I.- Projet de loi portant modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

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

Notre Conseil d'Etat entendu ;

De l'assentiment de la Chambre des Députés ;

Vu la décision de la Chambre des Députés du (…) et celle du Conseil d'Etat du (…) portant qu'il n'y pas lieu à second vote ;

Avons ordonné et ordonnons :

Art. 1er. L'article 1er (**Champ d'application**) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques est complété à la fin par l'ajout :

« (…), y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification ».

Art. 2. L'article 2 (**Définitions**) est modifié comme suit :

1. La définition de « *l'appel* » sous la lettre (b) est supprimée et les définitions subséquentes sont renumérotées.

2. A la définition des « *données de localisation* » sous la lettre (f) nouvelle ; il est inséré « *ou par un service de communications électroniques »* entre « réseau de communications électroniques » et « indiquant la position géographique (…) *».*

3. A la fin de l'article 2 une nouvelle définition, sous la lettre (m) nouvelle est ajoutée. Elle est libellée comme suit :

« (m) « violation de données à caractère personnel »: une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public ».

Art. 3. 1. Le titre de l'article 3 (**Sécurité**) est complété par l'ajout « *du traitement* ».

2. L'article 3 paragraphe (1) est complété par un nouveau ajout libellé comme suit :

« Sous réserve des dispositions générales de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, les mesures visées ci-dessus, pour le moins:

- *garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,*

- *protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et*

- *assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.*

La Commission nationale pour la protection des données est habilitée à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre. »

3. L'article 3 est complété par les paragraphes (3), (4) et (5) nouveaux qui ont la teneur suivante :

« (3). En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard la Commission nationale pour la protection des données de la violation.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de la Commission nationale pour la protection des données, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation du fournisseur d'informer l' abonné et le particulier concerné, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, la Commission

nationale pour la protection des données peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à la Commission nationale pour la protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.

La Commission nationale pour la protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission.

Lors d'un premier manquement aux obligations de notification, le fournisseur est averti par la Commission nationale pour la protection des données. En cas de manquement réitéré la Commission nationale peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.

(4) Les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, les données consignées devant être suffisantes pour permettre à la Commission nationale pour la protection des données de vérifier le respect des dispositions du paragraphe (3). Cet inventaire comporte uniquement les informations nécessaires à cette fin ».

(5) Quiconque contrevient aux dispositions des paragraphes (1) ; (2) et (4) 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. 4. A l'article 4 (**Confidentialité des communications**) paragraphe (3) la lettre b) est remplacée par le texte suivant :

« *(b) ne s'applique pas aux autorités judiciaires agissant au titre de l'article 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle 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.* »

La lettre (e) du paragraphe (3) est désormais libellée comme suit:

« (e) ne s'applique pas au stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu une information claire et complète, entre autres sur les finalités du traitement. Les méthodes retenues pour fournir l'information et offrir le droit de refus devraient être les plus conviviales possibles. Lorsque cela est techniquement possible et effectif, l'accord de l'abonné ou de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application.

Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »

Art. 5. A l'article 7 (**Identification de la ligne appelante et de la ligne connectée**) il est inséré au paragraphe (5) les lettres (a) et (b) libellées comme suit :

« (a)Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation transmet (« push ») pour chaque appel à destination d'un de ces numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation.

Aux termes du présent paragraphe on entend par « données disponibles » :

- les données relatives à l'identification: le numéro de téléphone, l'adresse électronique, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, adresse de facturation ou lieu d'établissement de l'abonné et de l'utilisateur pour autant que ce dernier soit identifié ou identifiable; l'indication du caractère public ou non public des données, ainsi que

- toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public (données de localisation).

(b) L'Institut luxembourgeois de régulation fixe, en cas de besoin, le format et les modalités techniques de mise à disposition des données visées au paragraphe (5).»

