraphe (1) précise que la Commission nationale est chargée du respect des dispositions de la présente loi. Cette mission se situe dans le cadre des missions et pouvoirs d'ordre général qui sont attribués à la commission nationale en vertu de l'article 32 de la loi du 2 août 2002.

L'article 12 paragraphe (2) a pour objet de régulariser la situation existante à ce jour.

L'article 12 paragraphe (3) modifie les articles 88-2 et 88-4 du Code d'instruction criminelle dont la terminologie est devenu obsolète au regard de la libéralisation des marchés des postes et télécommunications. Il s'agit de modifications purement rédactionnelles.

(a) Modification de l'article 88-2 du CIC:

Les modifications apportées aux différents alinéas de l'article 88-2 sont uniquement des adaptations d'ordre rédactionnel.

Ainsi faut-il remplacer à plusieurs endroits les termes de „directeur de l'Administration des postes et télécommunications“ par ceux de „opérateurs des postes ou télécommunications“.

En effet, l'Administration des Postes et télécommunications n'a plus le monopole de la diffusion des télécommunications, suite à la libéralisation du marché des télécommunications.

En ce qui concerne l'envoi de courrier, il faut noter qu'à côté des services offerts par la poste, les usagers font de plus en plus souvent appel à des prestataires de services universels indépendants (par exemple: DHL, OCS, TNT etc.).

Il faut dès lors adapter les termes employés à l'article 88-2 pour étendre le champ d'application de l'article à tous les opérateurs intervenant sur ce marché.

En ce qui concerne les modifications apportées à l'alinéa 3, il faut noter que par le terme „écrits“ utilisé à la dernière phrase de l'alinéa 3, les auteurs de la loi du 26 novembre 1982 visaient exclusivement la correspondance envoyée par voie postale.

Il suffit dès lors de faire référence à l'alinéa 3 aux seuls opérateurs des postes.

Par ailleurs, conformément à la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, il est important que les opérateurs remettent sans délai les „écrits“ non retenus ou saisis au destinataire.

Enfin, à l'alinéa 5 et en ce qui concerne les personnes liées par le secret professionnel, il est proposé de faire référence à l'article 458 du code pénal, conformément à la rédaction retenue par les articles 88-1 et 88-4 alinéa 3 CIC.

(b) Modification de l'article 88-4 du CIC:

Conformément aux modifications apportées à l'article 88-2, il est proposé de remplacer les termes „Directeur de l'administration des Postes et Télécommunications“ par „Opérateurs des Postes“.

L'article 12 paragraphe (4) apporte des modifications à la loi du 2 août 2002 en vue de redresser certaines incohérences ayant créées des difficultés quant à l'application de certaines dispositions.

Article 3.– Champ d'application

A l'article 3 paragraphe (5) second tiret:

L'ajout de la référence au Mémorial précise que les données des personnes morales qui doivent être publiées au Mémorial en application de la loi du 10 août 1915 sur les sociétés commerciales sont exclues du champ d'application de la loi du 2 août 2002 précitée. Ceci par opposition au registre destiné à l'information et à la consultation du public lequel est exempt de notification (article 12 paragraphe (3) lettre (b)) et de publication au registre public tenu par la Commission nationale en vertu de l'article 15 paragraphe (7).

L'article 3 paragraphe (5) second tiret ajoute également au terme de „règlement“ les mots „grand-ducal“ par souci de cohérence avec la terminologie utilisée aux articles 12 paragraphe (3) et 15 paragraphe (7).

Article 11. Traitement à des fins de surveillance sur le lieu du travail

Article 11 paragraphe 1er lettre (b):

Afin de remédier aux interrogations quant à l'applicabilité de l'article 11 à une entité publique, l'article 11 paragraphe (1) lettre (b) supprime la notion d'„entreprise“ pour la remplacer par

l'expression générale de „biens de production“ permettant d'englober ceux d'une entité privée et d'une entité publique.

Article 11.– paragraphe 1er lettre (f)

L'insertion d'une lettre (f) à l'article 11 paragraphe (1) permet de tenir compte de la question de savoir si l'Etat est autorisé à effectuer un traitement à des fins de surveillance si des actes sont susceptibles d'engager sa responsabilité civile ou pénale. Cas de figure non prévu par la loi du 2 août 2002.

Article 12.– Notification préalable à la Commission nationale

L'article 12 paragraphe (2) ajoute à la fin de l'énumération des directives une nouvelle phrase qui a pour objet d'établir une cohérence entre les indications à fournir pour une notification dite „ordinaire“ (voir article 13) et celles à fournir pour une notification simplifiée (article 12 paragraphe (2)). En effet il ne va pas sans dire que la personne qui notifie doit également indiquer le nom et l'adresse du responsable du traitement et le cas échéant de son représentant ou du sous-traitant (article 13 paragraphe 1er lettre a)) ainsi que la condition de légitimité du traitement (article 13 paragraphe 1er lettre b)) qui est une condition essentielle de tout traitement de données.

