N° 6921[3]

CHAMBRE DES DEPUTES

Session ordinaire 2015-2016

P R O J E T D E L O I

portant:

1) modification du Code d'instruction criminelle,

2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques,

3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,

4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste

* * *

SOMMAIRE:

*

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

(8.8.2016)

Monsieur le Président,

A la demande du Ministre de la Justice, j'ai l'honneur de vous saisir d'amendements gouvernementaux au projet de loi sous rubrique.

A cet effet, je joins en annexe le texte des amendements des commentaires, une fiche financière afférente ainsi qu'une version coordonnée du projet de loi tenant compte desdits amendements.

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

Le Ministre aux Relations
avec le Parlement,
Fernand ETGEN

*

TEXTE DES AMENDEMENTS GOUVERNEMENTAUX

1. L'intitulé du projet de loi est modifié comme suit:

„Projet de loi portant

1) modification du Code d'instruction criminelle,

2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques,

3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,

4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste"

2. A l'article 1 du projet de loi au point 4), l'alinéa 1 du paragraphe (1) de l'article 48-27 est modifié comme suit:

„**Art. 48-27:** (1) Dans le cadre de l'enquête pour crime ou délit ou de l'instruction préparatoire, le procureur d'Etat ou le juge d'instruction peut, par une décision motivée et écrite, en requérant au besoin le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de télécommunications, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients de l'opérateur ou sur base de l'article 10bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à:"

3. L'article 2 du projet de loi est supprimé et remplacé par le texte suivant:

Art. 2: Il est ajouté un nouvel article 10bis à la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, libellé comme suit:

„**Art. 10bis:** ***Fichier centralisé auprès de l'Institut***

(1) Il est créé un fichier sous forme électronique auprès de l'Institut qui contient les données transmises conformément au paragraphe (2). Le fichier a pour finalité de mettre à la disposition des autorités et services énumérés au paragraphe (4) les données y figurant.

Le fichier est hébergé auprès du Centre des technologies de l'information de l'Etat qui en assure la gestion opérationnelle.

(2) Les entreprises notifiées auprès de l'Institut conformément à la loi du 27 février 2011 sur les réseaux et les services de communications électroniques qui fournissent un service de communications électroniques accessible au public en ayant recours à des ressources de numérotation luxembourgeois (ci-après: „les entreprises notifiées") transmettent d'office et gratuitement à l'Institut par voie électronique et au moyen d'un interface sécurisé, les données suivantes:

a) Pour les personnes physiques: le nom, le prénom, le lieu de résidence habituelle, la date et le lieu de naissance ainsi que le numéro de contact de l'abonné,

Pour les personnes morales: la dénomination ou raison sociale, l'adresse du lieu d'établissement ainsi que le numéro de contact;

b) le nom de l'entreprise notifiée, la nature du service fourni par celle-ci, le numéro d'appel alloué pour lequel le service en question a été souscrit et si disponible, la date de la fin de la relation contractuelle ou en cas de service à prépaiement la date de désactivation du numéro d'appel.

La liste du type de services visés au point b) est déterminée par règlement de l'Institut;

c) pour les personnes physiques, le type, le pays de délivrance et le numéro de la pièce d'identité ou de l'attestation de dépôt d'une demande de protection internationale de l'abonné en cas de service à prépaiement.

Ces données doivent être actualisées au moins une fois par jour, même en l'absence de changement.

Un rapport sur le transfert des données est généré automatiquement une fois par jour auprès du Centre des technologies de l'information de l'Etat.

Le protocole et l'interface sécurisés ainsi que le format d'échange à utiliser pour le transfert de ces données sont déterminés par règlement de l'Institut.

(3) Le non-respect du paragraphe (2) du présent article et du règlement de l'Institut pris en son exécution peut être sanctionné par l'Institut conformément à l'article 83 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques.

(4) Le procureur d'Etat, le juge d'instruction et les officiers de police judiciaire visés à l'article 10 du Code d'instruction criminelle agissant dans le cadre de l'article 48-27 (7) du Code d'instruction criminelle, ainsi que le Service de renseignement de l'Etat accèdent de plein droit au fichier visé au paragraphe (1) du présent article. L'accès de plein droit se limite aux mesures prévues par l'article 48-27 du Code d'instruction criminelle et à celles prises dans le cadre de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Le central 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 aux seules données visées au paragraphe (2) a) du présent article. Cet accès se limite aux mesures particulières de secours d'urgence prestées dans le cadre des activités de le central 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 et s'effectue uniquement sur les communications entrantes.

Le motif de chaque consultation doit être enregistré au moment de l'accès.

