



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Projet de loi 6763

Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Date de dépôt : 07-01-2015

Date de l'avis du Conseil d'État : 13-07-2015

Auteur(s) : Monsieur Félix Braz, Ministre de la Justice

Liste des documents

Date	Description	Nom du document	Page
07-01-2015	Déposé	6763/00	<u>3</u>
24-02-2015	Avis de la Chambre de Commerce (13.2.2015)	6763/01	<u>10</u>
07-07-2015	Avis de la Commission nationale pour la Protection des données (19.6.2015)	6763/02	<u>13</u>
13-07-2015	Avis du Conseil d'État (10.7.2015)	6763/03	<u>18</u>
28-08-2015	1) Dépêche du Procureur Général d'Etat au Ministre de la Justice (28.7.2015) 2) Avis de la Cour Supérieure de Justice (19.2.2015) 3) Avis du cabinet d'instruction de Luxembourg (19.2.2015)<br/ [...]	6763/04	<u>26</u>
28-08-2015	Avis de la Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg (22.7.2015)	6763/05	<u>45</u>
30-10-2015	Avis de l'Ordre des Avocats du Barreau de Luxembourg (13.10.2015)	6763/06	<u>53</u>
06-04-2023	Arrêté Grand-Ducal de retrait du rôle des affaires de la Chambre des Députés (29.3.2023)	6763/07	<u>60</u>
09-03-2016	Commission juridique Procès verbal (18) de la reunion du 9 mars 2016	18	<u>63</u>
21-10-2015	Commission juridique Procès verbal (01) de la reunion JOINTE du 21 octobre 2015	01	<u>72</u>
21-10-2015	Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace Procès verbal (01) de la reunion JOINTE du 21 octobre 2015	01	<u>90</u>
11-02-2015	Commission juridique Procès verbal (14) de la reunion du 11 février 2015	14	<u>108</u>

6763/00

N° 6763**CHAMBRE DES DEPUTES**

Session ordinaire 2014-2015

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

*(Dépôt: le 7.1.2015)***SOMMAIRE:**

	<i>page</i>
1) Arrêté Grand-Ducal de dépôt (29.12.2014)	1
2) Texte du projet de loi	2
3) Exposé des motifs	4
4) Commentaire des articles	4

*

ARRETE GRAND-DUCAL DE DEPOT

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

Sur le rapport de Notre Ministre de la Justice et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.— Notre Ministre de la Justice est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Château de Berg, le 29 décembre 2014

Le Ministre de la Justice,
Félix BRAZ

HENRI

*

TEXTE DU PROJET DE LOI

Art. 1er. L'article 67-1 du Code d'instruction criminelle est modifié comme suit:

- 1) Au paragraphe 1, les termes „et si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement“ sont remplacés par les termes „et s'il est saisi pour une ou plusieurs des infractions prévues au paragraphe 4“.
- 2) Il est ajouté un paragraphe 4 nouveau libellé comme suit:

„(4) Les mesures prévues par le présent article peuvent être mises en oeuvre pour une ou plusieurs des infractions suivantes:

 - 1) crimes et délits contre la sûreté de l'Etat (art. 101 à 123 du Code pénal);
 - 2) participation à une organisation criminelle ou une association de malfaiteurs (art. 322 à 326 du Code pénal);
 - 3) terrorisme (art. 135-1 à 135-16 du Code pénal);
 - 4) traite des êtres humains, trafic de migrants, enlèvement de mineurs, attentats à la pudeur, viol, proxénétisme, exploitation sexuelle des enfants et pédopornographie (art. 368 à 385-2 du Code pénal);
 - 5) trafic de stupéfiants et de substances psychotropes (infractions prévues par la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie);
 - 6) trafic d'armes, de munitions et d'explosifs (infractions prévues par la loi modifiée du 15 mars 1983 sur les armes et munitions);
 - 7) corruption et trafic d'influence (art. 246 à 252 et 310 et 310-1 du Code pénal);
 - 8) fraudes et abus de confiance (art. 489 à 509 du Code pénal), y compris la fraude portant atteinte aux intérêts financiers des Communautés européennes au sens de la convention du 26 juillet 1995 relative à la protection des intérêts financiers des Communautés européennes;
 - 9) infractions relatives à l'industrie, au commerce et aux enchères publiques (art. 309 à 314-1 du Code pénal);
 - 10) infractions aux articles 220 et 231 de la loi générale sur les douanes et accises;
 - 11) infractions à l'article 32 de la loi du 9 mai 2006 relative aux abus de marché;
 - 12) blanchiment des produits du crime et recel (art. 505 à 506-8 et 508 et 509 du Code pénal);
 - 13) faux-monnayage et contrefaçon de monnaie (art. 162 à 192-2 du Code pénal);
 - 14) cybercriminalité et infractions en matière informatique (art. 509-1 à 509-7 du Code pénal);
 - 15) infractions à l'article 48 de la loi du 14 août 2000 relative au commerce électronique;
 - 16) infractions à l'article 11 de la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement de données à caractère personnel dans le secteur des communications électroniques;
 - 17) infractions contre l'environnement (article 64 de la loi modifiée du 19 janvier 2004 concernant la protection de la nature et des ressources naturelles, article 9 de la loi modifiée du 21 juin 1976 relative à la lutte contre la pollution de l'atmosphère, article 26 de la loi du 29 juillet 1993 concernant la protection et la gestion de l'eau et article 35 de la loi modifiée du 17 juin 1994 relative à la prévention et à la gestion des déchets);
 - 18) aide à l'entrée et au séjour irréguliers au sens de la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection et de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle;
 - 19) homicides et coups et blessures volontaires (art. 392 à 417 du Code pénal);
 - 20) trafic d'organes et de tissus humains (art. 18 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine et art. 32 de la loi du 1er août 2007 relative aux tissus et cellules humaines destinés à des applications humaines) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle;
 - 21) enlèvement, séquestration et prise d'otage (art. 434 à 442-1 du Code pénal);

- 22) harcèlement (art. 442-2 du Code pénal) et atteintes à la vie privée (articles 2 à 7 de la loi du 11 août 1982 concernant la protection de la vie privée);
- 23) racisme, révisionnisme, discrimination et xénophobie (art. 454 à 457-3 du Code pénal);
- 24) vol commis à l'aide de violences ou menaces et extorsion (art. 468 à 476 du Code pénal);
- 25) trafic illicite de biens culturels, y compris d'antiquités et d'oeuvres d'art (loi du 22 mai 2008 portant adaptation du droit interne aux dispositions du Deuxième Protocole relatif à la Convention de La Haye de 1954 pour la protection des biens culturels en cas de conflit armé, signé à La Haye le 26 mars 1999);
- 26) escroquerie (art. 496 à 501 du Code pénal);
- 27) contrefaçon (art. 179 à 191 du Code pénal);
- 28) falsification de documents administratifs et usage de faux (art. 193 à 212 du Code pénal);
- 29) trafic illicite de substances hormonales et d'autres facteurs de croissance (art. 14 de la loi modifiée du 4 août 1975 concernant la fabrication et l'importation des médicaments, art. 20 de la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments, art. 6 de la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments et art. 11 de la loi du 18 décembre 1985 relative aux médicaments vétérinaires, art. 14 à 18 de la loi modifiée du 31 juillet 1991 déterminant les conditions d'autorisation d'exercer la profession de pharmacien, art. 9 de la loi du 6 janvier 1995 relative à la distribution en gros des médicaments, art. 5 de la loi du 11 janvier 1989 réglant la commercialisation des substances chimiques à activité thérapeutique) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle;
- 30) trafic illicite de matières nucléaires et radioactives (art. 7 de la loi modifiée du 25 mars 1983 concernant la protection de la population contre les dangers résultant des radiations ionisantes et art. 12 de la loi du 10 août 1983 concernant l'utilisation médicale des rayonnements ionisants) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle;
- 31) vol commis sans violences ni menaces (art. 463 à 467 du Code pénal) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle;
- 32) incendie volontaire (art. 510 à 520 du Code pénal);
- 33) crimes relevant de la Cour pénale internationale (art. 136bis à 136quinquies du Code pénal).“

Art. 2. La loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques est modifiée comme suit:

- 1) A l'article 5 (1) (a), les termes „d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.“ sont remplacés par les termes „d'une des infractions prévues à l'article 67-1 (4) du Code d'instruction criminelle,“.
- 2) A l'article 5 (1), le point (b) est remplacé comme suit:
 - „(b)Après la période de conservation prévue au point (a), le fournisseur de services ou l'opérateur est obligé d'effacer irrémédiablement et sans délai les données relatives au trafic concernant les abonnés et les utilisateurs, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées.“.
- 3) A l'article 5 (6), les termes de „huit jours à un an“ sont remplacés par les termes de „six mois à deux ans“.
- 4) L'article 5-1 est remplacé comme suit:
 - „**Art. 5-1.** (1) Les données concernées par les articles 5 et 9 sont conservées sur le territoire de l'Union européenne.

(2) Ces données 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. Un règlement grand-ducal fixe des modalités d'exécution afin d'assurer la pleine intégrité et confidentialité de ces données.“

- 5) A l'article 9 (1) (a), les termes „d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement,“ sont remplacés par les termes „d'une des infractions prévues à l'article 67-1 (4) du Code d'instruction criminelle,“.

6) A l'article 9 (1), le point (b) est remplacé comme suit:

„(b)Après la période de conservation prévue au point (a), le fournisseur de services ou l'opérateur est obligé d'effacer irrémédiablement et sans délai les données de localisation autres que les données relatives au trafic concernant les abonnés et les utilisateurs, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées.“

7) A l'article 9 (6), les termes de „huit jours à un an“ sont remplacés par les termes de „six mois à deux ans“.

*

EXPOSE DES MOTIFS

Le présent projet de loi a comme objet d'adapter le dispositif légal relatif à la rétention des données de télécommunications à des fins de poursuites pénales aux exigences de l'arrêt rendu par la Cour de Justice de l'Union européenne en date du 8 avril 2014, dit „Digital Rights“ (affaires jointes C-293/12 et C-594/12), par lequel la Cour a invalidé la directive 2006/24/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves.

Etant donné que la directive 2006/24 a à l'époque été transposée par des modifications du Code d'instruction criminelle et 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 du 30 mai 2005“), il échet de modifier ces deux textes dans le sens préconisé par l'arrêt précité du 8 avril 2014.

*

COMMENTAIRE DES ARTICLES

Ad article 1er du projet de loi

Les points 1) et 2) de cet article, ensemble avec les dispositions de l'article 2 du projet de loi sous examen, visent à tenir compte, en ce qui concerne le Code d'instruction criminelle, des exigences formulées par l'arrêt rendu par la Cour de Justice de l'Union européenne en date du 8 avril 2014, dit „Digital Rights“ (affaires jointes C-293/12 et C-594/12), par lequel la Cour a invalidé la directive 2006/24/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves.

Le point 1) de l'article sous examen propose de remplacer à l'article 67-1 (1) du Code d'instruction criminelle le seuil de peine des infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs – actuellement toutes les infractions prévoyant une peine privative de liberté dont le maximum est égal ou supérieur à un an – par une liste précise et exhaustive d'infractions graves qu'il est proposé de faire figurer au paragraphe 4 nouveau de l'article 67-1.

Le point 2) de l'article sous examen propose d'ajouter à l'article 67-1 du Code d'instruction criminelle un paragraphe 4 nouveau qui énumère les catégories d'infractions pour lesquelles les autorités répressives peuvent avoir accès aux données de communication retenues. Cette liste s'inspire en principe de la liste des infractions prévues à l'annexe D de la directive 2014/41/Union européenne du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale alors que cette liste a été dressée pour une finalité qui s'apparente, dans le contexte de l'entraide pénale internationale, à celle du recours aux données de communication retenues par les opérateurs de télécommunications. Il est cependant proposé d'amender cette liste en la précisant par des renvois à des articles déterminés du Code pénal et de certaines lois spéciales afin de l'adapter aux spécificités du droit pénal luxembourgeois.

Ad article 2 du projet de loi

Le point 1) de cet article propose de modifier l'article 5 (1) (a) de la loi du 30 mai 2005 afin de l'adapter à la modification de l'article 67-1 du Code d'instruction criminelle au sein duquel le seuil de peine des infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs – actuellement toutes les infractions prévoyant une peine

privative de libellé dont le maximum est égal ou supérieur à un an – est remplacé par une liste précise d'infractions énumérées au paragraphe 4 nouveau de l'article 67-1 du Code d'instruction criminelle.