L'actuel paragraphe (5) devient la lettre (c). A la nouvelle lettre (c) les termes *« et les données de localisation de l'appelant »* sont insérés après « l'identification de la ligne appelante ».

Art. 6. Le nouveau paragraphe (2) de l'article 9 (**Données de localisation autres que les données relatives au trafic**) est complété à la fin par l'ajout. « *(…) visées au paragraphe (1) (a)* ».

Art. 7. L'article 11 (**Communications non sollicitées**) est modifié comme suit :

Le paragraphe (1er) de l'article 11 a désormais la teneur suivante :

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

Au paragraphe (2) 2^{e} ligne le terme « *directement* » est supprimé à la demi-phrase « (…) a obtenu *(...)* de ses clients leurs coordonnées électroniques (…) ».

Au paragraphe (3) le terme « *ou l'utilisateur »* est ajouté à « l'abonné ».

Art. 8. L'article 14 (**Dispositions modificatives**) est complété comme suit :

« Les articles suivants de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel sont modifiés comme suit :

*« A l'article 34 (**Composition de la Commission nationale**) paragraphe (2), 1er alinéa les mots « une fois » derrière le mot renouvelable sont supprimés.*

Le 10^{e} alinéa du paragraphe (2) se lit désormais comme suit : « *En cas de non-renouvellement ou de révocation d'un mandat d'un membre de la Commission nationale, celui-ci devient conseiller auprès de la Commission nationale avec maintien de son statut et de son niveau de rémunération de base, à l'exception des indemnités spéciales attachées à sa fonction antérieure.* »

*L'article 41 (**Dispositions spécifiques**) est abrogé. »*

Projet de texte coordonné de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques modifiée par

Loi du 27 juillet 2007
Loi du 24 juillet 2010
Loi du (…) (Transposition de la Directive 2009/136 « protection des données » du nouveau paquet télécom)

Art. 1er. Champ d'application

(Loi du…)

Sous réserve des dispositions générales concernant la protection des personnes à l'égard du traitement des données à caractère personnel ou régissant les réseaux et services de communications électroniques, les dispositions suivantes s'appliquent spécifiquement au traitement de ces données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics, « *y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification.*»

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;

(Loi du…)

«appel»: (…) ;

(*b*) «consentement»: toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement;

(*c*) «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;

(*d*) «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;
(*e*) «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;

(Loi du…)

(*f*) «données de localisation»: toutes les données traitées dans un réseau de communications électroniques « *ou par un service de communications électroniques* » indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

(*g*) «Institut»: l'Institut Luxembourgeois de Régulation;

(*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 des 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 à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

(Loi du…)

« (m) « violation de données à caractère personnel»: une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public».

(Loi du…)

Art. 3. Sécurité « *du traitement* »

(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 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.

(Loi du…)

« Sous réserve des dispositions générales de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, les mesures visées ci-dessus, pour le moins:

- *garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,*

- *protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et*

- *assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.*

La Commission nationale pour la protection des données est habilitée à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre. »

(2) Sans préjudice 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 ou des services mettant en cause la confidentialité des communications ainsi que du moyen éventuel pour y remédier, y compris en en indiquant le coût probable.

(Loi du…)

« (3). En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard la Commission nationale pour la protection des données de la violation. Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de la Commission nationale pour la protection des données, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation du fournisseur d'informer l'abonné et le particulier concerné, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, la Commission nationale pour la protection des données peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à la Commission nationale pour la protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.

La Commission nationale pour la protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission.

Lors d'un premier manquement aux obligations de notification, le fournisseur est averti par la Commission nationale pour la protection des données. En cas de manquement réitéré la Commission nationale peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.

(4) Les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, les données consignées devant être suffisantes pour permettre à la Commission nationale pour la protection des données de vérifier le respect des dispositions du paragraphe (3). Cet inventaire comporte uniquement les informations nécessaires à cette fin.