Le Service de renseignement de l'Etat, le central 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 désignent chacun en ce qui le concerne les agents qui bénéficient d'un accès individuel.

(5) L'accès à distance aux données du fichier centralisé se fera par voie de requête électronique et sera sécurisé par un mécanisme d'authentification forte.

(6) Les informations relatives à la personne ayant procédé à la consultation, les informations consultées, les critères de recherche, la date et l'heure de la consultation, ainsi que le motif de la consultation sont enregistrés. Ces données sont effacées irrémédiablement et sans délai, cinq ans à compter de la date d'accès.

Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation.

(7) Les données visées au paragraphe (2) doivent être effacées irrémédiablement et sans délai trois ans à compter de la fin de la relation contractuelle ou, en cas de service à prépaiement, à compter de la date de désactivation du numéro d'appel.

(8) L'Institut fait procéder régulièrement à un audit sur le fonctionnement du fichier prévu au paragraphe (1) pour contrôler la mise en oeuvre des mesures techniques et organisationnelles appropriées."

4. Il est ajouté un article 3 nouveau au projet de loi libellé comme suit:

Art. 3: Le fichier qui est prévu à l'article 10bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques doit être mis en oeuvre au plus tard un an après l'entrée en vigueur de la loi.

Les dispositions de l'article 10bis s'appliquent:

- aux contrats conclus après l'entrée en vigueur de la présente loi,
- aux contrats existants avant l'entrée en vigueur de la présente loi, dans la mesure où les données prévues en son paragraphe (2) avaient été collectées au moment de la conclusion du contrat, sans préjudice de l'obligation d'actualisation des données ultérieure prévue en son paragraphe (2) alinéa (2).

5. Il est ajouté un article 4 nouveau libellé comme suit:

Art. 4: La loi du 27 février 2011 sur les réseaux et les services de communications électroniques est modifiée comme suit:

1) A l'article 73, il est rajouté un nouveau paragraphe (3) libellé comme suit:

„(3) L'entreprise fournissant les services de communications électroniques accessible au public en ayant recours à des ressources de numérotation doit relever les données suivantes auprès de l'utilisateur final:

– Si l'utilisateur final est une personne physique: le nom, le prénom, le lieu de résidence habituelle, la date et le lieu de naissance de l'abonné;
– Si l'utilisateur final est une personne morale: la dénomination ou raison sociale, l'adresse du lieu d'établissement."

2) A l'article 83, il est rajouté un nouveau paragraphe (1)bis libellé comme suit:

„(1)bis: Toute violation par une entreprise soumise à notification en vertu de l'article 8 paragraphe (1) de la présente loi, de l'obligation prévue à l'article 10bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, ainsi que de ses règlements d'exécution, peut être sanctionnée par l'Institut conformément au présent article".

*

EXPOSE DES MOTIFS

CONSIDERATIONS GENERALES

Le projet de loi 6921 a été préparé dans les jours qui ont suivi les tragiques attentats de Paris.

Il propose plusieurs mesures concrètes qui s'inspirent notamment des législations belge et française.

Une des mesures est de permettre un accès direct aux fichiers des opérateurs réunis dans une banque de données unique à tenir par l'Institut Luxembourgeois de régulation. Dans cette optique, le projet de loi propose de remettre en vigueur l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Cet article, bien que voté, n'a jamais été mis en application à l'époque.

Après le dépôt du projet de loi et après des premiers échanges avec les instances concernées par cette banque de données, il semble plus opportun de créer cette banque de données en prévoyant cet article dans la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques en prévoyant un article 10bis nouveau.

Les différentes modalités de l'article ont par ailleurs été revues, actualisées et complétées, suite à une large consultation des acteurs concernés (ILR; Parquet général, Ministère d'Etat, Police, Services de secours).

Cette modification fait l'objet des présents amendements.

*

COMMENTAIRE DES ARTICLES

Amendement 1

Une des innovations proposées par le projet de loi 6921 visait à l'article 2 à mettre en place une banque de données qui permet dans les conditions de l'article 48-27 un accès direct au fichier des opérateurs réunis dans cette banque de données. Il était prévu dans le texte initial de réintroduire dans ce but l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des données à l'égard du traitement des données à caractère personnel qui avait été supprimé par loi du 28 juillet 2011 portant modification 1) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques; 2) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; 3) de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat; 4) du Code de la consommation.

Après réflexion, il s'avère qu'il serait plus opportun de prévoir la création de cette banque de données dans la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques.