Le point 2) de l'article du projet de loi sous examen propose de modifier l'article 5 (1) (b) de la loi du 30 mai 2005 afin de préciser que les données retenues doivent être effacées irrémédiablement et sans délai à l'expiration du délai de rétention, dans le but de tenir compte notamment du paragraphe 67 de l'arrêt précité du 8 avril 2014 suivant lequel les données concernées devraient être définitivement et irrémédiablement détruites à l'issue de la période de rétention fixée. Il ne sera donc plus possible de les sauvegarder sous une forme anonymisée après la fin de la durée de rétention.

Le point 3) de cet article modifie le paragraphe 6 de l'article 5 de la loi du 30 mai 2005 en vue de relever les peines d'emprisonnement y prévues afin d'augmenter le caractère dissuasif de cette peine et de souligner ainsi l'importance accordée à la protection de ces données, et afin d'assurer qu'un mandat de dépôt prévu par l'article 94 du Code d'instruction criminelle peut être émis à l'égard des personnes suspectées d'avoir commis une infraction y relative.

Le point 4) de cet article vise à remplacer l'article 5-1 de la loi du 30 mai 2005.

Le paragraphe 1 nouveau de cet article vise à tenir compte notamment du paragraphe 68 de l'arrêt précité du 8 avril 2014 en obligeant dorénavant les opérateurs de télécommunications à conserver les données retenues sur le territoire de l'Union européenne afin d'assurer que les dispositions de protection des personnes à l'égard du traitement de ces données en vigueur au sein de l'Union européenne s'appliquent en tout état de cause à ces données.

Le paragraphe 2 nouveau vise à tenir compte notamment des paragraphes 66 et 67 de l'arrêt précité du 8 avril 2014 en prévoyant qu'un règlement grand-ducal déterminera des dispositions d'exécution plus détaillées afin d'assurer au maximum la pleine intégrité et la confidentialité de ces données. Au vu du caractère inévitablement très détaillé et technique de ces dispositions, il a paru inopportun de les faire figurer au sein d'une loi, ceci d'autant plus qu'il faut s'attendre à ce que ces dispositions doivent être adaptées régulièrement et rapidement afin de suivre les évolutions techniques en la matière. A noter que le paragraphe 2 du texte actuel de l'article 5-1 a été repris aux points (b) des articles 5 (1) et 9 (1) de la loi du 30 mai 2005.

Le point 5) de cet article propose d'adapter l'article 9 (1) (a) de la loi du 30 mai 2005 pour les mêmes raisons que le point 1) de l'article sous examen propose de modifier l'article 5 (1) (a) de cette loi. Cette double modification s'impose en effet alors que l'article 5 de la loi du 30 mai 2005 traite des données relatives au trafic de télécommunications, tandis que l'article 9 de cette loi traite des données de localisation autres que les données relatives au trafic.

Le point 6) de cet article du projet de loi propose d'adapter l'article 9 (1) (b) de la loi du 30 mai 2005 pour les mêmes raisons que le point 2) de l'article du projet de loi sous examen propose de modifier l'article 5 (1) (b) de cette loi.

Le point 7) propose de modifier le paragraphe 6 de l'article 9 pour les mêmes raisons que le point 3) de l'article 2 du projet de loi sous examen propose de modifier le paragraphe 6 de l'article 5 de la loi du 30 mai 2005.

CTIE – Division Imprimés et Fournitures de bureau

6763/01

N° 6763¹

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

AVIS DE LA CHAMBRE DE COMMERCE

(13.2.2015)

Le projet de loi sous avis a pour objet d'adapter le dispositif légal national relatif à la rétention des données de télécommunications à des fins de poursuites pénales suite à un arrêt récent rendu par la Cour de Justice de l'Union européenne (ci-après la „CJUE“).

En effet, la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications (ci-après la „Directive 2006/24/CE“), avait pour objectif d'harmoniser les dispositions nationales relatives aux obligations des fournisseurs de services de télécommunications électroniques en vue de garantir la disponibilité de leurs données à des fins de recherche, de détection et de poursuite d'infractions graves telles que définies au niveau national par chaque Etat membre.

La Directive 2006/24/CE obligeait ainsi les Etats membres à prévoir pour les fournisseurs de services de télécommunications électroniques une obligation de conservation des données de trafic et de localisation en vue de garantir leur disponibilité pour la recherche et la constatation d'infractions graves, tout en laissant aux Etats membres la compétence de définir ces infractions. La Directive 2006/24/CE harmonisait également les catégories de données à conserver et prévoyait une durée de conservation de ces données comprise entre 6 et 24 mois.

La Directive 2006/24/CE fut transposée au Luxembourg par des modifications des dispositions du Code d'instruction criminelle (ci-après le „CIC“) et 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“).

Or, la CJUE a, par un arrêt du 8 avril 2014¹, déclaré la Directive 2006/24/CE invalide aux motifs qu'elle porterait une atteinte excessive à la vie privée des utilisateurs des services de communications électroniques et qu'elle serait contraire à la Charte des droits fondamentaux de l'Union européenne.

La CJUE fonde notamment sa décision sur le fait que:

- l'obligation de conservation des données s'applique de manière générale sans exiger le moindre lien, même indirect, entre la personne dont les données sont conservées et un risque d'infraction,
- la Directive 2006/24/CE n'établit aucun lien entre la durée de conservation des données et la nature de l'infraction,
- la Directive 2006/24/CE ne fixe aucune limitation à l'utilisation des données conservées ni aucun critère objectif concernant leur accès,
- la durée maximale de conservation des données, pouvant aller jusqu'à deux ans, est disproportionnée,
- la Directive 2006/24/CE n'impose pas le stockage de ces données au sein de l'Union européenne.

¹ CJUE 8.4.2014, „Digital Rights“, affaires jointes C-293/12 et C-594/12.

Tirant les conséquences de l'invalidation de la Directive 2006/24/CE sur notre législation nationale, les auteurs du projet de loi sous avis entendent adapter les dispositions du Code d'instruction criminelle et de la Loi modifiée du 30 mai 2005 aux griefs formulés par la CJUE, ce dont la Chambre de Commerce se félicite.

Ainsi, alors qu'actuellement, l'article 67-1 CIC autorise le juge d'instruction à demander le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications lorsque les faits présumés emportent une peine criminelle ou correctionnelle dont le maximum est égal ou supérieur à un an, l'article 1er du projet de loi sous avis entend désormais limiter cette possibilité à une liste précise et exhaustive d'infractions graves.

En outre, l'article 2 du présent projet de loi modifie notamment l'article 5 (1) (b) de la Loi du 30 mai 2005 afin de préciser que les données retenues devront être effacées irrémédiablement et sans délai après l'expiration du délai de rétention, ce délai demeurant fixé à six mois².

Ces données devront également être désormais conservées sur le territoire de l'Union européenne afin de s'assurer que les dispositions communautaires relatives à la protection des personnes à l'égard du traitement de leurs données à caractère personnel s'appliquent en tout état de cause.

Les peines encourues en cas de non-respect des dispositions de la Loi du 30 mai 2005 se voient également relevées d'un emprisonnement de 8 jours à un an à un emprisonnement de 6 mois à deux ans afin d'augmenter leur caractère dissuasif et de souligner l'importance accordée à la protection des données personnelles.

Finalement un règlement grand-ducal déterminera les modalités d'exécution afin d'assurer la pleine intégrité et la confidentialité des données.

La Chambre de Commerce n'a pas d'observations particulières à formuler et s'en tient à l'exposé des motifs qui explique clairement le cadre et les objectifs du présent projet de loi.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous avis.

² Article 5 (1) (a) de la Loi du 30 mai 2005.

6763/02

N° 6763²

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI**portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques**

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(19.6.2015)

Conformément à l'article 32 paragraphe (3) lettres (e) et (f) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée „la loi du 2 août 2002“), la Commission nationale pour la protection des données a notamment pour mission de présenter au gouvernement toutes suggestions susceptibles d'améliorer le cadre légal et d'aviser „tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi“.

Par lettre du 5 janvier 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Dans son avis n° 214/2014 du 13 mai 2014¹, la Commission nationale avait analysé la législation luxembourgeoise existante au regard de l'arrêt de la Cour de justice de l'Union européenne rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12. Dans ledit avis, la CNPD avait attiré l'attention sur plusieurs points de la législation qui devraient faire l'objet de modifications suite à l'arrêt précité.

Ci-dessous seront passés en revus les sujets évoqués dans l'avis précité à la lumière des dispositions afférentes du projet de loi sous avis.

1) Défaut d'exceptions pour les personnes dont les communications sont soumises au secret professionnel

Dans le considérant (58) de son arrêt du 8 avril 2014, la Cour de justice de l'Union européenne a relevé le fait que la directive 2006/24/CE „ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel“.

Le projet de loi sous avis n'introduit aucune exception pour ce qui est des communications soumises au secret professionnel, ni au niveau de la conservation elle-même (articles 5 et 9 de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement

¹ Avis de la Commission nationale pour la protection des données quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication

des données dans le secteur des communications électroniques), ni au niveau de l'accès aux données (article 67-1 du Code d'instruction criminelle).

Dans son avis n° 214/2014 du 13 mai 2014, la CNPD avait suggéré d'aligner le régime de l'accès aux données issues de la conservation à celui existant en matière d'écoutes téléphoniques pour ce qui est des aménagements en matière de communications couvertes par le secret professionnel, en estimant que „*cette voie [...] reviendrait à réduire de façon équivalente les conséquences pour la vie privée résultant de l'ingérence dans le secret de leurs communications électroniques des personnes visées par la CJUE au regard de la protection spéciale dont ils bénéficient dans les activités considérées.*“ Par ailleurs, elle avait plaidé pour une exception en faveur des journalistes.

La CNPD réitère dès lors sa proposition et estime nécessaire d'introduire ces exceptions dans le projet de loi conformément à l'arrêt de la CJUE.

Si une telle exception est prévue au niveau de l'accès aux données, la disposition y afférente devrait être insérée, outre à l'article 67-1 du Code d'instruction criminelle, également le cas échéant à l'article 24-1 alinéa 3 du Code d'instruction criminelle et à l'article 10 paragraphe (2) du *projet de loi n° 6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat, la loi du 31 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, le Code d'Instruction criminelle, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, et la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Ledit projet de loi a été déposé à la Chambre des Députés comme projet de loi n° 6675 en date du 2 avril 2014.*

2) Durée de conservation et obligation de destruction à l'expiration de la durée de conservation légale

Dans son avis n° 214/2014, la CNPD a rendu attentif au fait que l'arrêt de la CJUE mentionne l'exigence que la législation impose la destruction irrémédiable des données à caractère personnel à la fin de la période de conservation obligatoire.

La Commission nationale salue la nouvelle formulation de l'article 5 paragraphe 1er lettre (b) et de l'article 9 paragraphe 1er lettre (b), articles qui prescrivent désormais, sans équivoque possible, la destruction des données, une fois la fin de la durée de conservation de 6 mois atteinte.

Pour ce qui est de la durée de conservation elle-même, la démarche du législateur luxembourgeois était exemplaire dans la mesure où, en 2010, la durée de conservation a été réduite à la durée minimale prévue par la directive 2006/24/CE, à savoir 6 mois. Cependant ladite directive ayant été déclarée invalide, il se pose désormais la question de savoir si une durée de conservation encore plus courte ne pourrait pas être envisagée, par exemple à l'instar des propositions actuelles du gouvernement allemand en la matière.

3) Obligation de conserver les données sur le territoire de l'Union européenne

Dans son avis n° 214/2014, en se référant à l'arrêt de la Cour, la CNPD avait plaidé pour l'obligation de conserver les données sur le territoire de l'Union européenne en raison de „*la nécessité de voir soumettre le traitement et la conservation de ces vastes quantités de données sensibles par une autorité de contrôle indépendante mettant en oeuvre le droit européen de protection des libertés et droits fondamentaux*“.

La Commission nationale note avec satisfaction que l'article 5-1 de la loi modifiée du 30 mai 2005 impose désormais que les données soient conservées sur le territoire de l'Union européenne.

4) Mesures techniques et d'organisation destinées à assurer la confidentialité et la sécurité des données conservées

Dans ses avis n° 85/2010 du 26 avril 2010² et n° 214/2014 du 13 mai 2014, la CNPD avait suggéré de prévoir des mesures spécifiques en matière de sécurité des données pour la conservation des données de télécommunications. Comme l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014, le simple renvoi aux règles générales applicables en matière de sécurité des données „*ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles*“ (considérant 67).

Le projet de loi sous avis prévoit la fixation des règles en question par voie de règlement grand-ducal.

Selon l'arrêt susmentionné, une directive européenne, en l'espèce la directive 2006/24/CE, qui prescrit la conservation des données de télécommunication sans mesures de sécurité adaptées, viole le droit communautaire, et plus précisément les articles 7, 8 et 52 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne.