(5) Quiconque contrevient aux dispositions des paragraphes (1) ; (2) et « (4) » 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. 4. Confidentialité des communications

(1) Tout fournisseur de services ou opérateur garantit 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 autre personne que l'utilisateur 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'utilisateur 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;

(Loi du…)

« *(b) ne s'applique pas aux autorités judiciaires agissant au titre de l'article 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle 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 afférentes aux communications visées ci-dessus, y compris 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 au plus;

(Loi du 27 juillet 2007)

(d) n'affecte pas l'enregistrement 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*».

Les parties aux transactions « *ou à toutes autres communications commerciales »* sont informées au préalable de ce que des enregistrements sont susceptibles d'être effectués, de la ou des raisons pour lesquelles les communications sont enregistrées et de la durée de conservation maximale des enregistrements. Les communications enregistrées sont à effacer dès que la finalité est atteinte, et en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction;

(Loi du…)

« (e) ne s'applique pas au stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu une information claire et complète, entre autres sur les finalités du traitement. Les méthodes retenues pour fournir l'information et offrir le droit de refus devraient être les plus conviviales possibles. Lorsque cela est techniquement possible et effectif, l'accord de l'abonné ou de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application.

Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.»

(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

(Loi du 27 juillet 2007)
(Loi du 24 juillet 2010)

« (1) (a) Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, 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 ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données relatives au trafic est tenu de conserver ces données pendant une période de « six mois » à compter de la date de la communication. L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet) dans le cadre de la fourniture des services de communications concernés. Un règlement grand-ducal détermine les catégories de données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires.»

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

(2) Tout fournisseur de services ou tout opérateur qui traite des données relatives au trafic concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires pour 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 ou aux traitements prévus par les dispositions sub (3) et (4), à l'exception des accès qui sont:

(Loi du 24 juillet 2010)

- *« ordonnés par les autorités judiciaires agissant au titre de l'article 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle 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 visées au paragraphe (1) (a), ou »*

- demandés par les organes compétents 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 et ne peut en tout état de cause

dépasser 6 mois lorsque la facture a été payée et n'a pas fait l'objet de litige ou de contestation.

(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 ou l'opérateur informe préalablement l'abonné ou l'utilisateur 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 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) à (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur qui sont chargés d'assurer la facturation ou la gestion du trafic, répondre aux demandes de clientèle, détecter les fraudes, commercialiser les services de communications électroniques ou 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) à (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.

(Loi du 24 juillet 2010)

« **Art. 5-1** *(1) Les données conservées au titre des articles 5 et 9 sont soumises aux exigences prévues aux articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*

(2) Les données sont détruites lorsque la durée de conservation prend fin, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées.

***Art. 5-2**. (1) La Commission nationale pour la protection des données transmet annuellement à la Commission de l'Union européenne des statistiques sur la conservation de données au titre des articles 5 et 9.*

A cet effet les fournisseurs de services ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment :

- *les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,*

- *le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,*

- *les cas dans lesquels des demandes de données n'ont pu être satisfaites.*

(2) Ces statistiques ne contiennent pas de données à caractère personnel.»

Art. 6. Facturation détaillée

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

(2) Les appels gratuits y compris ceux aux lignes d'assistance 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 les cas où la présentation de l'identification de la ligne appelante est offerte, 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 les cas où la présentation de l'identification de la ligne appelante est offerte, 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 les cas où la présentation de l'identification de la ligne appelante est offerte 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 à l'utilisateur appelant.

(Loi du…)

(5) *« (a)Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation transmet (« push ») pour chaque appel à destination d'un de ces*

numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation.

Aux termes du présent paragraphe on entend par « données disponibles » :

- les données relatives à l'identification: le numéro de téléphone, l'adresse électronique, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, adresse de facturation ou lieu d'établissement de l'abonné et de l'utilisateur pour autant que ce dernier soit identifié ou identifiable; l'indication du caractère public ou non public des données, ainsi que

- toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public (données de localisation).