Ainsi il appert approprié de prévoir cette banque de données dans un article 10bis nouveau de cette loi. Etant donné que cet amendement comporte une modification de la loi précitée du 30 mai 2005 il

y a lieu de la mentionner dans l'intitulé du projet de loi. Il en va de même des modifications de la loi du 27 février 2011 qui figurent à l'article 4 nouveau tel que proposé.

L'intitulé du projet de loi est dès lors modifié afin de tenir compte de ces amendements.

Amendement 2:

L'article 48-27 tel que proposé dans le projet de loi fait un renvoi à l'article 41bis que le projet de loi propose de créer.

Etant donné que la création de la banque de données est dorénavant prévue à l'article 10bis de la loi modifiée du 30 mai 2005 (et non plus à l'article 41bis de la loi modifiée du 2 août 2002), il y a lieu de corriger la référence prévue à l'article 48-27 et figurant à l'article 1 du projet de loi.

Amendement 3

A l'instar de ce qui a été précisé ci-avant, il y a lieu de remplacer l'article 2 actuel du projet de loi par une disposition prévoyant l'ajout d'un nouvel article 10bis à la loi du 30 mai 2005.

Il est proposé de créer cette banque de données ou ce fichier centralisé auprès de l'Institut Luxembourgeois de Régulation (ci-après: „l'Institut"). Ce nouvel instrument présente une plus-value et efficacité indiscutables alors qu'il permet un accès direct et à distance par voie de communication électronique aux informations portant sur les abonnés des opérateurs. Il faut rappeler qu'en l'état actuel une telle mesure nécessite un mandat du juge d'instruction et des perquisitions individuelles auprès des opérateurs pour obtenir les informations en question.

Le fichier créé auprès de l'Institut sera hébergé auprès du Centre des Technologies et de l'Information de l'Etat qui en assurera la gestion quotidienne opérationnelle. En effet, cette solution permet de mutualiser les infrastructures informatiques opérées par le CTIE et également de profiter du cadre de sécurité du centre. L'Institut est ainsi le responsable du traitement de la banque de données et le CTIE la gère en sous-traitance.

Le paragraphe (2) de l'article reprend la liste des données à transmettre dans le fichier. Sont soumises à cette obligation les entreprises qui fournissent un service de communication électroniques accessible au public en ayant recours à des ressources de numérotation. Cette transmission de données se fait uniquement grâce à l'utilisation d'un protocole ou interface sécurisé et dans un format spécifique. Les modalités techniques détaillées sont déterminées dans un règlement de l'Institut, permettant une adaptation rapide aux évolutions techniques et aux besoins de sécurité futurs.

Les données à transmettre sont le nom, prénom, lieu de résidence, numéro de contact de la personne physique ou morale, le nom de l'opérateur, le numéro d'appel, la nature du service fourni et des renseignements sur la date de la fin de la relation contractuelle.

Pour les services à prépaiements, l'opérateur devra également fournir des informations sur la pièce d'identité de l'abonné qui est à verser.

Le texte prévoit également une obligation de mettre ces données à jour toutes les 24 heures. En effet, compte tenu de l'importance du caractère actuel des informations concernées, une telle adaptation journalière est nécessaire.

Le paragraphe (3) prévoit les sanctions qui peuvent s'appliquer en cas de non-respect de l'obligation. Il est renvoyé à l'article 83 de la loi modifiée du 27 février 2011 dont le libellé est également modifié par les présents amendements. Il est renvoyé à ce sujet à l'amendement n° 5.

Le paragraphe (4) nouveau tel que proposé reprend des dispositions des paragraphes 1 et 3 de l'article 41 tel que proposé dans le projet de loi et tel qu'il avait existé après le vote de 2002.

Ce texte reprend ainsi la liste des autorités qui peuvent accéder de plein droit au fichier qui sera créé. Il s'agit en l'espèce du Procureur d'Etat, du Juge d'instruction, d'officiers de police judiciaire dans le cadre de l'article 48-27 ainsi que du SRE. L'accès des Services 112, la Police grand-ducale et le Service d'incendie se limite aux seuls données nécessaires dans le cadre de leur mission et ceci uniquement lorsqu'ils sont sollicités. Il est également prévu que le motif de chaque consultation devra être enregistré.

Il faut noter que les modalités d'accès à la base pour les services de secours seront en fait différentes de celles pour les acteurs des autorités judiciaires et de la Police grand-ducale dans le cadre de leurs enquêtes respectives. Ainsi lors d'un appel au central des secours d'urgence 112 ou aux centres d'appels d'urgence de la police grand-ducale, un processus automatique et immédiat lance la requête à cette

base. Sur l'écran du CSU 112 ou d'un des centres d'appels d'urgence de la police grand-ducale s'affichera le numéro et l'identification et ce sans l'intervention manuelle du gestionnaire des appels au central des secours d'urgence 112 et aux centres d'appel d'urgence de la police.