En toute logique, une loi nationale légiférant dans le champ d'application du droit de l'Union européenne³ qui prescrit le même type de rétention des données sans prévoir les mesures de sécurité adéquates devrait tout autant violer la Charte.

Par ailleurs, l'article 11 paragraphe (3) de la Constitution dispose ce qui suit: „*L'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi*“. Selon la jurisprudence constante de la Cour constitutionnelle, „*dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc*“⁴. L'article 5-1 paragraphe (2) projeté de la loi modifiée du 30 mai 2005 ne saurait guère satisfaire à cette exigence.

Dans ces circonstances, la CNPD estime que les dispositions essentielles en matière de sécurité doivent être comprises dans la loi.

Dans l'hypothèse où l'article 5-1 paragraphe (2) projeté était maintenu en ses termes actuels, la CNPD aurait préféré qu'un projet de règlement grand-ducal aurait été soumis pour avis ensemble avec le projet de loi.

5) Sanction des abus

La Commission nationale note avec satisfaction que les sanctions en matière d'abus prévues par les articles 5 paragraphe (6) et 9 paragraphe (6) ont été alourdies.

En revanche, la CNPD regrette que, contrairement à ce qu'elle avait suggéré dans ses avis n° 85/2010 du 26 avril 2010 et n° 214/2014 du 13 mai 2014, le projet de loi ne prévoit pas la nullité de la preuve obtenue moyennant une violation de la législation sur la rétention des données de télécommunication et réitère sa recommandation d'„*inscrire en outre expressément dans le Code d'instruction criminelle la nullité de la preuve obtenue moyennant un accès illicite ou un abus des données en question*“.

6) Les infractions visées

Conformément aux recommandations de la CNPD exprimées dans ses avis n° 85/2010 du 26 avril 2010 et n° 214/2014 du 13 mai 2014, le projet de loi prévoit une liste limitative d'infractions qui permettent un accès aux données par les autorités.

2 Avis de la Commission nationale pour la protection des données concernant le projet de loi n° 6113 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 et le projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics

3 Plus précisément dans le champ d'application de l'article 15 paragraphe (1) de la *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*

4 Arrêt 117 de la Cour constitutionnelle

Selon le commentaire des articles, le catalogue des infractions s'inspire en principe de la liste des infractions prévues à l'annexe D de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale. Vu la difficulté de l'exercice de l'établissement d'une telle liste, il est compréhensible que l'on s'inspire d'une liste existante en droit européen. Il se pose cependant la question de savoir si l'amélioration de la lutte contre la criminalité grave, but recherché lors de la mise en place de la conservation des données par la directive 2006/24/CE (certes invalidée par la CJUE), et la coopération judiciaire en matière pénale traitée par la directive 2014/41/UE sont censées concerner les mêmes infractions.

Par ailleurs, selon le même commentaire d'articles, cette liste est amendée en la précisant par des renvois à des articles déterminés du Code pénal et de certaines lois spéciales afin de l'adapter aux spécificités du droit pénal luxembourgeois.

La rétention des données de télécommunication avait été rendue obligatoire par la directive 2006/24/CE en réaction aux attentats terroristes et pour pouvoir prévenir et sanctionner de tels attentats à l'avenir⁵, mais son champ d'application avait été étendu à la criminalité grave de manière générale.

On peut se demander si, effectivement, toutes les infractions énumérées au projet sous avis relèvent de la criminalité grave et si certaines d'entre elles ne s'éloignent pas des actes initialement visées par l'esprit de la directive déclarée invalide. Les mesures de conservation de données prévues constituant une limitation à l'exercice de droits fondamentaux, leur champ d'application devrait être défini de manière aussi limitative que possible.

Enfin, la CNPD suggère d'insérer, à l'article 24-1 alinéa 3 du Code d'instruction criminelle, qui permet un recours aux données de télécommunication en dehors d'une instruction préparatoire, un renvoi vers la liste des infractions de l'article 67-1.

Ainsi décidé à Esch-sur-Alzette en date du 19 juin 2015.

La Commission nationale pour la protection des données

Tine A. LARSEN
Présidente

Thierry LALLEMANG
Membre effectif

Georges WANTZ
Membre effectif

⁵ Cf. considérants 8 et 10 du préambule de la directive 2006/24/CE

6763/03

N° 6763³

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

AVIS DU CONSEIL D'ÉTAT

(10.7.2015)

Par dépêche du 7 janvier 2015, le Premier ministre, ministre d'État, a soumis à l'avis du Conseil d'État le projet de loi sous rubrique élaboré par le ministre de la Justice.

Au texte du projet de loi étaient joints un exposé des motifs, un commentaire des articles, une fiche d'évaluation d'impact et une fiche financière.

Les avis de la Chambre de commerce et de la Commission nationale pour la protection des données (CNPD) ont été communiqués au Conseil d'État par dépêches respectivement des 20 février 2015 et 6 juillet 2015.

*

CONSIDÉRATIONS GÉNÉRALES

Il découle de l'exposé des motifs du projet de loi sous examen qu'il a „pour objet d'adapter le dispositif légal relatif à la rétention des données de télécommunications à des fins de poursuites aux exigences de l'arrêt rendu par la Cour de Justice de l'Union européenne en date du 8 avril 2014, dit „Digital Rights“ (affaires jointes C-293/12 et C-594/12)“, par lequel cette cour a invalidé la directive 2006/24/CE du 15 mars 2006 du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

Pour ce faire, le projet se propose de reformuler en tout ou en partie tant l'article 67-1 du Code d'instruction criminelle que les articles 5, 5-1 et 9 de 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 télécommunications et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle, et qui avait à l'époque opéré transposition en droit national de la directive annulée.

L'arrêt du 8 avril 2014 de la Cour de justice de l'Union européenne „Digital Rights“ a, en résumé et pour l'essentiel, reconnu que si, certes, la directive visée au recours porté devant elle poursuivait un objectif d'intérêt général¹ et que la conservation des données de communication pouvait être considérée comme apte à réaliser l'objectif poursuivi par ladite directive², elle ne remplissait pas le caractère de proportionnalité imposant que l'atteinte à la vie privée que comporte, le cas échéant, une réglementation européenne pour être conforme aux principes établis par la Charte des droits fondamentaux de l'Union européenne, soit limitée au strict nécessaire³. En outre la Cour de justice de l'Union européenne reproche à la même directive d'avoir négligé de prévoir un critère objectif permettant de délimiter

1 point 44 de l'arrêt visé au texte;

2 *ibid.*, point 49;

3 *ibid.*, points 52 à 59;

l'accès des autorités nationales compétentes aux données retenues⁴. Enfin, la Cour critique la directive sur ses indications relatives à la durée de la rétention⁵, et sur ses dispositions relatives à la sécurité, la protection ainsi que l'effacement des données à la fin de leur période de sauvegarde⁶.

Si l'annulation de la directive 2006/24/CE n'entraîne pas *ipso jure* la caducité des législations nationales de transposition, les vices qui ont amené la Cour de justice de l'Union européenne à sa décision sont cependant partagés par ces législations pour autant qu'elles ont suivi la directive et l'exposent dès lors au reproche de la violation des mêmes droits fondamentaux que ceux visés à l'arrêt en question.

Il en a ainsi été récemment en Belgique, où, par un arrêt de la Cour constitutionnelle n° 84/2015 rendu le 11 juin 2015, la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et l'article 90decies du Code d'instruction criminelle, a été annulée dans son ensemble „par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive „conservation des données“ invalide pour avoir „excédé les limites qu'impose le respect du principe de proportionnalité“ au regard de la Charte des droits fondamentaux de l'Union européenne“⁷.

Le Conseil d'État approuve dès lors l'initiative du législateur de vouloir se conformer aux voies proposées par le juge de l'Union européenne, ce qui non seulement est dans l'intérêt de la protection des libertés individuelles, mais encore évite à des dossiers pénaux basés sur des données de communication conservées de se heurter à des écueils de procédure qui seraient de nature à entraîner des incertitudes juridiques majeures.

*

EXAMEN DES ARTICLES

Observation préliminaire

Contrairement à la démarche retenue dans le cadre 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 criminelle⁸, les auteurs du projet de loi entendent, dans l'article 1^{er} du projet de loi, modifier le Code d'instruction criminelle pour ensuite, dans son article 2, modifier la loi précitée du 30 mai 2005. Or, l'article 67-1 du Code d'instruction criminelle ne fait que poser les conditions d'accès aux données que les fournisseurs et opérateurs sont obligés de retenir en vertu de la loi du 30 mai 2005. Le Conseil d'État propose dès lors d'intervertir les articles du projet, l'article 1^{er} devenant l'article 2 et l'article 2 devenant l'article 1^{er}.

Article 1^{er} (2 selon le Conseil d'État)

Le commentaire des articles renseigne sur l'intention des auteurs du projet de loi, qui est de „tenir compte (...) des exigences formulées par l'arrêt „Digital Rights“ en remplaçant à l'article 67-1 du Code d'instruction criminelle la mention d'un seuil de peine déterminant les infractions pour lesquelles les autorités judiciaires⁹ peuvent accéder les données de communication retenues par les fournisseurs et opérateurs, par une liste d'infractions considérées comme infractions graves.“ La liste en question fait l'objet du nouveau paragraphe 4 dudit article 67-1 du Code d'instruction criminelle.

Cette modification tend dès lors à rencontrer le reproche du juge de l'Union européenne adressé à la directive annulée, consistant en ce que „la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et de leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions

4 *ibid.*, points 60 à 62;

5 *ibid.*, points 62 et 64;

6 *ibid.*, points 65 à 68;

7 point B.11.1 de la décision 84/2015;

8 Mém. A. 122 du 29 juillet 2010, p. 2060;

9 Le commentaire des articles parle d'ailleurs, à tort, d'autorités répressives, alors que seul le juge d'instruction, autorité judiciaire, peut avoir recours à cet instrument;

*pouvant (...) être considérées comme suffisamment graves pour justifier*¹⁰ une ingérence dans les droits fondamentaux.

La Cour de justice de l'Union européenne retient à ce propos à l'encontre de la directive, outre le défaut d'indications quant aux règles procédurales d'accès, deux points de critique distincts: le défaut de précision suffisante quant aux infractions pouvant justifier un accès aux données retenues, d'une part, et le défaut de limitations quant au nombre de personnes pouvant effectuer un accès aux dites données, d'autre part.

Le Conseil d'État note que les auteurs du projet n'entendent pas revenir sur le principe que, dans le cadre de poursuites pénales, seul le juge d'instruction, régulièrement saisi par le ministère public, peut accéder aux données retenues par les fournisseurs et opérateurs. Cette solution, retenue dès l'insertion de l'article 67-1 au Code d'instruction criminelle par la loi du 21 novembre 2002¹¹, est de nature à répondre – pour ce qui est de la transposition en droit national de la directive annulée – aux critiques formulées au regard des limitations des accès aux données retenues étant donné que l'ordonnance rendue par le juge d'instruction est susceptible de recours juridictionnels au vu de l'article 67-1, paragraphe 3, du Code d'instruction criminelle.

La loi nationale prévoit ainsi des règles procédurales précises déterminant tant les accès que les recours contre ceux-ci. De même, le cercle des personnes pouvant recourir à cette mesure est déterminé par les dispositions sur l'organisation judiciaire, et est dès lors non seulement restreint, mais encore fermé.

Les auteurs du projet de loi proposent, pour répondre au reproche formulé relativement aux infractions pouvant justifier un accès, de recourir à une liste d'infractions considérées comme graves.

Le Conseil d'État rappelle que, dans le cadre du projet de loi n° 6113, qui devait devenir la loi précitée du 24 juillet 2010, la question de l'insertion d'une liste au lieu d'un seuil de peine avait déjà fait l'objet de débats. Ainsi, on peut lire dans le rapport de la Commission parlementaire de l'enseignement supérieur, de la recherche, des médias et des communications¹² que *„quant à une liste des peines, telle que favorisée par exemple par la Commission nationale pour la protection des données et la Commission consultative des droits de l'homme dans leurs avis respectifs, les auteurs du projet de loi estiment que la détermination des infractions à retenir aurait été d'une complexité et d'une envergure énorme. Retenir uniquement les infractions d'actes de terrorisme et de criminalité organisée serait un manquement grave dans le cadre de la lutte contre cette sorte d'infractions, puisque les infractions primaires ne seraient plus prises en considération. Selon les auteurs du projet de loi, le seuil de peine d'un an représente un compromis entre, d'une part, la recherche de l'efficacité du système, militant plutôt pour un seuil de peine relativement bas, et, d'autre part, la protection de la vie privée et des droits fondamentaux des citoyens, qui exigerait un seuil de peine plus élevé.“*.