(b) L'Institut luxembourgeois de régulation fixe, en cas de besoin, le format et les modalités techniques de mise à disposition des données visées au paragraphe (5). »

(c) 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 « *et les données de localisation de l'appelant »* sont toujours présentées même lorsque l'appelant les a empêchées.

(6) Les dispositions du paragraphe (1) 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 sus énoncées.

(8) L'abonné appelé prétendant être victime d'appels à contenu malveillant ou dérangeant peut demander l'identification de la ligne appelante ou connectée, des appels répétés ou intempestifs, déclarés comme étant malveillants ou dérangeants, 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 ou l'opérateur ainsi que par les abonnés prétendant être victime d'appels à contenu malveillant ou dérangeant. Il précisera également les caractéristiques d'un appel à contenu malveillant ou dérangeant 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, 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

(Loi du 27 juillet 2007)
(Loi du 24 juillet 2010)

« (1) (a) Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, 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 ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données de localisation autres que des données relatives au trafic est tenu de conserver ces données pendant une période de « six mois » à compter de la date de la communication. L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet) dans le cadre de la fourniture des services de communications concernés. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou appel. Un règlement grand-ducal détermine les catégories de données de localisation autres que les données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires».

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

(Loi du 24 juillet 2010)
(Loi du…)

«(2) Tout fournisseur de services ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient conservées pendant la période prévue au paragraphe (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 judiciaires agissant au titre de l'article 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle 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 « visées au paragraphe (1) (a)».».

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

(4) Le fournisseur du service et le cas échéant l'opérateur informe préalablement l'abonné ou l'utilisateur 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. L'abonné ou l'utilisateur a la possibilité de retirer à tout moment son consentement pour le traitement des données de localisation autres que les données relatives au trafic. Lorsque l'abonné ou l'utilisateur a donné son consentement au traitement des données de localisation autres que les données relatives au trafic, il doit garder 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) à (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services 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.

(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. 10. Annuaires d'abonnés

(1) L'abonné doit être informé gratuitement et avant d'y être inscrit 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) 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

(Loi du …)

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

(Loi du …)

(2) Nonobstant le paragraphe (1), le fournisseur qui, dans le cadre d'une vente d'un produit ou d'un service, a obtenu *(...)* de ses clients leurs coordonnées électroniques en vue d'un courrier électronique, peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues que lui-même fournit pour autant que lesdits clients se voient donner clairement et expressément le droit de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques « *au moment où* » elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.

(Loi du…)

(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 « *ou l'utilisateur* » 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 faire cesser ces communications.

(5) Les paragraphes (1) et (3) s'appliquent à l'abonné qui est une personne physique.

(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. Commission nationale pour la protection des données

(Loi du 27 juillet 2007)

La Commission nationale pour la protection des données instituée par 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 est chargée d'assurer l'application des dispositions de la présente loi et de ses règlements d'exécution *« sans préjudice de l'application de l'article 8 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. »*

Art.13. Disposition transitoire

Le fournisseur offrant un annuaire public au sens de l'article 10 avant l'entrée en vigueur de la présente loi informe l'abonné sans délai et conformément à l'article 10 paragraphe (1) de la finalité du traitement de ses données.

Art. 14. Dispositions modificatives

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 du Code d'instruction criminelle 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.

(Loi du…)

« Les articles suivants de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel sont modifiés comme suit :

*« A l'article 34 (**Composition de la Commission nationale**) paragraphe (2), 1er alinéa les mots « une fois » derrière le mot renouvelable sont supprimés.*

Le 10e alinéa du paragraphe (2) se lit désormais comme suit : « *En cas de non-renouvellement ou de révocation d'un mandat d'un membre de la Commission nationale, celui-ci devient conseiller auprès de la Commission nationale avec maintien de son statut et de son niveau de rémunération de base, à l'exception des indemnités spéciales attachées à sa fonction antérieure.* »

*L'article 41 (**Dispositions spécifiques**) est abrogé. »*

Art. 15. Disposition diverse

La référence à la présente loi se fait sous une forme abrégée en recourant à l'intitulé suivant: «Loi du…concernant la protection de la vie privée dans le secteur des communications électroniques».