La dernière phrase de l'article 12 paragraphe (2) précise que (la notification doit se faire) „par support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique“.

Suite au schéma de notification établi par la Commission nationale et en l'absence à ce stade d'un système de signature électronique opérationnel, il est jugé nécessaire de ne pas se délimiter dans la détermination de la forme de la soumission des requêtes de notification. Il s'agit avant tout d'une disposition facilitant le traitement des notifications en pratique.

L'article 12 paragraphe (3) lettre b) remplace l'expression „disposition légale“ par celle „d'une loi ou d'un règlement grand-ducal“. Le but étant d'aligner le texte sur celui de l'article 15 paragraphe (7).

Article 13.– Contenu et forme de la notification

Article 13 paragraphe (3)

Voir observations sous article 12 (dernière phrase de l'article 12 paragraphe (2)).

Article 14.– Autorisation préalable de la Commission nationale

Il est inséré un *nouveau paragraphe (3)* qui détermine le sort réservé à toute modification d'une autorisation préalable. Il s'agissait d'un oubli de la part du législateur lors de l'élaboration de la loi du 2 août 2002 précitée.

L'actuel paragraphe (3) devient le paragraphe (4). Le texte reste inchangé.

Il est également inséré un *nouveau paragraphe (5)* qui prévoit la perception d'une redevance pour les autorisations et ceci afin d'établir un certain parallélisme entre les procédures de notification et d'autorisation préalable.

Les dispositions du *nouveau paragraphe (6)* se situent dans le contexte des modifications apportées aux articles 12 paragraphe (2) et 13 paragraphe (3). Son but étant d'aligner le texte des 3 types de procédures (notification „ordinaire“, notification simplifiée, autorisation) Il s'agit également d'une disposition facilitant le traitement des autorisations en pratique.

Article 15.– Publicité des traitements

L'article 15 paragraphe (2) lettre a) essaie de pallier à un oubli en précisant que le registre public tenu par la Commission nationale contient les notifications dites „ordinaires“ (article 12 paragraphe (1er)) ainsi que les notifications simplifiées (article 12 paragraphe (2)).

Article 27.– Exceptions au droit à l'information de la personne concernée

L'article 27 paragraphe 1 de la loi rajoute un point g) ayant une teneur identique à celle du point h) des articles 15 (paragraphe 5) et 29 (paragraphe 1).

Il s'agit de redresser une omission alors que l'article 13 f) de la directive porte indistinctement sur le droit à l'information (art. 27) le droit d'accès (art. 28), et sur la publicité instaurée au moyen du registre national des traitements (art. 15).

Article 34.– Composition de la Commission nationale

Il y a lieu d'insérer à l'article 34 paragraphe (2) second paragraphe entre les alinéas 6 et 7 un nouvel alinéa avec la teneur suivante:

„Toutefois, si l'autorité investie du pouvoir de nomination estime que la nature du travail accompli et l'expérience acquise par l'intéressé au sein de la Commission nationale justifient sa nomination à une fonction supérieure à celle visée ci-dessus, elle peut procéder à une telle nomination sans que le bénéficiaire ne puisse, de ce fait, accéder à une fonction ou obtenir un rang plus élevé que les fonctionnaires de la même carrière entrés au service de l'Etat en même temps que lui ou avant lui.“

Par souci de parallélisme des textes, cette modification a pour objet de reprendre le texte figurant à l'article 8 paragraphe (1er) alinéa 3 de la loi du 25 juillet 2002 dont la loi du 2 août 2002 s'est inspirée.

Article 41.– Dispositions spécifiques

L'article 41 paragraphe (1er) dernier alinéa ainsi que le paragraphe (3) ajoute au 112 et à la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg également les centres d'appels d'urgence de la police grand-ducale.

Cet ajout permet de tenir compte d'une réalité existante au Luxembourg. En effet l'existence de 2 centres d'appels d'urgence à savoir le 112 et 113 est un fait et perçu comme tel dans le comportement des citoyens. La limitation du mécanisme prévu à l'article 41 au 112 et aux „pompiers de la Ville de Luxembourg“ reviendrait à introduire une hiérarchie dans la prestation du secours.

Notons en outre que la police grand-ducale contient 2 unités distinctes à savoir la police de secours et la police judiciaire avec 2 directions distinctes chacune. La police judiciaire est couverte par le champ d'application de l'article 41 par le biais de l'article 40 du code d'instruction criminelle; une exclusion de la police de secours de l'article 41 serait dès lors peu logique pour les raisons susénoncées.

Article 13.– Entrée en vigueur

Sans commentaire.