Le Conseil d'État avait à l'époque exprimé sa préférence pour un seuil de peine¹³, sans entrer plus amplement dans le débat entre les défenseurs d'un système de liste et les auteurs du projet de loi en question.

La directive 2006/24/CE, en son article 4, avait laissé le choix aux États membres de déterminer selon leur droit national notamment *„les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité“*. Elle a été censurée sur ce point entre autres pour ne pas disposer *„expressément que [l'] accès et l'utilisation [...] doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci“*¹⁴.

Le Conseil d'État n'en déduit pas la nécessité absolue pour le législateur national de devoir revenir sur sa décision initiale de procéder à une limitation par le recours à un seuil de peine. Tout au plus, mais il s'agit là d'un choix politique qui ne convient pas au Conseil d'État, pourrait-on vérifier si le seuil actuel d'un an¹⁵ doit être maintenu, ou bien s'il doit être porté à un niveau plus élevé, ainsi que cela avait été notamment discuté dans le cadre de la loi précitée du 24 juillet 2010.

10 Arrêt „Digital Rights“, point 60;

11 Loi du 21 novembre 2002, Mém. A 2002, n° 132, p. 3052;

12 Doc. parl. 6113¹⁰, précité, p. 6;

13 Doc. parl. 4889/4886¹, p. 4, et 6113³, p. 2;

14 Point 61 de la décision „Digital Rights“;

15 À noter que le seuil avait initialement été fixé à six mois (loi du 21 novembre 2002);

Si toutefois le recours à une liste devait être maintenu, le Conseil d'État s'interroge sur la nécessité de créer une nouvelle liste, qui viendrait s'ajouter à celles figurant déjà actuellement aux différents codes, à l'exemple de l'article 506-1 du Code pénal et des articles 66-2 et 66-3 du Code d'instruction criminelle, au risque de créer des confusions au niveau des praticiens du droit appelés, d'un côté de la barre ou de l'autre, à appliquer ces textes. Ne serait-il pas plus judicieux de recourir à une liste déjà existante, et notamment à celle figurant à l'article 506-1 du Code pénal, qui a le mérite, non seulement, de correspondre aux directives européennes édictées en matière de blanchiment de fonds provenant d'infractions criminelles, qui retiennent également le critère de crime grave, mais encore, d'être bien connue des praticiens du droit.

À tout le moins, si les auteurs du projet entendent maintenir la liste actuellement proposée, le Conseil d'État estime qu'il serait indiqué, afin d'éviter que la liste ne se révèle incomplète pour ce qui des infractions qualifiées de crime, d'en retirer tous les crimes spécifiquement mentionnés et de remplacer ces mentions individuelles par la mention générique de „*toutes les infractions qualifiées de crime par la loi*“ pour ne maintenir pour le surplus dans la liste que les infractions qualifiées de délit que les auteurs jugeront opportun d'y insérer. Le Conseil d'État relève à cet égard que la liste ne contient notamment pas l'infraction de blanchiment de fonds provenant du trafic de stupéfiants, étant donné que le point 5) du nouveau paragraphe (4) ne vise que le „trafic de stupéfiants (...)“, sans parler des produits de ce trafic. Or, l'article 506-1 du Code pénal ne vise pas ces produits, de telle sorte que l'article 67-1 du Code d'instruction criminelle risque de ne pas s'appliquer à cette infraction en vertu du principe de l'interprétation stricte des lois pénales.

Il y a en tout état de cause lieu, afin de respecter les critères de précision et de prévisibilité requis pour toute loi pénale, de remplacer les références à des infractions, voire à des groupes d'infractions, génériques par des références à des articles précis du Code pénal, ou à des lois spéciales, ainsi que cela est déjà pratiqué à l'article 506-1 du Code pénal. Cet exercice pourrait être mis à profit pour énumérer les infractions en question dans un ordre logique suivant, pour celles tirées du Code pénal, une suite numérique et, pour celles tirées des lois spéciales, une suite chronologique.

Le Conseil d'État tient cependant à attirer l'attention des auteurs du projet de loi sur ce que ledit projet ne répond pas à une des questions fondamentales soulevées par l'arrêt „*Digital Rights*“, à savoir la protection des données de personnes soumises à un régime de protection spécial en raison de leur secret professionnel¹⁶, et qui a été discuté dans le cadre de l'arrêt précité de la Cour constitutionnelle belge. Dans leur requête introductive, l'Ordre des barreaux francophones et germanophone, les associations sans but lucratif „*Liga voor Mensenrechten*“ et „*Ligue des Droits de l'Homme*“ ont en effet reproché à la loi belge „*de traiter de manière identique les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, dont notamment les avocats, et les autres utilisateurs de ces services sans tenir compte du statut particulier de l'avocat, du caractère fondamental du secret professionnel auquel il est soumis et de la nécessaire relation de confiance qui doit l'unir à son client*“¹⁷.

L'article 67-1 du Code d'instruction criminelle actuel est muet sur ce point, et il ne semble pas que la problématique ait fait l'objet de décisions des tribunaux luxembourgeois à ce jour. Mais il n'en est pas moins vrai que le problème est réel et que le projet sous examen, qui, justement, entend adapter le droit luxembourgeois aux exigences formulées par la Cour de justice de l'Union européenne, devrait également en tenir compte.

Le Conseil d'État propose par conséquent d'insérer entre l'actuel paragraphe 3 de l'article 67-1 du Code d'instruction criminelle et le paragraphe 4 projeté, qui deviendrait alors le paragraphe 5, un paragraphe 4 s'inspirant du paragraphe 4 de l'article 88-1 du Code d'instruction criminelle, libellé comme suit:

„(4) Les mesures visées à l'alinéa (1) 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.“

Dans son avis, la CNPD suggère également l'inclusion à l'article 67-1 du Code d'instruction criminelle d'une disposition analogue à celle reprise ci-dessus, mais estime nécessaire de modifier encore dans le même sens l'article 24-1, alinéa 3, du Code d'instruction criminelle. Le Conseil d'État estime

¹⁶ Arrêt „*Digital Rights*“, point 58;

¹⁷ Arrêt 84/2015, précité, point B.2.2.;

une telle modification superfétatoire, étant donné que, en effectuant un renvoi vers l'article 67-1 du Code d'instruction criminelle, l'article 24-1 du même code vise à l'évidence l'ensemble de cette disposition, donc y compris les limites que le Conseil d'État propose d'y ajouter.

Article 2 (1^{er} selon le Conseil d'État)

Point 1)

Aux termes de l'exposé des motifs, la modification proposée à l'article 5, paragraphe 1^{er}, point a), de la loi précitée du 30 mai 2005 réglant la rétention des données relatives au trafic des télécommunications, tend à mettre la disposition y visée, qui indique la finalité pour laquelle les données sont retenues par les fournisseurs et opérateurs, en conformité avec la modification proposée à l'article 67-1 du Code d'instruction criminelle.

Si le Conseil d'État n'a pas d'observation particulière à formuler pour ce qui est de la modification proposée, il tient cependant à rappeler que dans son avis précité relatif au projet de loi n° 6113, il avait souligné que, „comme les fournisseurs et opérateurs devront de toute façon tout conserver, ne sachant a priori ni aux fins de recherche de quelle infraction serviront les données ni quelle donnée sera utile à cette fin“¹⁸, il y aurait lieu de supprimer cet ajout. Cet avis est maintenu à l'heure actuelle.

Point 2)

Selon les auteurs du projet, la modification proposée tend à adapter la loi précitée du 30 mai 2005 à l'exigence formulée par l'arrêt „Digital Rights“ relativement à l'effacement des données retenues par les fournisseurs et opérateurs.

Le texte actuel de l'article 5, paragraphe 1^{er}, point a), prévoit que „Après la période de conservation prévue sub (a), le fournisseur de service ou l'opérateur est obligé d'effacer les données relatives au trafic concernant les abonnés et les utilisateurs, ou de les rendre anonymes.“.

La modification proposée introduit la précision que cet effacement doit être „irréversible“ et être fait „sans délai“. La possibilité d'une sauvegarde des données sous une forme anonymisée disparaît de la loi. Le nouveau texte de l'article 5, paragraphe 1^{er}, point a), reprend pour le surplus pour l'essentiel, les principes établis à l'actuel article 5-1, paragraphe 2, de la loi modifiée du 30 mai 2005, qui fait l'objet d'une reformulation partielle dans le projet sous examen.

Comme l'obligation d'effacement est sanctionnée pénalement par le paragraphe 6 du même article, la modification est de nature à créer une protection effective des utilisateurs et trouve dès lors l'approbation du Conseil d'État.

Point 3)

Les auteurs du projet de loi proposent d'élever les peines d'emprisonnement prévues à l'article 5, paragraphe 6, de la loi du 30 mai 2005. Si le Conseil d'État peut suivre le raisonnement indiqué dans l'exposé des motifs, il tient cependant à faire remarquer que cette modification instaure un déséquilibre entre la disposition pénale inscrite à l'article 5, paragraphe 6, et celles inscrites à d'autres endroits de la même loi¹⁹, alors pourtant que les droits protégés par ces autres dispositions sont de valeur égale.

Point 4)

C'est encore en conséquence de l'arrêt „Digital Rights“ que le projet sous examen introduit la précision que les „données concernées par les articles 5 et 9 sont conservées sur le territoire de l'Union européenne“, précision qui trouve l'assentiment du Conseil d'État.

Il y a cependant lieu de supprimer à la seconde phrase du paragraphe 2, le terme de „pleine“ pour ne pas apporter une plus-value législative quelconque. Le texte se lira dès lors comme suit: „... afin d'assurer l'intégrité et la confidentialité de ces données.“.

Le Conseil d'État déplore par ailleurs que le règlement grand-ducal visé à l'article 5-1, paragraphe 2, reformulé, n'ait pas été joint au projet de loi, ce qui, en cas de retard dans la mise en place

¹⁸ Doc. parl. n° 6113³, avis du Conseil d'État, p. 3;

¹⁹ Voir articles 3 (5), 4 (4), 7 (9), 10 (3) et 11 (6). L'article 9 (6) a été omis de cette liste étant donné qu'il figure parmi les dispositions visées au projet sous examen.

des détails techniques appelés à régir l'intégrité et la confidentialité des données retenues, risque d'entraîner l'inapplicabilité pratique des principes établis par la loi.

Points 5), 6) et 7)

Comme ces points ne font qu'apporter à l'article 9 (rétention des données de localisation autres que les données relatives au trafic) de la loi précitée du 30 mai 2005 des modifications identiques à celles proposées pour l'article 5 de ladite loi, le Conseil d'État peut se référer aux observations qu'il a faites à propos de ces dernières.

Ainsi délibéré en séance plénière, le 10 juillet 2015.

Le Secrétaire général,

Marc BESCH

La Présidente,

Viviane ECKER

CTIE – Division Imprimés et Fournitures de bureau

6763/04

N° 6763⁴**CHAMBRE DES DEPUTES**

Session ordinaire 2014-2015

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

SOMMAIRE:

	<i>page</i>
1) Dépêche du Procureur Général d'Etat au Ministre de la Justice (28.7.2015).....	1
2) Avis de la Cour Supérieure de Justice (19.2.2015).....	2
3) Avis du cabinet d'instruction de Luxembourg (19.2.2015)	4
4) Avis du Parquet de Luxembourg	
– Dépêche du Procureur d'Etat de Luxembourg au Procureur Général d'Etat (3.2.2015)	5
5) Avis du Parquet de Diekirch (13.2.2015).....	6
6) Avis du Parquet Général (29.7.2015)	8

*

**DEPECHE DU PROCUREUR GENERAL D'ETAT
AU MINISTRE DE LA JUSTICE**

(28.7.2015)

Monsieur le Ministre,

Le 5 janvier 2015 vous avez fait parvenir au soussigné le projet de loi sous rubrique avec prière de solliciter également les avis de la Cour Supérieure de Justice, des parquets et des cabinets d'instruction de Luxembourg et de Diekirch.

A ce jour les avis suivants ont été transmis au Parquet général

- l'avis de la Cour Supérieure de Justice
- l'avis de Monsieur le juge d'instruction directeur du Luxembourg
- l'avis de Monsieur le procureur d'Etat de Luxembourg
- l'avis de Monsieur le procureur d'Etat de Diekirch

Ces documents sont joints à la présente de même que l'avis du soussigné de ce jour.