Art. 16. Entrée en vigueur

La présente loi entre en vigueur le premier jour du mois qui suit sa publication au Mémorial. Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

II.- Exposé des motifs

Le présent projet de loi a pour objet de modifier les articles 1er (champ d'application); 2 (définitions) ; 3 (sécurité) ; 4 (confidentialité) et 11 (communications non sollicitées) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (ci-après « la loi modifiée du 30 mai 2005 »), afin de transposer en droit luxembourgeois la directive 2009/136/CE.

La directive 2009/136/CE[1] (ci-après « la directive ») fait partie du nouveau « paquet télécom » », réforme du cadre réglementaire de l'Union européenne pour les réseaux et services de communications électroniques, qui est entré en vigueur le 19 décembre 2009. La directive modifie donc la directive 2002/58/CE « directive vie privée et communications électroniques » qui a été transposée en droit national par la loi du 30 mai 2005 précitée.

Les modifications se situent dans le contexte de la réforme du cadre réglementaire de l'Union européenne pour les réseaux et services de communications électroniques. Cette réforme est devenue nécessaire suite à l'évolution des technologies et du marché. Les modifications ont pour objet d'instaurer un niveau de protection élevé de la vie privée et des données à caractère personnel qui soit équivalent pour chaque consommateur et utilisateur quelle que soit la technologie utilisée pour fournir un service donné.

Le présent projet de loi a encore pour but de procéder à une modification ponctuelle de deux dispositions concernant le mandat et le statut des membres de la Commission nationale pour la protection des données pour l'ajuster à celui d'autres établissements publics (Commissariat aux assurances, CSSF, Banque Centrale).

En effet, il est proposé de prévoir qu'à l'avenir, le mandat des membres de la CNPD est renouvelable sans limitation de durée. En outre, le membre issu du secteur privé dont le mandat n'est pas renouvelé, bénéficiera à l'avenir de la possibilité de devenir conseiller auprès de la CNPD. Le texte actuellement en vigueur prévoit dans l'hypothèse d'une cessation de mandat le maintien de la rémunération pendant une durée maximale d'un an.

III.- Commentaire des articles

Article 1er

L'ajout complète la transposition de l'article 3 de la directive dont la majeure partie demeure inchangée par rapport au texte initial. L'ajout tient compte des nouvelles technologies d'identification telles que RFID. Il s'agit d'un dispositif d'identification qui utilise des fréquences radio pour saisir les données

[1] Directive 2009/136/CE nouveau « paquet télécom » publiée au JO de l'UE L337/11 du 18.12.2009

provenant d'étiquettes identifiées de manière unique, ces données peuvent ensuite être transférées via les réseaux de communications existants. Une large utilisation de ces technologies peut générer des avantages économiques et sociaux considérables pour autant que l'usage inspire confiance auprès du consommateur. Pour ce faire il faut que les droits fondamentaux du citoyen en tant qu'utilisateur et consommateur, y compris son droit à sa vie privée et à la protection de ses données, soient suffisamment protégés.

Article 2

1. La définition de « *l'appel* » sous la lettre (b) est supprimée comme le prévoit l'article 2 lettre b) de la directive. Il s'agit d'une définition qui, pour des raisons de neutralité technologique, n'est plus utilisée par le nouveau paquet télécom. L' « appel » est désormais traité comme un service de communication électronique parmi d'autres. L' »appel » ne connaît donc plus de définition particulière.