Les conditions d'accès sont contrôlées par le droit commun, à savoir pour la Commission article 17 respectivement par la CNPD.

Le paragraphe (5) tel que libellé prévoit que l'accès a lieu via requête électronique. L'accès à distance doit par ailleurs être sécurisé par un mécanisme d'authentification forte.

Paragraphe (6): à l'instar d'autres banques de données, les informations sur les logs (qui a consulté, quand et pour quelle raison) sont gardées pendant un délai de 5 ans à partir de la date d'accès. Ce délai permet un contrôle d'abus éventuels en cas de plainte de personnes concernées.

Le délai de 5 ans correspond au délai de prescription de l'action publique en cas de délits.

Les informations collectées sur un abonné doivent par contre uniquement être gardées 3 ans à partir de la fin de la relation contractuelle.

Pour des enquêtes policières et judiciaires, il est important de garder des informations portant sur l'historique des changements des numéros d'appel. En effet, il est fréquent que des personnes mal intentionnées changent souvent de numéro d'appel afin de compliquer les recherches à leur encontre et de brouiller des pistes.

Ce délai de 3 ans semble raisonnable et proportionné compte tenu notamment du caractère peu sensible des données collectées. Ainsi il faut rappeler que la banque de données collecte des numéros d'appel et constitue ainsi une forme d'annuaire centralisé électronique.

La conservation pendant un certain temps de l'historique des numéros d'appel peut également jouer en faveur d'une personne innocente lorsqu'un contrat d'abonnement est résilié et le numéro est attribué dans la suite à une autre personne qui commet une infraction.

Enfin le paragraphe (8) prévoit des audits réguliers sur le fonctionnement du fichier pour contrôler la mise en oeuvre des mesures techniques et organisationnelles appropriées.

Amendement 4: article 3 nouveau du projet de loi

Cet article prévoit une disposition transitoire et énonce l'obligation pour les opérateurs de contribuer à la mise en place de ce fichier qui doit être mis en oeuvre 1 an après l'entrée en vigueur de la loi.

Amendement 5: modification de la loi de 2011

1) Il est proposé de compléter l'article 73 de la loi de 2011 afin de souligner dans la loi sur les communications électroniques l'obligation qui incombe aux opérateurs de relever les données qu'ils doivent fournir à la banque de données créée par l'article 10bis nouveau.
2) Article 83: cet ajout à l'article 83 est nécessaire afin de préciser que toute violation des obligations prévues à l'article 10 bis notamment de l'obligation de transmettre d'office et à titre gratuit à l'Institut des données à incorporer au fichier centralisé sera punie de la sanction prévue à l'article 83 précité.

*

FICHE FINANCIERE

Le projet de loi n° 6921 prévoit dans son article 2 tel qu'amendé l'ajout d'un article 10bis nouveau à la loi de 2005.

Cet article prévoit la création auprès de l'Institut luxembourgeois de régulation d'une banque de données qui centralise les données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.

Cette banque de données, tenue auprès de l'ILR, sera matériellement gérée par le CTIE ceci afin de mutualiser les infrastructures informatiques opérées par le CTIE ainsi que de profiter du cadre de sécurité du centre.

Cette banque de données devra être opérationnelle au moment de l'entrée en vigueur de la loi.

1) Le projet de loi n° 6921 a été préparé dans l'urgence après les attentats du 13 novembre 2015 de sorte qu'aucun poste en relation avec les changements proposés n'a encore été prévu à cet effet dans le numerus clausus.

Vu l'importance et la complexité de la création de ce système, il y a lieu d'octroyer un poste d'employé A1 supplémentaire au CTIE pour lancer les travaux visant la mise en place de cette banque de données.

2) La Police grand-ducale a signalé par ailleurs que l'intégration de la nouvelle banque de données dans leur application de gestion des appels de secours (JDI/ELS) impliquera des dépenses de l'ordre de 20.000 euros.

*

TEXTE COORDONNE

PROJET DE LOI

portant

1) modification du Code d'instruction criminelle,

2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques,

3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,

4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste

Art. 1er. Le Code d'instruction criminelle est modifié et complété comme suit:

1) L'article 24-1, paragraphe 1 est modifié comme suit:

„**Art. 24-1** (1) Pour tout délit, le procureur d'Etat peut requérir du juge d'instruction d'ordonner une perquisition, une saisie, l'audition d'un témoin ou une expertise sans qu'une instruction préparatoire ne soit ouverte.