Le Procureur Général d'Etat,
Robert BIEVER

*

AVIS DE LA COUR SUPERIEURE DE JUSTICE

(19.2.2015)

Le projet de loi tend à modifier l'article 67-1, alinéa 1er, du code d'instruction criminelle relatif aux écoutes judiciaires à ordonner par le juge d'instruction saisi de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, en remplaçant cette désignation générale des infractions permettant le recours aux écoutes judiciaires, par une énumération détaillée et limitative des différentes infractions pouvant entrer en ligne de compte et devant figurer dorénavant dans un nouvel alinéa 4.

La liste des infractions graves proposée dans le projet de loi est inspirée par l'annexe D de la directive 2014/41/CE du Parlement Européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale.

L'établissement d'une liste exhaustive des infractions serait exigée par l'arrêt rendu le 8 avril 2014 par la Cour de Justice de l'Union Européenne (CJUE) dans les affaires jointes C-293/12 et C-594/12, par lequel la Cour a invalidé la directive 2006/24/CE du Parlement Européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

L'arrêt du 8 avril 2014 de la CJUE a invalidé la directive 2006/24/CE notamment parce qu'elle ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, entre autres en ce qu'elle se borne à renvoyer, à son article 1er, § 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne (n° 60 de l'arrêt).

Il faut cependant se garder d'en induire que la directive 2006/24/CE serait pour ce seul motif contraire aux droits garantis par la Charte. Ce résultat s'explique par un ensemble de déficiences exposées par la CJUE qui l'ont amenée à conclure à une violation du principe de proportionnalité au regard des articles 7, 8, et 52, § 1, de la Charte.

Le progrès censé être procuré par l'établissement d'une liste limitative des infractions qualifiées de graves n'est pas évident, la gravité d'une infraction se définissant toujours par la rigueur de la peine d'emprisonnement comminée.

La durée minimum de la peine d'emprisonnement qui doit être encourue pour permettre le recours aux écoutes judiciaires varie d'un pays à l'autre. Au Luxembourg une peine d'emprisonnement d'au moins un an est suffisante, tandis qu'en France, l'article 100 du code de procédure pénale exige une peine égale ou supérieure à deux ans d'emprisonnement.

La confection d'une liste n'est pas de nature à contribuer à une harmonisation plus poussée sur le plan européen. L'article 90ter, § 2, du code d'instruction criminelle belge comporte une énumération des infractions pouvant justifier une mesure de surveillance partiellement différente de celle prévue par le projet de loi.

Cette harmonisation n'est d'ailleurs nullement requise, puisque la mesure de surveillance de l'article 67-1 du code d'instruction criminelle a un champ d'application territorial ou national et non européen. Chaque Etat définit comme il l'entend les infractions graves qui justifient une surveillance des télécommunications sur son territoire. Il n'existe donc en l'état actuel du droit communautaire aucune nécessité, voire obligation, de recourir à une soi-disant liste européenne des infractions graves.

La liste des infractions graves proposée dans le projet de loi constitue une énumération pêle-mêle de délits et de crimes repris, sans aucun ordre ni logique de classification apparente, tantôt du code pénal tantôt de lois spéciales. Il faut en outre constater que la liste proposée comporte des lacunes, ce qui est un désavantage inhérent à la méthode choisie, et que l'énumération manque de cohérence (voir par exemple le n° 24 relatif au vol) et les indications relatives aux infractions sont dans plusieurs cas partiellement contradictoires en ce sens que les infractions nommément visées ne correspondent pas exactement avec les articles du code pénal auxquels il est fait référence.

Ainsi à titre d'exemples:

Quant au **n° 1) crimes et délits contre la sûreté de l'Etat** (articles 101 à 123 du code pénal).

L'intitulé vise les „crimes et délits contre la sûreté de l'Etat“ sans distinction entre la sûreté extérieure et la sûreté intérieure de l'Etat. Les articles mentionnés ne concernent cependant que les infractions à

la sûreté extérieure de l'Etat. Qu'en est-il des articles 124 à 135 du code pénal? Qu'est ce qui doit l'emporter: les infractions visées par les articles indiqués ou les infractions comprises dans la désignation générale „crimes et délits contre la sûreté de l'Etat“?

Dans d'autres cas, c'est l'inverse: les articles du code pénal mentionnés vont au-delà de l'infraction nommément indiquée (par exemple le n° 28 relatif au faux).

Quant au **n° 8** fraudes et abus de confiance (articles 489 à 509 du code pénal), y compris la fraude portant sur l'atteinte aux intérêts financiers des Communautés Européennes (...).

Le terme „fraude“ est un terme générique qui englobe plusieurs infractions spécifiques, comme, entre autres, l'abus de confiance, mais aussi la banqueroute (frauduleuse), l'abus de faiblesse et l'escroquerie.

Soit on énumère toutes les infractions spécifiques rentrant dans la notion de „fraude“ et non seulement l'une d'elle, en l'occurrence l'abus de confiance, soit on se borne à indiquer une notion générale („fraudes“) et les articles du code pénal y relatifs sans autre précision.

Mais on ne peut pas, sans créer une équivoque, mentionner seulement l'abus de confiance et pour le surplus se référer les articles 489 à 509 du code pénal. On se demande ce qui doit l'emporter, l'énoncé de l'infraction ou les articles du code pénal?

On s'interroge en outre pourquoi l'escroquerie, qui constitue un cas de fraude comme l'abus de confiance, figure à part, au **n° 26**.

A remarquer que l'infraction d'abus de biens sociaux ne figure pas sur la liste.

Quant au **n° 12** blanchiment des produits du crime et recel (articles 505 à 506-8 et 508 à 509 du code pénal), le blanchiment et le recel sont nommément mentionnés, mais pas le cel et les traites de complaisance bien que les articles qui les concernent le soient.

Quant au **n° 24** vol commis à l'aide de violences ou menaces et extorsion (articles 468 à 476 du code pénal).

La liste contient encore un **n° 31** consacré au vol commis sans violences ni menaces (articles 463 à 467 du code pénal) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Qu'en est-il du vol simple et du vol qualifié (avec effraction, escalade ou fausses clefs, vol commis par fonctionnaire public à l'aide de ses fonctions, par des voleurs qui ont pris le titre ou les insignes d'un fonctionnaire public ou qui ont allégué un faux ordre de l'autorité publique article 467 code pénal) sans lien avec une association de malfaiteurs ou une organisation criminelle?

Pourquoi ne pas regrouper tous les cas de vol sous un seul numéro?

Pourquoi intégrer un délit mineur comme le cel dans la liste des infractions graves et en écarter des crimes comme les vols qualifiés visés à l'article 467 du code pénal, non commis dans le cadre d'une association de malfaiteurs?

Pourquoi retenir spécialement le vol commis sans violences ni menaces (articles 463 à 467 du code pénal) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle bien que la simple participation à une association de malfaiteurs ou à une organisation criminelle permette déjà une surveillance judiciaire indépendamment de tout vol (n° 2 de la liste)?

Les infractions de contrefaçon visées aux articles 179 à 191 du code pénal (**n° 27**) devraient figurer logiquement avec le faux-monnayage (n° 13).

Quant au **n° 28** qui vise la falsification de documents administratifs et usage de faux ensemble avec les articles 193 à 212 du code pénal.

Pourquoi mentionner nommément la „falsification de documents administratifs“, notion qui ne figure pas au code pénal, alors que les articles 193 à 212 traitent du faux en écritures authentiques et publiques, en écritures de commerce ou de banque et en écritures privées ainsi que du faux commis dans les passeports, permis de chasse ou de pêche, livrets, feuilles de route, certificats et attestations?

On remarque au passage, à titre d'exemple, que ni l'infraction de faux bilan ni les infractions de faux témoignage, de faux serment et de subornation ne figurent dans la liste des infractions graves,

bien que, par exemple, le faux témoignage en matière criminelle soit puni de la réclusion de cinq à dix ans.

Il en est de même du crime prévu à l'article 235 du code pénal qui n'est pas visé au n° 1 de la liste qui se réfère uniquement aux articles 101 à 123 du code pénal.

Il serait peut-être préférable de maintenir en l'état actuel des choses l'article 67-1 dans sa version actuelle.

Subsidiairement, si l'on veut néanmoins établir une liste des infractions graves, il serait avantageux de suivre l'ordre des infractions dans le code pénal et indiquer ensuite les infractions prévues dans les lois spéciales entrant en ligne de compte.

*

AVIS DU CABINET D'INSTRUCTION DE LUXEMBOURG

(19.2.2015)

Le projet de loi a pour but d'adapter notre législation suite à l'arrêt rendu par la Cour de Justice de l'Union Européenne en date du 8 avril 2014, qui a invalidé la directive 2006/12/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de détection et de poursuite des infractions graves.

La directive invalidée avait été transposée par la loi du 30 mai 2005 qui a retenu une durée de conservation des données de seulement 6 mois, tout en adoptant un critère assez large pour déterminer l'infraction grave justifiant ainsi l'accès aux données qui était donné à chaque fois qu'une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement était prévue.

L'article 67-1 du code d'instruction criminelle tel qu'introduit par une loi du 21 novembre 2002 réserve le repérage téléphonique au seul juge d'instruction, délimite son champ d'application des données avec l'obligation pour le magistrat d'indiquer dans une ordonnance motivée qu'il communique au procureur d'Etat les circonstances de fait de la cause justifiant la mesure.

Le projet de loi sous discussion maintient le principe de la conservation des données de télécommunications pendant un délai de 6 mois au plus et se propose de définir de manière limitative et exhaustive les infractions graves par une énumération de 33 catégories d'infractions reprise de l'article 11 de la directive 2014/41/UE.

L'idée du projet de loi est d'énumérer dans le paragraphe 4 nouveau de l'article 67-1 du Code d'Instruction criminelle des catégories d'infractions pour lesquelles les autorités répressives peuvent avoir accès aux données de communications obtenues. Cette liste s'inspire de la liste des infractions prévues à l'annexe D de la directive 2014/41/UE du parlement européen et du conseil du 3 avril 2014 concernant la décision d'enquête européennes en matière pénale. Cette liste a été dressée pour une finalité qui s'apparente, dans le contexte de l'entraide pénale internationale, à celle du recours aux données de communications retenues par les opérateurs de télécommunications. Le projet propose cependant d'amender cette liste en la précisant par des renvois à des articles déterminés du Code pénal et de certaines lois spéciales afin de l'adapter aux spécificités du droit pénal luxembourgeois.

Force est de constater qu'une nouvelle liste d'infractions à ajouter dans notre législation pénale nationale aura nécessairement comme conséquence que les règles de procédure pénale deviennent de moins en moins lisibles et que leur application devient de plus en plus difficile pour les praticiens et à la limite incompréhensible pour les justiciables.

Le projet de loi abandonne d'une certaine manière le principe de la sécurité juridique assurée sur le critère objectif du seuil de peine privative de liberté dont le maximum est égal ou supérieur à 1 an en adoptant une nouvelle liste d'infractions qui s'inspirent de notions et de concepts repris d'une directive UE en y ajoutant des articles déterminés du Code pénal luxembourgeois et de certaines lois spéciales.

La liste des infractions figurant dans le projet de loi sous examen appelle les observations suivantes:

- a) Il convient de relever d'emblée que ne figurent pas dans la liste certains délits et notamment la fausse alerte et la menace d'attentat alors que ces infractions sont très souvent perpétrées par l'utilisation de communication téléphoniques ou électroniques et que très souvent aussi le seul moyen

afin de pouvoir les élucider consistant à faire procéder du moins dans un premier temps à un retraçage de ces communications.

- b) Il convient aussi de s'interroger à la lecture de la liste des infractions sur la notion du trafic qui est une notion et un concept repris du droit international et qui n'existe pas comme infraction spécifique dans le droit pénal luxembourgeois.
- c) Force est également de relever que certaines infractions n'atteignent pas le degré de gravité requis afin de justifier le retraçage et le repérage de télécommunications que si elles ont été commises dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle alors que d'autres infractions sont considérées comme suffisamment graves sans cette circonstance aggravante comme en espèce le recel (point 12 de la liste des infractions). Il convient par ailleurs de souligner que le vol simple repris dans le point 31 dans la même liste exige pour justifier la mesure de repérage que ce dernier a été commis dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Le juge d'instruction directeur,
Ernest NILLES

*

AVIS DU PARQUET DE LUXEMBOURG

DEPECHE DU PROCUREUR D'ETAT DE LUXEMBOURG AU PROCUREUR GENERAL D'ETAT

(3.2.2015)

Monsieur le Procureur Général d'Etat,

Comme suite à votre demande du 16 janvier 2015, je me permets de vous soumettre l'avis du Parquet de Luxembourg sur le projet de loi visé.

Le texte en projet entend mettre la législation pénale luxembourgeoise en adéquation avec l'arrêt de la Cour de Justice de l'Union Européenne, pour autant que cela soit possible.