2. L'insertion « *ou par un service de communications électroniques* à la définition des « *données de localisation* » sous la lettre (f) nouvelle est une adaptation de la terminologie qui s'explique par la transposition du nouveau paquet télécom. Il s'agit de l'article 2 lettre a) de la directive.

3. L'insertion d'une nouvelle définition *« violation de données à caractère personne »* sous la lettre (m), telle que prévue par l'article 2 lettre c) de la directive, s'explique par l'introduction d'une nouvelle procédure de notification en cas de violation de la sécurité et de mise en péril des données personnelles prévue à l'article 3 paragraphes (3) et (4) nouveaux du projet de loi..

Article 3

1. Le titre de l'article 3 (Sécurité) est complété par l'ajout « *du traitement* ». Il transpose l'article 4 lettre a) de la directive. Il s'agit d'une adaptation de la terminologie qui n'apporte pas de commentaire particulier.

2. L'article 3 paragraphe (1) est complété par un nouvel ajout qui précise davantage les exigences en matière de sécurité du traitement. L'ajout tient compte des préoccupations formulées par la CNPD dans son avis du 10 novembre 2010 quand bien même les dispositions générales prévues aux articles 22 (Sécurité des traitements) et 23 (Mesures de sécurité particulières) de la loi générale du 2 août 2002 s'appliquent également dans le cadre de la loi modifiée du 30 mai 2005 précitée (voir article 1er Champ d'application de la loi modifiée du 30 mai 2005).

La CNPD se prononce en faveur de l' insertion des mesures de sécurité dans le texte du projet de loi plutôt que de renvoyer aux articles 22 et 23 de la loi générale du 2 août 2002 au motif que « *les auteurs de la directive ont vu une*

utilité suffisante pour les insérer dans la directive par souci de sécurité juridique et de précision quant aux prérogatives de l'autorité de contrôle dans l'application pratique ».

3. L'introduction d'une nouvelle procédure de notification en cas de violation des données à caractère personnel aux paragraphes (3) et (4) nouveaux de l'article 3 constitue la principale modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques. Elle transpose l'article 4 lettre c) de la directive. Cette mesure souligne l'importance d'informer la personne concernée et la CNPD lorsque les données personnelles de la personne concernée sont compromises ou risquent de l'être.

Il ressort du considérant (61) de la directive qu' « *une violation devrait être considérée comme affectant les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier lorsqu'elle est susceptible d'entraîner, par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée en rapport avec la fourniture de services de communications accessibles au public dans la Communauté.* »

La notification des violations de sécurité se traduit d'une part par l'intérêt général du citoyen à être informé des violations de sécurité qui pourraient se traduire par la perte ou l'altération de ses données à caractère personnel et d'autre part par l'obligation du responsable du traitement de mettre en œuvre des mesures de protection appropriées sur le plan technique et organisationnel afin de minimiser les pertes économiques ou dommages sociaux éventuels pouvant découler de ces violations.

L'introduction d'une procédure de notification des violations est la réponse communautaire aux cas de vol, perte et détérioration de données personnelles qui se sont produits récemment dans certains Etats Membres de l'Union européenne.

L'article 3 paragraphe (3) nouveau alinéa 6 décrit la faculté pour la CNPD d'adopter des lignes directrices et, le cas échéant d'édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation des données, le format applicable à cette notification et sa procédure de transmission. Il s'agit d'une transposition fidèle de l'article 4 lettre c) point 4 de la directive réclamée par la CNPD dans son avis.

L'alinéa 7 de l'article 3 paragraphe (3) nouveau introduit, suite à la demande de la CNPD, une sanction administrative au lieu d'une sanction pénale. Les sanctions prévues à l'alinéa 7 (l'avertissement et l'amende administrative) ont pour objet de sanctionner tout manquement à l'obligation de notification des violations de données de la part du fournisseur. Comme le souligne la CNPD aucune sanction prévue à l'article 33 de la loi modifiée du 2 août 2002 paraît appropriée pour sanctionner le non respect répété de l'obligation de notification. La sanction pécuniaire d'ordre administratif est donc considérée comme étant plus appropriée pour permettre à la CNPD de réagir rapidement

dans le cadre de la procédure de notification. L'avertissement et la sanction pécuniaire d'ordre administratif devraient en outre permettre de désengorger les juridictions pénales.