Le procureur d'Etat peut procéder de même pour les infractions visées aux articles 196 et 197 du Code pénal pour ce qui concerne l'usage des faux visés à l'article 196, et pour les infractions visées aux articles 467, 468 et 469 du Code pénal.

Pour les infractions visées à l'alinéa qui précède, pour les crimes flagrants et pour les délits qui emportent une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, le procureur d'Etat peut requérir du juge d'instruction d'ordonner les mesures prévues aux paragraphes (1) et (2) de l'article 67-1 et sans qu'une instruction préparatoire ne soit ouverte.

La personne dont un moyen de télécommunication a fait l'objet de la mesure prévue au paragraphe (1) de l'article 67-1 est informée de la mesure ordonnée au cours même de l'enquête préliminaire et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance.

Lorsque les mesures de repérage de télécommunications ordonnées par le juge d'instruction n'ont donné aucun résultat, les données obtenues seront retirées du dossier de l'enquête préliminaire et détruites dans la mesure où elles concernent des personnes non visées par l'enquête préliminaire."

2) L'article 39, paragraphe 1 est modifié comme suit:

„**Art. 39.** (1) Si les nécessités de l'enquête l'exigent, l'officier de police judiciaire peut, avec l'autorisation du procureur d'Etat, retenir pendant un délai qui ne peut excéder vingt-quatre heures, les personnes contre lesquelles il existe des indices graves et concordants de culpabilité.

Le délai de vingt-quatre heures court à partir du moment où la personne est retenue en fait par la force publique.

Dans le cadre d'une enquête de flagrance portant en tout ou en partie sur un ou plusieurs des faits énumérés ci-après:

1. crimes et délits contre la sûreté de l'Etat au sens des articles 101 à 123 du Code pénal;
2. actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal;

le juge d'instruction, agissant sur réquisition du procureur d'Etat peut prendre une ordonnance visant à prolonger ce délai.

La privation de liberté qui. résulte de cette ordonnance ne peut, en aucun cas, excéder vingt-quatre heures, à compter de la notification de l'ordonnance. L'ordonnance est motivée et ne peut être prise qu'une seule fois. Elle mentionne les éléments qui justifient l'ouverture d'un nouveau délai, à savoir:

1° les indices graves de culpabilité relatifs à un crime ou à un délit;

2° les circonstances particulières de l'espèce.

Elle est notifiée à la personne retenue dans un délai de vingt-quatre heures. Celui-ci commence à courir à partir du moment où la personne est retenue en fait par la force publique. A défaut de signification régulière dans ce délai, la personne est libérée.

L'ordonnance de prolongation est communiquée immédiatement au procureur d'Etat. Elle n'est susceptible d'aucun recours.

Durant la nouvelle période de vingt-quatre heures, la personne a le droit de se concerter confidentiellement, pendant trente minutes, avec son avocat."

3) Il est ajouté au titre II du livre I du Code d'instruction criminelle après le chapitre X un chapitre XI nouveau, libellé comme suit:

„**Chapitre XI – *De l'enquête sous pseudonyme***

Art. 48-26. (1) Dans le but de constater les infractions énumérées ci-après au paragraphe (2) et, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers de police judiciaire agissant au cours de l'enquête de flagrance ou de l'enquête préliminaire peuvent, sans que ceci ne constitue une infraction au sens de l'article 231 du Code pénal, procéder aux actes suivants sans en être pénalement responsables:

1. participer sous un pseudonyme aux échanges électroniques;
2. être en contact, sous un pseudonyme, avec les personnes susceptibles d'être les auteurs de ces infractions;
3. extraire, acquérir ou conserver par ce moyèn les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions;
4. extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites.

A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions.

(2) L'enquête sous pseudonyme est susceptible d'être mise en oeuvre dans le but de la constatation des faits énumérés ci-après:

1. crimes et délits contre la sûreté de l'Etat au sens des articles 101 à 123 du Code pénal;
2. actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 136-6, 135-9 et 135-11 à 135-16 du Code pénal."

4) Il est ajouté au titre II du livre I du Code d'instruction criminelle, après le chapitre XI nouveau, un chapitre XII nouveau, libellé comme suit:

„**Chapitre XII – *De l'identification de l'utilisateur d'un moyen de télécommunication***

Art. 48-27. (1) Dans le cadre de l'enquête pour crime ou délit ou de l'instruction préparatoire, le procureur d'Etat ou le juge d'instruction peut, par une décision motivée et écrite, en requérant au besoin le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de télécommunications. procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients de l'opérateur ou sur base de l'article 10bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à:

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé;

2° l'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête ou d'instruction.