L'opportunité de la démarche n'est donc pas à discuter. Les dispositions en projet, pour ne pas abandonner de manière intégrale la possibilité de recourir à l'exploitation des données de télécommunications pour les besoins de l'instruction de certaines infractions, visent donc principalement et en premier lieu à remplacer la référence à un certain seuil de peine privative de liberté pour déterminer les infractions entrant en ligne de compte, par une liste d'infractions nommément désignées. Une liste comporte des risques d'omission et le recours à cette méthode a déjà fait l'objet de critiques à de nombreuses reprises dans le cadre de l'examen d'autres textes de loi dans le domaine pénal et de procédure pénale.

Il convient donc d'apprécier si les dispositions arrêtées par le Projet de loi sont en concordance avec les réalités de la lutte contre la criminalité.

A cet égard le commentaire se limitera à révéler certaines lacunes dans la liste et à proposer en conséquence certaines adjonctions et certaines modifications/rectifications.

Ad article 1er – PL 6763

Il convient de compléter la liste développée sous 2) de l'article 1er du Projet de loi, par l'infraction de fausse alerte – article 319 CP, de même que par celle des menaces d'attentat – article 327 CP et celle des offres ou propositions de commettre un crime – article 331 CP, infractions qui souvent comportent le recours à des moyens de télécommunication.

Au point 7) de la même liste, aux fins d'être complet dans le domaine des infractions de corruption et apparentées, il convient d'ajouter l'infraction de prise illégale d'intérêts et d'indiquer en début de la référence aux articles du Code pénal visés, l'article 245 CP.

Au point 8) de la même liste, aux fins d'être complet dans le domaine des comportements frauduleux, il convient d'ajouter l'infraction d'abus de biens sociaux (article 171-1 de la loi modifiée du 10 août 1915 concernant les sociétés commerciales).

Au point 13) de la liste, il est préférable de remplacer les termes „faux monnayage et contrefaçon de monnaie“ par les termes „contrefaçon de moyens de paiement, de titres, de sceaux, timbres, poinçons, marques. etc.“ les articles du Code pénal indiqués entre parenthèses couvrant des hypothèses diverses allant bien au-delà de la fausse monnaie.

Au point 27) de la liste, il convient de préciser qu’est visée la contrefaçon „d’œuvres protégées par des droits de propriété intellectuelle (Loi modifiée du 18 avril 2001 sur les droits d’auteur, les droits voisins et les bases de données)“, les articles 179 à 191 du Code pénal se trouvant déjà repris sous le point 13) de la liste.

Au point 28) de la liste il est préférable de remplacer les termes „falsification de documents administratifs“ par le terme „faux“, en raison des termes „usage de faux“ employés par la suite et au regard des infractions visées par les articles du Code pénal indiqués entre parenthèses; dans le même contexte il convient de remplacer l’article 212 par 214, plus adapté.

Au point 31) de la liste, il convient de faire abstraction du cadre spécifique visé pour l’infraction de vol sans violence ni menaces, les autres infractions contre la propriété, comme les fraudes et abus de confiance et l’escroquerie, de même que le recel, n’étant pas non plus limitées par la condition de devoir se situer dans le cadre des agissements d’une association ou organisation criminelle.

L’article 2 du Projet de loi ne soulève pas d’observations particulières.

Profond respect.

Le Procureur d’Etat,
J.P. FRISING

*

AVIS DU PARQUET DE DIEKIRCH

(13.2.2015)

Le projet de loi a pour but d’adapter notre législation suite à l’arrêt rendu par la Cour de Justice de l’Union Européenne en date du 8 avril 2014, qui a invalidé la directive 2006/12/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves.

La Cour a plus particulièrement reproché à cette directive d’avoir omis de prévoir des règles claires et précises en vue de régir la portée de l’ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, constatant que la directive comportait une ingérence d’une vaste ampleur dans ces droits fondamentaux et d’une gravité particulière dans l’ordre juridique de l’Union, sans que cette ingérence fût précisément encadrée par des dispositions permettant de garantir qu’elle se limitait effectivement au strict nécessaire. (cf. Arrêt pt. 65)

La Cour a ainsi critiqué:

- a. L’absence générale de limite (Arrêt pt. 58 et 59)
 - o La directive visait de manière globale toute personne faisant usage de services de communications électroniques (peu importe l’existence d’indices d’infraction ou le secret professionnel).
 - o La directive n’exigeait aucune relation entre les données dont la conservation était prévue et une menace pour la sécurité publique (période temporelle, zone géographique, cercle de personnes suspectées).
- b. L’absence de critère objectif pour délimiter l’accès des autorités nationales compétentes et leur utilisation ultérieure (Arrêt pt. 60 à 62).
- c. S’agissant de la durée de conservation des données, la directive fixait un délai sans que fût opérée une distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l’objectif poursuivi ou selon les personnes concernées. La durée de conservation (entre 6 et 24 mois) aurait dû être fondée sur des critères objectifs afin de garantir que celle-ci fut limitée au strict nécessaire (Arrêt pt. 63 et 64).
- d. La protection des données par les fournisseurs accompagnée de l’obligation de destruction irrémédiable au terme de la durée de conservation et de conservation sur le territoire de l’Union, n’était pas suffisamment garantie (p. 66 et 67).

La directive invalidée avait été transposée par la loi du 30 mai 2005 qui opta pour une durée de conservation des données très courte (6 mois), tout en adoptant un critère assez large pour déterminer l'infraction grave, et justifiant ainsi l'accès aux données, qui était donné chaque fois qu'une peine correctionnelle d'un maximum égal ou supérieur à un emprisonnement d'un an était prévue par la loi.

Le projet de loi sous discussion maintient le principe de la conservation des données de télécommunication pendant un délai de 6 mois au plus, ce qui fut le minimum prévu par la directive invalidée, et se propose de définir restrictivement et limitativement les infractions graves par une énumération de 33 infractions qui est reprise de l'article 11 de la directive 2014/41/UE.

L'article 11 de cette directive énonce les motifs possibles d'une non-reconnaissance ou non-exécution d'une décision d'enquête européenne, c'est-à-dire les cas où un Etat dispose de la faculté de refuser la reconnaissance ou l'exécution d'une décision d'enquête européenne. Conformément à l'article 11, point g), cette faculté est exclue au cas où les faits constituent dans l'Etat d'émission une des susdites 33 infractions et sont punissables dans le pays d'émission d'une peine ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins trois ans.

Le fait d'ajouter une nouvelle liste d'infractions dans notre législation pénale nationale, en dehors de celles qui y figurent d'ores et déjà comme par exemple celle prévue dans la loi sur le mandat d'arrêt européen (loi modifiée du 17 mars 2004, article 3) ou celle inscrite à l'article 506-1 du Code pénal sur l'infraction de blanchiment, aura non seulement comme conséquence inéluctable que les règles de procédure pénale deviendront de moins en moins lisibles, mais également que leur application deviendra de plus en plus difficile pour les praticiens, voire incompréhensible pour les justiciables.

Au lieu de veiller à créer des règles de procédure pénale claires et facilement prévisibles pour toute personne visée par une instruction ou pour toute victime préjudiciée par une telle infraction, on aboutira de plus en plus à faire application de textes compliqués, avec des listes d'infractions variables, sans relation apparente avec la gravité des peines prévues par le législateur.

Si on peut comprendre l'initiative du législateur d'énumérer les infractions qui, à ses yeux, relèvent d'une gravité telle que leur élucidation devrait pouvoir se faire, dans des circonstances spécialement motivées par un juge d'instruction, en procédant par un repérage et retraçage de télécommunications et de ne plus maintenir le seuil fixé par la loi du 30 mai 2005 à une peine d'emprisonnement correctionnel d'un maximum égal ou supérieur à un an pour définir cette gravité, il est par contre difficilement compréhensible pourquoi tous les crimes, infractions punissables d'une peine de réclusion, partant d'une peine particulièrement grave et sévère aux yeux du législateur, ne seraient pas considérés comme suffisamment graves pour justifier, dans les mêmes circonstances spéciales dûment motivées, le recours au retraçage et au repérage de télécommunications pour les élucider.

Il est dès lors proposé d'ajouter à la liste, à l'instar de ce qui a été fait en matière de blanchiment, **„ainsi que toute autre infraction punie d'une peine criminelle“**.

Comment peut-il en effet se justifier qu'en matière de crime, certaines mesures d'investigation seraient exclues d'emblée par le législateur, nonobstant les circonstances exceptionnelles d'une espèce déterminée à relever par le juge d'instruction, et à contraindre les organes de poursuite à se résigner, dans ces hypothèses, à ne pas pouvoir utiliser toutes les mesures techniques disponibles pour essayer de les élucider.

La liste d'infractions figurant actuellement dans le projet de loi, appelle de surcroît les observations suivantes:

- a. Il est étonnant de constater que dans un texte à vocation nationale, le législateur entend faire figurer des notions et concepts repris d'une directive UE, mais n'existant pas en tant que tels en droit luxembourgeois, telle que la notion de „trafic“, et il est difficile de voir l'utilité de recourir en droit national à ces concepts de droit international.
- b. En termes de technique législative, il semble également surprenant de se référer principalement des incriminations reprises d'une directive UE pour les faire correspondre en quelque sorte en ordre subsidiaire, puisque énoncées entre parenthèses, à des infractions prévues dans notre législation nationale, alors qu'il pourrait sembler plus adéquat de faire principalement référence à des infractions prévues dans notre législation nationale, avec des éléments constitutifs bien définis et facilement déterminables, avant de se référer à des notions internationales qui ont essentiellement vocation à englober toutes les spécificités des différentes législations des Etats membres.

Ainsi, à titre d'exemple, il convient de renvoyer à l'infraction visée au point 28) „falsification de documents administratifs et usage de faux (art. 193 à 212 du Code pénal)“, puisque la législation

nationale énoncée entre parenthèses vise la perpétration de faux commis en écritures tant publiques que privées ainsi que l'usage de ces faux, et ne se limite nullement à une falsification de documents administratifs.

- c. Il paraît encore discutable qu'un certain nombre d'infractions n'atteignent le degré de gravité requis pour justifier le repérage et le retraçage de télécommunications que si elles ont été commises „dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle“ (points 18, 20, 29, 30 et 31), alors que d'autres sont considérées comme assez graves sans cette circonstance aggravante, dont par exemple le recel prévu au point 12. Or, le vol simple mentionné au point 31, lequel peut être à la base du recel, n'y figure que dans l'hypothèse où il a été commis dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Il convient d'y ajouter la grivèlerie (peine maximale 6 mois d'emprisonnement au vu de l'article 491 du Code pénal), les coups et blessures simples (peine maximale 6 mois d'emprisonnement maximum au vu de l'article 398 du Code pénal) qui sont, d'après le projet de loi, per se d'une gravité telle qu'elles peuvent justifier l'accès aux données de communication, alors qu'au vu du point 31 un vol à l'aide d'effraction ou de fausse clé (article 467 du Code pénal) n'est considéré comme infraction assez grave pour justifier cette mesure que s'il a été commis dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Le Code pénal met d'ailleurs sur le même pied en termes de peines et donc de gravité (réclusion de 5 à 10 ans) le vol qualifié de l'article 467 (point 31) avec celui commis à l'aide de violences ou de menaces de l'article 468 du Code pénal (point 24), ce dernier n'ayant toutefois pas besoin d'être commis dans le cadre d'une association de malfaiteurs pour permettre un repérage des télécommunications.

- d. Reste à relever que les délits de fausse alerte et de menaces d'attentat ne figurent pas dans la liste, malgré le fait que ceux-ci sont très souvent perpétrés par le biais de communications téléphoniques ou électroniques, et que ces délits ne peuvent ainsi être élucidés dans la majorité des cas que par un retraçage de ces communications.

*Le Procureur d'Etat près le Tribunal
d'arrondissement de Diekirch,*

Aloyse WEIRICH

*

AVIS DU PARQUET GENERAL

(29.7.2015)

I) REMARQUE PRELIMINAIRE

Aux termes de l'exposé des motifs le projet de loi tend à „adapter le dispositif légal relatif à la rétention des données de télécommunications à des fins de poursuites pénales aux exigences de l'arrêt rendu par la Cour de Justice de l'Union européenne en date du 8 avril 2014, dit „Digital Rights“ (affaires jointes C-293/12/ et C-594/12), par lequel la Cour a invalidé la directive 2006/24/CD du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves.“.

Le projet tend donc à modifier notre législation pour l'adapter suite à l'arrêt de la Cour de Justice de l'Union européenne invalidant la directive 2006/24/CE du 15 mars 2006 relative à l'objet indiqué ci-avant.

Il se trouve toutefois que notre loi, qui date du 30 mai 2005, n'a pas transposé en droit luxembourgeois la directive 2006/24¹.