4. Le paragraphe (4) nouveau de l'article 3 est une transposition fidèle de l'article 4 lettre c) point 4 dernier alinéa de la directive et n'apporte pas de commentaire particulier.

5. Le paragraphe (5) nouveau de l'article 3 reprend la sanction pénale telle que prévue dans le texte originaire de la loi modifiée du 30 mai 2005 et l'applique aux paragraphes (1), (2) et (4) nouveau. Le paragraphe (5) nouveau observe ainsi le parallélisme des dispositions pénales prévues dans le texte de loi.

Article 4

La nouvelle lettre b) du paragraphe (3) de l'article 4 a pour objet de pallier à un oubli de la loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle d'aligner le texte de la nouvelle lettre b) sur celui du nouveau paragraphe (2) des articles 5 (tiret 1er) et 9 qui exige une autorisation judiciaire comme condition préalable d'accès aux données relatives au trafic et aux données de localisation autres que les données relatives au trafic.

La nouvelle lettre e) du paragraphe (3) de l'article 4 transpose l'article 5 paragraphe (3) de la directive. Le nouveau texte de la lettre e) est une adaptation de la terminologie qui tient compte de l'évolution technique en matière de témoins de connexion (« cookies »). Le nouveau texte vise le cas où des tiers souhaitent stocker des informations sur l'équipement d'un utilisateur, ou obtenir l'accès à des informations déjà stockées, à des fins diverses, qu'elles soient légitimes ou qu'elles impliquent une intrusion non autorisée dans la sphère privée (logiciels espions ou virus). Il est donc important que l'utilisateur dispose d'informations claires et complètes lorsqu'il entreprend une démarche susceptible de déboucher sur un stockage ou un accès de ce type. Le nouveau libellé de la lettre e) intègre également les précisions contenues au considérant (66) de la directive, à savoir l'exigence de la convivialité pour l'utilisateur et la référence à l'utilisation de solutions techniques pour l'expression de l'accord. Ces précisions sont en effet essentielles pour garantir une certaine flexibilité dans l'exécution de cette obligation.

Notons encore que la teneur de l'article 6 paragraphe (3) de la directive est identique au texte actuel de l'article 5 paragraphe (4) de la loi modifiée du 30 mai 2005. Le texte actuel demeure donc inchangé.

Article 5

Au paragraphe (5) de l'article 7 il est inséré une nouvelle lettre a) qui a pour objet de pallier à un vide juridique créé par la loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle laquelle a supprimé à l'article 9 (1) a) la dernière phrase libellée comme suit : «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 ».

La lettre a) réintroduit la base légale jugée indispensable pour les services d'appels d'urgence d'accéder aux informations relatives à la localisation de l'appelant en détresse.

Puisque les précisions apportées par la lettre a) ont trait à l'identification de la ligne appelante et de la ligne connectée, il est jugé plus opportun de préciser ces dispositions à l'article 7 (Identification de la ligne appelante et de la ligne connectée) paragraphe (5) plutôt qu'à l'article 9 (données de localisation autres que les données relatives au trafic).

Le lettre a) couvre les cas d'appel vers un numéro d'appel d'urgence déterminé par l'ILR. Il s'agit en l'occurrence des numéros 112 et 113. Dans ces cas, le fournisseur ou opérateur de services de téléphonie fixe ou mobile est obligé de transmettre en mode « push »et en temps réel les informations disponibles dont la localisation concernant l'appelant aux centres de réception des appels d'urgence respectifs. L'obligation énoncée à la nouvelle lettre a) incombe à chaque fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès aux numéros d'appel d'urgence tels que définis par l'ILR. La nouvelle lettre a) précise en outre pour le cas spécifique en question ce qu'il faut entendre par données disponibles.