En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur d'Etat ou du juge d'instruction, et par une décision motivée et écrite requérir ces données. L'officier de police judiciaire communique cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur d'Etat ou au juge d'instruction et motive par ailleurs l'extrême urgence.

(2) Chaque opérateur de télécommunications et chaque fournisseur d'un service de télécommunications communique les informations qui ont été demandées dans les meilleurs délais.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, est punie d'une amende de 100 à 5.000 €."

5) L'article 65 est modifié comme suit:

„**Art. 65.** (1) Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets dont la découverte serait utile à la manifestation de la vérité.

(2) Le juge d'instruction en donne préalablement avis au procureur d'Etat.

(3) Sauf le cas d'infraction flagrante, celui de l'instruction préparatoire portant, en tout ou en partie, sur un ou plusieurs des faits énumérés ci-après:

1. crimes et délits contre la sûreté de l'Etat au sens des articles 101 à 123 du Code pénal;
2. actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal;

et les autres cas expressément prévus par la loi, les perquisitions ne peuvent, à peine de nullité, être commencées avant six heures et demie ni après vingt heures.

(4) Les dispositions des articles 33 à 38 sont applicables aux perquisitions effectuées par le juge d'instruction."

6) Les articles figurant sous la section VIII. „Des mesures spéciales de surveillance" du titre III du Livre I^{er} sont modifiés comme suit:

„**Art. 88-1.** (1) Le juge d'instruction peut, sous les conditions précisées ci-après, ordonner l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication.

Celle-ci s'effectue au moyen:

– de la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale,
– de la sonorisation de certains lieux ou véhicules, et
– de la captation de données informatiques.

(2) La sonorisation de certains lieux ou véhicules consiste dans la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement des paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics.

(3) La captation de données informatiques consiste dans la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels.

Art. 88-2. (1) Les mesures visées à l'article 88-1 ne peuvent être décidées par le juge d'instruction qu'à titre exceptionnel et par décision spécialement motivée d'après les éléments de l'espèce et par référence aux conditions indiquées au paragraphe (2).

(2) Elles sont subordonnées aux conditions:

a) que la poursuite pénale a pour objet, s'agissant de la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale, en tout ou en partie, un fait d'une gravité particulière emportant une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à deux ans d'emprisonnement, et, s'agissant de la sonorisation de certains lieux ou véhicules et de la captation de données informatiques, en tout ou en partie, un ou plusieurs des faits énumérés ci-après:

   1. crimes et délits contre la sûreté de l'Etat au sens des articles 101 à 123 du Code pénal;
   2. actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal;

b) que des faits déterminés rendent la personne à surveiller suspecte, soit d'avoir commis l'infraction ou d'y avoir participé, soit de recevoir ou de transmettre des informations destinées à l'inculpé ou au suspect ou qui proviennent de lui; et

c) que les moyens ordinaires d'investigation s'avèrent inopérants en raison de la nature des faits et des circonstances spéciales de l'espèce.

(3) Elles doivent être levées dès qu'elles ne sont plus nécessaires. Elles cessent de plein droit un mois à compter de la date de l'ordonnance. Elles peuvent toutefois être prorogées chaque fois pour un mois, sans que la durée totale puisse dépasser un an, par ordonnance motivée du juge d'instruction, approuvée par le président de la chambre du conseil de la cour d'appel qui statue dans les deux jours de la réception de l'ordonnance, le procureur général d'Etat entendu en ses conclusions.

(4) Elles ne peuvent être ordonnées à l'égard d'un inculpé après son premier interrogatoire par le juge d'instruction et celles ordonnées antérieurement cessent leurs effets de plein droit à cette date.

(5) Ces mesures ne peuvent être ordonnées à l'égard d'une personne liée par le secret professionnel au sens de l'article 458 du Code pénal, à moins qu'elle ne soit elle-même suspecte d'avoir commis l'infraction ou d'y avoir participé.

(6) Elles ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du juge d'instruction. Le fait qu'elles révèlent des infractions autres que celles visées dans ces décisions ne constitue pas une cause de nullité des procédures incidentes.

Art. 88-3. En vue de mettre en place le dispositif technique mentionné aux paragraphes (2) et (3) de l'article 88-1, le juge d'instruction peut, après approbation par le président de la chambre du conseil de la cour d'appel, autoriser l'introduction dans un véhicule ou un lieu privé qui n'est pas accessible au public, dans un domicile ou ses dépendances au sens des articles 479, 480 et 481 du Code pénal, y compris hors des heures prévues à l'article 65, paragraphe (3), le cas échéant à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur ceux-ci. Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous l'autorité et le contrôle du juge d'instruction. Les dispositions du présent alinéa sont également applicables aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place.