Il s'y ajoute que lors de la modification de la loi du 30 mai 2005 par la loi du 18 juillet 2011, on n'a pas fait la moindre référence à la directive 2006/24 qui allait être annulée le 8 avril 2014.

¹ Il ne s'agit en l'occurrence en rien d'une simple erreur matérielle de dates.

A préciser que ni dans les travaux parlementaires ayant abouti à la loi de 2005 ni dans ceux qui ont abouti à la loi de 2011 il n'est fait la moindre référence à la directive (annulée) 2006/24.

Notre législation est donc tout à fait indépendante des dispositions du droit de l'Union Européenne, qui ont été invalidées par l'arrêt „Digital Rights“.

Il en résulte, et le point est important voire essentiel, que l'annulation de la directive visée par la Cour de Justice de l'Union Européenne n'a aucune incidence sur la validité de la législation luxembourgeoise et ce d'autant moins que dans sa motivation la Cour de Justice de l'Union Européenne s'est uniquement basée sur des articles relatifs à la protection de la vie privée figurant dans la Charte des droits fondamentaux de l'Union Européenne. Or, cette Charte dispose dans son article 51, paragraphe 1, que ses dispositions „s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres uniquement lorsqu'elles mettent en oeuvre le droit de l'Union.“.

La loi luxembourgeoise modifiée de 2005 n'ayant pas mis en oeuvre le droit de l'Union Européenne, l'arrêt de la Cour de Justice de l'Union Européenne n'a juridiquement aucune incidence sur la validité de notre législation².

*

L'avis relatif au projet soumis pourrait dès lors parfaitement s'arrêter ici.

Toutefois l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (C.E.D.H.) protège également la vie privée des citoyens et n'admet des exceptions à ce principe que si celles-ci sont proportionnelles à l'atteinte à la vie privée et justifiées notamment par la sûreté et la sécurité.

La C.E.D.H. étant d'application directe elle peut être invoquée directement devant nos juridictions.

Dès lors, qu'on le veuille ou non, la question risque de surgir sous peu sous une forme ou une autre devant nos juridictions ou encore devant le Cour Européenne des Droits de l'Homme elle-même et il

2 La Belgique avait transposé la directive 2006/24/CE (invalidée par l'arrêt C-293/12 et C-594/12 de la CJUE du 8 avril 2014) par une loi du 30 juillet 2013. Cette loi avait notamment modifié par son article 5 un article 126 d'une loi du 13 juin 2005 relative aux communications électroniques en faisant précisément et de manière expresse référence à la directive 2006/24. Sans le cadre d'un recours devant la Cour constitutionnelle de Belgique les requérants ont considéré que la loi de 2013, et notamment son article 5, méconnaissent l'arrêt de la CJUE.

La thèse du Gouvernement belge était de soutenir:

- o Que certes l'arrêt de la CJUE a pour effet d'obliger tout juge de considérer la directive comme invalide.
- o Que ce constat s'étend aux dispositions nationales qui transposent la directive. Ces dispositions perdent leur validité par suite de l'arrêt de la Cour (A.5.1.).
- o Que ce ne seraient cependant que les articles 2 et 3 de la loi de 2013 auxquels s'appliquerait ce sort.
- o Qu'en revanche l'article 5 de la loi pourrait être séparé du reste de la loi attaquée, de sorte que l'irrégularité d'autres articles de cette loi n'affecterait pas l'article 5 (A.5.1.).
- o Que l'arrêt de la CJUE, en invalidant la directive, redonne compétence aux Etats membres de régler la problématique de la rétention des données (faute d'harmonisation en la matière) (idem).
- o Que l'article 5 de la loi n'est donc doublement pas affectée par l'arrêt: il ne transposerait pas la directive, donc ne tomberait pas avec celle-ci et il s'appliquerait, suite à l'invalidation de la directive, dans un domaine dans lequel le législateur belge reste libre de légiférer sans interférence du droit de l'Union européenne. (A.5.1 et B.7).

La Cour constitutionnelle de la Belgique a par un arrêt du 11 juin 2015 rejeté ce raisonnement au motif, en substance, que l'article 5 transpose bien la directive, donc tombe avec elle et se voit, dans la mesure où il transpose la directive, appliquer la Charte des droits fondamentaux (B.8).

La Charte des droits fondamentaux dispose dans son article 51, paragraphe 1, que ses dispositions „s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres **uniquement lorsqu'ils mettent en oeuvre le droit de l'Union**“.

Tel ayant été le cas en Belgique la Cour constitutionnelle du Royaume de Belgique a, par l'arrêt du 11 juin 2015 annulé la loi belge afférent qui a été adoptée précisant en vue de mettre en oeuvre le droit de l'Union Européenne.

La Cour constitutionnelle note dans son arrêt que les méthodes proposées par les requérants pour séparer les métadonnées des avocats de celles du commun des mortels sont impraticables (voir notamment A.3.3.). La seule issue possible serait de renoncer à la rétention de données. C'est le tout ou rien. Voir le point A.4.5, résumant la thèse des requérants: „Quant à l'impossibilité invoquée de mettre en oeuvre une distinction selon que les données émanent de titulaires du secret professionnel ou d'autres personnes, ces difficultés ne justifieraient pas qu'une annulation pure et simple de la disposition critiquée ne puisse être prononcée afin de mettre fin à une situation discriminatoire“.

est à prévoir que les requérants soulèveront alors plus ou moins les mêmes moyens que ceux qui ont été abordés dans l'arrêt de la Cour de Justice de l'Union Européenne du 8 avril 2014.

Il est dès lors indispensable d'analyser le problème.

*

**II) ANALYSE SUCCINCTE DE L'ARRET DE LA COUR DE
JUSTICE DE L'UNION EUROPEENNE
du 8 avril 2014 par lequel la directive 2006/24 de l'Union Européenne
a été annulée, l'arrêt peut être résumé comme suit:**

La Cour de Justice de l'Union européenne a annulé la directive 2006/24/CE (ci-après la directive) après un examen approfondi des textes aux motifs notamment que „*cette directive importe une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire*“ (point 65), après avoir relevé que, **les dispositions de la directive 2006/24/CE relative à la conservation des données électroniques portent atteinte à certaines dispositions de la Charte des Droits Fondamentaux de l'Union Européenne.**

Est d'abord mise en cause la protection de la vie privée reconnue à **l'article 7 de la Charte** (points 25 et 34), qui est affectée „*de manière directe et spécifique*“ (point 29): il est à ce sujet souligné que les „*données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées*“ (point 27), la Cour insistant sur le fait qu'il importe peu que „*les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence*“ (point 33) et que „*l'accès des autorités nationales compétentes aux données constituent une ingérence supplémentaire dans ce droit fondamental*“ (point 35).

Quant à la mise en oeuvre d'une dérogation aux exigences posées par **l'article 8 de la Charte** en matière de protection des données à caractère personnel (points 29 & 36), dont le régime est organisé par les directives 95/46 et 2002/58 relatives au traitement des données à caractère personnel dans le secteur des communications électroniques (point 32), la Cour estime, „*la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci*“ (point 53).

La Cour conclut que: „*l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère [...] d'une vaste ampleur*“; „*elle doit être considérée comme particulièrement grave*“; „*la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante*“ (point 37).

Toutefois, et ce point a été négligé – de manière délibérée ou non – par maint commentateur de l'arrêt, la Cour analyse ensuite le respect de **l'article 52 § 2 de la Charte** en vertu duquel „*toute limitation de l'exercice des droits et des libertés consacrés du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui*“. Elle analyse de ce point de vue:

- la reconnaissance de la poursuite d'un objectif d'intérêt général; et
- le respect des principes de nécessité et de proportionnalité.

Elle répond de façon positive à **la question de savoir si la directive 2006/24/CE respecte le „contenu essentiel“ des droits considérés.**

Il en est ainsi selon elle parce que „*la directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel*“ (point 39) et que les „*fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, doivent respecter certains principes selon lesquels les Etats membres veillent à l'adoption de mesures tech-*

niques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données" (point 40).

La Cour poursuit son travail d'examen, mettant ainsi en évidence que le respect du contenu essentiel des droits n'est pas suffisant en soi, mais que toutes les exigences posées par l'article 52 § 2 de la Charte doivent être respectées.

Elle s'attache en conséquence à vérifier si les atteintes aux droits fondamentaux constatées sont justifiées par la poursuite d'un objectif d'intérêt général.

Elle estime – et ce point est essentiel – que „*la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquêtes*“.

Néanmoins, elle ajoute immédiatement que „*un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte*“ (point 51). Autrement dit, **la lutte contre la criminalité organisée et contre le terrorisme, au nom de la préoccupation de sécurité intérieure, ne saurait autoriser des atteintes inutiles et inadéquates, inappropriées et injustifiées aux droits fondamentaux des citoyens européens**. En effet, comme le rappelle la Cour, „*dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci*“ (point 47).

La Cour contrôle ensuite le respect des principes de nécessité et de proportionnalité, en s'assurant d'abord que les mesures adoptées sont bien nécessaires à la réalisation de l'objectif poursuivi, et ensuite que les dispositions en cause emportent des limitations des droits fondamentaux proportionnées d'une part à l'objectif poursuivi et d'autre part aux résultats escomptés.

Elle se livre ici encore à un **contrôle strict** étant donné que: „*compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict*“ (point 48).

Pour ce qui est de **la nécessité des mesures adoptées pour atteindre l'objectif fixé**, la Cour admet que la conservation des données constitue „*un instrument utile*“ en matière de poursuites pénales (point 49)³.

Elle examine **la proportionnalité des dispositions de la directive à l'objectif matériel poursuivi**. Est rappelée l'exigence pour le législateur européen de „*prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données*“ (point 54), cette exigence de prévoir de telles garanties étant „*d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données*“ (point 55).

Or, cet impératif n'est, aux yeux du juge de l'Union, pas respecté de façon satisfaisante par la directive 2006/24/CE, et ce pour plusieurs raisons.

Premièrement, le texte impose „*la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet*“ et „*couvre tous les abonnés et utilisateurs inscrits*“ (point 56), tant et si bien qu'elle „*concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques*“ (point 58), et par là même emporte „*une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne*“ (point 56).

³ La Cour ne s'oppose donc nullement par principe à toute rétention de données, ce qui serait irresponsable, elle estime tout simplement qu'il faut l'encadrer de conditions strictes.

Deuxièmement, **le texte n'établit aucune limitation de l'accès aux données conservées** des autorités nationales de sécurité (point 60), n'énonce aucune condition matérielle et procédurale pour l'exercice d'un tel accès (point 61), n'envisage aucun contrôle préalable par une juridiction ou une entité administrative indépendante (point 62).

Troisièmement, **le texte n'encadre pas la conservation des données** durant la période de 6 mois à 2 ans établie, puisqu'il n'opère pas de distinction entre les données conservées en catégories conçues en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées (point 63), n'impose pas de dispositifs „*permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données*“ (point 66), n'exige **aucunement** la conservation des données sur le territoire de l'Union (point 68)⁴.

Ensuite la Cour critique encore les faits que:

- le défaut de limitation de la conservation porte soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes déterminé susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, et
- le fait que la directive n'impose pas que les données en cours soient conservées sur le territoire de l'Union de sorte que le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3 de la Charte.

Aussi est-ce pour l'ensemble de ces raisons que la Cour a estimé que la directive est contraire à la Charte, alors qu'elle est trop imprécise et laisse ouverte beaucoup de questions.

*

III) L'OBJET DU PROJET DE LOI SOUS EXAMEN

Il importe de souligner que l'objet essentiel du projet de loi est de préciser les conditions dans lesquelles un juge d'instruction peut ordonner le repérage de communications.

A lire tant l'arrêt de la Cour de Justice que des articles de doctrine parus dans la suite on ne peut se défaire de l'impression qu'il y a une confusion entre la rétention de données et le repérage de données précises.

La **rétention** visée est la conservation des données recueillies par les fournisseurs de services dans le cadre de leurs activités de mise à disposition de communications électroniques au public ou de réseaux publics de communication. Il s'agit d'atteintes purement virtuelles à la vie privée des utilisateurs de tels moyens de communication.

⁴ Sur ce point il semble y avoir un malentendu majeur:

Le propre de toute enquête policière ou judiciaire est de rechercher les auteurs, coauteurs ou complices d'une infraction. Il est dès lors impossible de délimiter la rétention des données „*selon les personnes concernées*“, puisqu'on ne les connaît pas: d'où d'ailleurs le problème que les données, une fois qu'on admet le principe de la rétention de données et de repérage consécutif il est impossible de les limiter à des personnes déterminées, à moins que l'on ait l'idée – pour le moins saugrenue – d'établir des listes contenant d'une part des personnes au-dessous de tout soupçon et d'autre part des personnes suspectes (de par leurs antécédents? leur personnalité? le milieu dans lequel ils vivent?). Il s'entend qu'un tel système serait contraire aux principes les plus élémentaires en matière de protection des droits de l'homme.