La nouvelle lettre b) crée une base légale permettant à l'ILR de définir, le cas échéant, les modalités techniques pour faciliter le transfert de données entre fournisseurs ou opérateurs de services de téléphonie fixe ou mobile et les centres de réception des appels d'urgence respectifs.

La nouvelle lettre c) reprend le texte de l'ancien paragraphe (5) et précise que les informations qui doivent être présentées aux services d'urgence sont non seulement celles relatives à « l'identification de la ligne appelante » mais également «les données de localisation de l'appelant ». Cette précision est prévue à l'article 26 paragraphe (5) de la directive « service universel » du nouveau paquet « télécom ».

Article 6

La référence au seuil de peine au paragraphe (2) nouveau de l'article 9 corrige un oubli de la loi du 24 juillet 2010 portant modification des articles 5

et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle. La référence au seuil de peine limite l'accès aux données de localisation autres que les données relatives au trafic pour les infractions qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.

Article 7

Le champ d'application du paragraphe (1er) nouveau de l'article 11 est étendu aux SMS, MMS et autres applications de nature semblable. Le paragraphe (1er) nouveau précise, pour une plus grande sécurité juridique, que l'envoi à des fins de prospection directe n'est possible que s'il vise l'abonné ou l'utilisateur qui a donné son consentement préalable.

Au paragraphe (2) 2e ligne de l'article 11 la suppression de l'adjectif « directement » tient également compte de l'hypothèse où les coordonnées électroniques peuvent être obtenues auprès du client par un intermédiaire.

L'ajout « ou l'utilisateur » au paragraphe (3) de l'article 11 est une adaptation de la terminologie par le nouveau paquet télécom et n'apporte pas de commentaire particulier.

Les modifications de l'article 11 transposent l'article 13 de la directive.

Article 8

La modification apportée à l'article 34 (Composition de la Commission nationale) paragraphe (2) alinéa 1er de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel a pour objet de garantir une stabilité élémentaire dans l'exercice de mandat des membres de la Commission nationale. Par référence à d'autres établissements publics, il est proposé de prévoir au niveau du renouvellement du mandat la possibilité d'un renouvellement répété, ce qui est d'ailleurs aussi prévu pour les membres de la direction d'autres établissements publics, comme la CSSF, la Banque Centrale et le Commissariat aux Assurance.

La modification apportée à l'article 34 paragraphe (2) 10e alinéa consiste à prévoir, dans l'hypothèse où le mandat n'est pas renouvelé ou lorsqu'il est révoqué, la possibilité pour les membres qui sont issus du secteur privé de devenir conseiller de la CNPD pour une durée illimitée, avec maintien de leur rémunération (ceux issus de la Fonction Publique bénéficient de la possibilité d'invoquer en plus un changement d'administration). Cette possibilité est également prévue (en cas de non renouvellement ou de révocation pour la CSSF et la Banque Centrale, en cas de non renouvellement pour la Cour des Comptes et en cas de remplacement suite à une démission ou décès pour le Commissariat) mais il échet de signaler que les membres de la direction de ces établissements ont tous la qualité de fonctionnaire.

L’abrogation de l’article 41 (Dispositions spécifiques) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l’égard du traitement des données à caractère personnel s’explique essentiellement par 2 types de difficultés rencontrés lors de la tentative de mise en œuvre pratique du système décrit à l’article 41. L’un tient à la spécificité du système – notamment du fait de devoir gérer le système d’information sans avoir le droit d’accéder aux informations y traitées - et à la complexité de l’architecture du système d’information, l’autre tient à la maintenance du système. La mise en œuvre pratique de l’article 41 aurait en outre généré des coûts exorbitants et disproportionnés par rapport à sa finalité.