En vue de mettre en place le dispositif technique mentionné au paragraphe (3) de l'article 88-1, le juge d'instruction peut également, après approbation par le président de la chambre du conseil de la cour d'appel, autoriser la transmission de ce dispositif par un réseau de communications électroniques. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction. Le présent alinéa est également applicable aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place.

Art. 88-4. (1) Les décisions par lesquelles le juge d'instruction ou le président de la chambre du conseil de la cour d'appel ordonne la surveillance et le contrôle de télécommunications ainsi que de correspondances confiées à la poste sont notifiées aux opérateurs des postes et télécommunications qui font sans retard procéder à leur exécution. Ces décisions et les suites qui leur sont données sont inscrites sur un registre spécial tenu par chaque opérateur des postes et télécommunications.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, est punie d'une amende de 100 à 5.000 €.

(2) 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 sont remis sous scellés et contre récépissé au juge d'instruction qui dresse procès-verbal de leur remise. Il fait copier les correspondances pouvant servir à conviction ou à décharge et verse ces copies, les enregistrements ainsi que tous autres données et renseignements reçus au dossier. Il renvoie les écrits qu'il ne juge pas nécessaire de saisir aux opérateurs des postes qui les remettent sans délai au destinataire.

(3) Lorsque les mesures de surveillance et de contrôle des communications ordonnées sur la base de l'article 88-1 n'ont donné aucun résultat, les copies et les enregistrements ainsi que tous autres données et renseignements versés au dossier sont détruits par le juge d'instruction au plus tard douze mois après l'ordonnance de cessation des mesures de surveillance.

Dans le cas où le juge d'instruction estime que ces copies ou ces enregistrements ou les données ou renseignements reçus peuvent servir à la continuation de l'enquête, il ordonne leur maintien au dossier par une ordonnance motivée d'après les éléments de l'espèce.

Lorsqu'à la suite des mesures de surveillance et de contrôle des communications ordonnées sur la base de l'article 88-1, l'inculpé a fait l'objet d'une décision de non-lieu, d'acquittement ou de condamnation ayant acquis force de chose jugée, les copies et les enregistrements ainsi que tous autres données et renseignements sont détruits par le procureur général d'Etat ou le procureur d'Etat dans le mois qui suit la date où la décision judiciaire a acquis force de chose jugée.

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 peuvent être utilisées. Leur enregistrement et leur transcription sont immédiatement détruits par le juge d'instruction.

(4) La personne dont les communications ont été surveillées au sens de l'article 88-1, paragraphe (1), est informée de la mesure ordonnée au cours même de l'instruction et en tout cas au plus tard dans les douze mois qui suivent la cessation de la prédite mesure. Toutefois ce délai de 12 mois ne s'applique pas lorsque la mesure a été ordonnée dans une instruction pour des faits qui se situent dans le cadre ou en relation avec des crimes et délits contre la sûreté de l'Etat au sens des articles 101 à 123 du Code pénal, ou qui se situent dans le cadre ou en relation avec des actes de terrorisme et de financement du terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal.

La requête en nullité doit être produite sous peine de forclusion, dans les conditions prévues à l'article 126 du Code d'instruction criminelle.

(5) Après le premier interrogatoire, l'inculpé et son conseil peuvent prendre communication des télécommunications enregistrées, des correspondances et de tous autres données et renseignements versés au dossier.

L'inculpé et son conseil ont le droit de se faire reproduire les enregistrements en présence d'un officier de police judiciaire."

Art. 2. Il est ajouté un nouvel article 10*bis* à la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, libellé comme suit:

„**Art. 10*bis*. *Fichier centralisé auprès de l'Institut***

(1) Il est créé un fichier sous forme électronique auprès de l'Institut qui contient les données transmises conformément au paragraphe (2). Le fichier a pour finalité de mettre à la disposition des autorités et services énumérés au paragraphe (4) les données y figurant.

Le fichier est hébergé auprès du Centre des technologies de l'information de l'Etat qui en assure la gestion opérationnelle.

(2) Les entreprises notifiées auprès de l'Institut conformément à la loi du 27 février 2011 sur les réseaux et les services de communications électroniques qui fournissent un service de communica-

tions électroniques accessible au public en ayant recours à des ressources de numérotation luxembourgeois (ci-après: „les entreprises notifiées“) transmettent d'office et gratuitement à l'Institut par voie électronique et au moyen d'un interface sécurisé, les données suivantes:

a) Pour les personnes physiques: le nom, le prénom, le lieu de résidence habituelle, la date et le lieu de naissance ainsi que le numéro de contact de l'abonné,

   Pour les personnes morales: la dénomination ou raison sociale, l'adresse du lieu d'établissement ainsi que le numéro de contact;

b) le nom de l'entreprise notifiée, la nature du service fourni par celle-ci, le numéro d'appel alloué pour lequel le service en question a été souscrit et, si disponible, la date de la fin de la relation contractuelle ou en cas de prépaiement la date de désactivation du numéro d'appel.

   La liste du type de services visés au point b) est déterminée par règlement de l'Institut.

c) pour les personnes physiques, le type, le pays de délivrance et le numéro de la pièce d'identité ou de l'attestation de dépôt d'une demande de protection internationale de l'abonné en cas de service à prépaiement.

Ces données doivent être actualisées au moins une fois par jour, même en l'absence de changement.

Un rapport sur le transfert des données est généré automatiquement une fois par jour auprès du Centre des technologies de l'information de l'Etat.

Le protocole et l'interface sécurisés ainsi que le format d'échange à utiliser pour le transfert de ces données sont déterminés par règlement de l'Institut.

(3) Le non-respect du paragraphe (2) du présent article et du règlement de l'Institut pris en son exécution peut être sanctionné par l'Institut conformément à l'article 83 de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques.

(4) Le procureur d'Etat, le juge d'instruction et les officiers de police judiciaire visés à l'article 10 du Code d'instruction criminelle agissant dans le cadre de l'article 48-27 (7) du Code d'instruction criminelle, ainsi que le Service de renseignement de l'Etat accèdent de plein droit au fichier visé au paragraphe (1) du présent article. L'accès de plein droit se limite aux mesures prévues par l'article 48-27 du Code d'instruction criminelle et à celles prises dans le cadre de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Le central 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 aux seules données visées au paragraphe (2) a) du présent article. Cet accès se limite aux mesures particulières de secours d'urgence prestées dans le cadre des activités de le central 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 et s'effectue uniquement sur les communications entrantes.

Le motif de chaque consultation doit être enregistré au moment de l'accès.

Le Service de renseignement de l'Etat, le central 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 désignent chacun en ce qui le concerne les agents qui bénéficient d'un accès individuel.

(5) L'accès à distance aux données du fichier centralisé se fera par voie de requête électronique et sera sécurisé par un mécanisme d'authentification forte.

(6) Les informations relatives à la personne ayant procédé à la consultation, les informations consultées, les critères de recherche, la date et l'heure de la consultation, ainsi que le motif de la consultation sont enregistrés. Ces données sont effacées irrémédiablement et sans délai, cinq ans à compter de la date d'accès.

Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation.

(7) Les données visées au paragraphe (2) doivent être effacées irrémédiablement et sans délai trois ans à compter de la fin de la relation contractuelle ou, en cas de service à prépaiement, à compter de la date de désactivation du numéro d'appel.

(8) L'Institut fait procéder régulièrement à un audit sur le fonctionnement du fichier prévu au paragraphe (1) pour contrôler la mise en oeuvre des mesures techniques et organisationnelles appropriées.

Art. 3. Le fichier qui est prévu à l'article 2 de la présente loi doit être mis en oeuvre au plus tard un an après l'entrée en vigueur de la loi.

Les dispositions de l'article 10*bis* s'appliquent:

- aux contrats conclus après l'entrée en vigueur de la présente loi,
- aux contrats existants avant l'entrée en vigueur de la présente loi, dans la mesure où les données prévues en son paragraphe (2) avaient été collectées au moment de la conclusion du contrat, sans préjudice de l'obligation d'actualisation des données ultérieure prévue en son paragraphe (2) alinéa (2).

Art. 4. La loi du 27 février 2011 sur les réseaux et les services de communications électroniques est modifiée comme suit:

1) A l'article 73, il est rajouté un nouveau paragraphe 3 libellé comme suit:

„(3) L'entreprise fournissant les services de communications électroniques accessible au public en ayant recours à des ressources de numérotation doit relever les données suivantes auprès de l'utilisateur final:

– si l'utilisateur final est une personne physique, le nom, le prénom, le lieu de résidence habituelle, la date et le lieu de naissance de l'abonné;
– si l'utilisateur final est une personne morale, la dénomination ou raison sociale, l'adresse du lieu d'établissement."

2) A l'article 83, il est rajouté un nouveau paragraphe 1*bis* libellé comme suit:

„(1*bis*) Toute violation par une entreprise soumise à notification en vertu de l'article 8 paragraphe (1) de la présente loi, de l'obligation prévue à l'article 10*bis* de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, ainsi que de ses règlements d'exécution, peut être sanctionnée par l'Institut conformément au présent article".

Impression: CTIE – Division Imprimés et Fournitures de bureau