La Cour constitutionnelle de Belgique a d'ailleurs fort bien vu ce problème dans son arrêt du 11 juin 2015, dans une affaire où les requérants (des avocats) faisaient grief à la législation belge en la matière de ne pas exclure du système des personnes dont l'activité tombe sous le secret professionnel, de sorte que celui-ci serait ainsi violé, la Cour ayant souligné „*que les méthodes proposées par les requérants pour séparer les métadonnées des avocats de celles du commun des mortels sont impraticables (voir notamment A.3.3.). La seule issue possible serait de renoncer à la rétention de données. C'est le tout ou rien. Voir le point A.4.5, résumant la thèse des requérants: „Quant à l'impossibilité invoquée de mettre en oeuvre une distinction selon que les données émanent de titulaires du secret professionnel ou d'autres personnes, ces difficultés ne justifieraient pas qu'une annulation pure et simple de la disposition critiquée ne puisse être prononcée afin de mettre fin à une situation discriminatoire*“.

Le même problème se pose en ce qui concerne la détermination des mesures visées à une zone géographique déterminée. S'il y a certes des situations où une telle détermination se justifie (et elle est d'ailleurs réalisée à l'heure actuelle), on ne saurait limiter la rétention de données par principe à des zones géographiques déterminées, la mondialisation du terrorisme – et les résultats de certaines enquêtes étant là pour nous le démontrer tous les jours.

D'ailleurs, tout près de nous le tueur des victimes du Musée juif de Bruxelles ne venait-il pas de Marseille où se trouvent d'ailleurs les membres de son organisation?

Une **mesure de repérage** a pour but de retrouver et d'identifier la source d'une communication, la destination de celle-ci, la date, l'heure, la durée et le type de la communication, le matériel utilisé à cette fin, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.

„Seulement ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.“ (point 27 de l'arrêt de la Cour).

Cette intrusion dans la vie privée est infiniment plus grande que la simple rétention de données, même si par une mesure de repérage le contenu des informations échangées reste, par définition, parfaitement inconnu.

Il n'y donc pas lieu de confondre non plus repérage et par exemple écoutes téléphoniques.

L'article 67-1 de notre code d'instruction criminelle prescrit de manière détaillée les conditions et modalités auxquelles le juge d'instruction doit soumettre ses ordonnances relatives à une **mesure de repérage**.

*

IV) NOTRE LEGISLATION EST-ELLE CONFORME AUX CRITERES DEGAGES PAR LA COUR DE JUSTICE?

Il est un fait que notre législation en la matière est bien plus protectrice du droit à la vie privée que ne l'était la directive 2006/24/CE.

En effet notre législation prévoit un certain nombre de garanties:

- Seule une autorité judiciaire indépendante, à savoir le juge d'instruction peut par une ordonnance motivée décider un repérage.
- Le repérage est réservé, aux termes de la loi sous avis, aux autorités judiciaires donc à une autorité indépendante et impartiale qui prend sa décision sur la base d'une enquête judiciaire préalable.
- Aux termes de l'article 67-1 du code d'instruction criminelle toute personne qui a fait l'objet d'une mesure de repérage doit en être informé, au cours de l'instruction et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance. La durée d'une mesure de repérage ne peut en principe excéder un mois sauf renouvellement.
- Tout justiciable visé dispose de la possibilité d'introduire une requête en nullité contre la mesure ordonnée et, finalement, si la mesure de repérage n'a donné aucun résultat, *„les données obtenues seront retirées du dossier de l'instruction et détruits dans la mesure où elles concernent des personnes non-inculpées“* (Alinéa final de l'article 67-1 du code d'instruction criminelle).
- Notre loi ne permet un repérage et la rétention de données dans sa suite que si le fait visé par l'instruction préparatoire emporte une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an.
- La durée de rétention de données est limitée dans notre législation à 6 mois et ne peut en aucune hypothèse s'étendre jusqu'à 24 mois (ainsi que le permettait la directive annulée).
- Le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics (Mémorial A, 2010, n° 122, page 2016) précise, conformément aux exigences de la Cour de justice les catégories de données à retenir.

S'il est exact que notre loi ne correspond pas en tous points aux critères exigés par la Cour, il n'en reste pas moins que notre législation s'en approche de très près et est de toute façon bien plus proche que des exigences „vagues“ de la directive visée. La discussion de savoir si notre législation aurait

également subi les „foudres“ d’une juridiction nationale ou internationale est certes intéressante mais dans les conditions données de nature purement académique.

*

Il importe toutefois de noter que le justiciable ne dispose d’aucune garantie si la rétention (et le repérage consécutif) est effectuée par le SREL.

A noter qu’aucune des garanties indiquées ci-avant ne figure aux paragraphes (2) et (3) de l’article 10 du projet de loi 6675 portant organisation du Service de Renseignement de l’Etat (ni la version originale du projet, ni l’avis du Conseil d’Etat n’abordent le sujet).

La question se pose dès lors s’il n’y a pas lieu de modifier ce projet sur ce point, étant donné qu’il ne saurait y avoir deux législations parallèles ayant le même objet mais accordant aux citoyens plus ou moins de droits selon le service qui ordonne la mesure!

A noter encore que les auteurs des textes semblent avoir moins de confiance dans la Justice que dans le service secret. Les dangers de ces confusions ont d’ailleurs été longuement exposés dans l’avis du soussigné du 2 avril 2015 relatif au projet de loi 6761 relatif au terrorisme.

*

V) EXAMEN DU TEXTE DU PROJET DE LOI

Ad article 1er

Pour les raisons développées ci-avant il importe de préciser les infractions pour lesquelles le juge d’instruction peut, en cas d’une instruction préparatoire, ordonner une mesure de repérage.

La Cour de justice sanctionne bien logiquement une telle „absence générale de limites“ (point 60) par l’annulation intégrale et immédiate de la directive 2006/24/CE, annulation dont les implications se révèlent très exigeantes tant pour les institutions européennes que pour les autorités nationales.

Au lieu de prévoir que les faits pour lesquels le juge d’instruction peut ordonner un repérage doivent emporter une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d’emprisonnement, le projet prévoit une liste d’infractions ce qui se justifie, du moins en principe, parfaitement.

Notre législation pénale est en effet, du point de vue des peines, trop hétéroclite et incohérente pour que le critère, permettant de procéder à un repérage, soit fixé par une référence au seuil des peines.

Les auteurs du projet se sont inspirés pour la rédaction du texte proposé, du moins dans une certaine mesure, de la liste des infractions prévues à l’annexe D de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d’enquête européenne en matière pénale.

Si la référence à une liste d’infractions est en soit à saluer, il convient toutefois de signaler que notre législation pénale contiendra désormais plusieurs listes d’infractions permettant de recourir à l’une ou l’autre mesure procédurale, ce qui risque évidemment d’entraîner inévitablement des interférences et des confusions.

La lisibilité et la cohérence de notre législation pénale n’y gagneront rien.

La question principale est toutefois celle de savoir si les infractions énumérées au projet sont à considérer comme relevant toutes de „la criminalité grave“ visée par le point 51 de l’arrêt de la Cour de justice.

Celle-ci fait uniquement référence de manière précise au terrorisme et à la criminalité organisée.

Si la référence au terrorisme ne saurait en l’espèce donner lieu à difficultés, bien que la notion de „terrorisme“ ait obtenue, surtout ces derniers temps, des contours légaux de plus en plus flous.

La référence à la notion de „criminalité organisée“ est par contre bien plus difficile à cerner. Il s’agit en l’espèce bien plus qu’un concept relatif „modus operandi“ qu’à une infraction précise! L’existence même de ce concept est d’ailleurs régulièrement remise en cause. Il peut y avoir une criminalité organisée ayant pour objet des pommes de terre, des billes ou du chewing-gum!

A noter encore que les notions de „criminalité organisée“ recouvrent dans notre législation tant les „associations de malfaiteurs“ que les „organisations criminelles“ ont pour point commun qu’il s’agit

d'associations „en vue“ de commettre certains crimes ou délits. Il s'agit donc d'infractions par intention et non par commission.

La différence est de taille.

Reste alors l'hypothèse que la Cour de justice a eu en vue la notion de crime organisé dans son sens criminalistique, mais non juridique.

Les choses se compliquent par le fait que la Cour de justice retient tant aux points 43 que 51 que la rétention de données est un instrument utile dans la prévention des infractions et la lutte contre la criminalité et **notamment** la criminalité organisée.

En utilisant l'adverbe „notamment“ la C.J.U.E. admet le recours au repérage pour d'autres infractions d'une gravité incontestable.

Pour cette raison il convient d'examiner minutieusement la liste des infractions prévues au projet de loi, aux fins d'examiner si toutes les infractions y prévues peuvent bien être considérées comme étant d'une gravité particulière.

Cet exercice est par nature très difficile étant donné que la notion d'infraction grave n'est pas une notion juridique, et manque donc de la précision pourtant requise par principe en matière pénale. Par la force des choses la notion de „*criminalité grave*“ n'est dès lors pas objective mais subjective.

En application des articles 2, 3 et 4 de la C.E.D.H., signée à Rome le 4 novembre 1950 le droit à la vie (y compris la défense de toute personne contre la violence illégale) l'interdiction de la torture et l'interdiction de l'esclavage et du travail forcé sont indubitablement à considérer comme les droits de l'homme les plus fondamentaux, de même que toutes les atteintes à la vie et atteintes graves à l'intégrité physique.

Le système de la liste d'infractions montre d'ailleurs en l'espèce ses limites en ce qu'elle risque toujours d'être incomplète. Il est ainsi, à titre d'exemple, indiscutable que des infractions en rapport avec des réseaux de pédophilie relèvent de la criminalité grave, mais ne figurant pas sur la liste.

Qu'il y ait possibilité de repérage et de rétention de données dans ces cas de figure ne saurait donner lieu à discussion.

Pour les raisons exposées ci-avant les infractions énumérées au point 2) de l'article premier de la loi sous examen et portant modification de l'article 67-1 sous 3), 4), 18), 19), 20), 21), 30) et 33) doivent figurer sans aucun doute sur la liste des infractions susceptibles de faire l'objet d'une mesure de repérage.

Il devrait en être de même pour les infractions énumérées sous 1), 7), 13), 23) et 29).

Par contre pour les infractions énumérées aux points 8), 9), 10), 11), 15), 17), 25), 26), 27), 28) et 31) il s'agit d'infractions ayant exclusivement pour objet l'appropriation d'objets matériels. En l'espèce à titre d'illustration, de ce que les listes d'infraction sont toujours incomplètes, la question se pose encore pourquoi, à titre d'exemple, le délit d'initiés n'y figure pas.

S'agit-il en l'espèce et par principe d'infraction d'une gravité objective réelle?

Voilà bien le problème.

Si l'on se place du côté des droits de l'homme et de la philosophie sous-jacente de l'arrêt de la Cour de justice on devrait conclure à ce que ces infractions ne sauraient faire l'objet d'une mesure de repérage.

Par contre si l'on estime qu'il y a lieu de sanctionner l'appropriation illicite de biens et de s'assurer à cette fin de tous les moyens de preuves techniquement disponibles l'on n'hésitera pas à trouver évident que les auteurs de ces infractions puissent faire l'objet d'une mesure de repérage.

Dans ce contexte, il importe de relever que la Cour européenne des droits de l'homme a précisé en 2010 dans une affaire Uzun contre Allemagne (arrêt du 2 septembre 2010, n° 35623/05) que „*eu égard au risque d'abus inhérent à tout système de surveillance secrète, de telles mesures doivent se fonder sur une loi particulièrement précise, en particulier compte tenu de ce que la technologie disponible devient de plus en plus sophistiquée*“ (point 61 de l'arrêt).

Les infractions énumérées sous 22), à savoir le harcèlement et les atteintes à la vie privée sont certes du point de vue de la victime d'une gravité subjective réelle. Mais peut-on les considérer comme étant d'une gravité objective réelle? Au moins un doute est permis.

Les infractions énumérées au point 14) et relatives à la cybercriminalité donnent lieu à une observation particulière.

En effet en application de l'article 3 de la loi du 18 juillet 2014 relative à la cybercriminalité (Mémorial A, 2014, n° 133, page 2134) au moins cinq infractions nouvelles ont été introduites dans notre code pénal qui ne sont cependant en rien énumérées dans le projet de loi sous examen.

Il s'y ajoute qu'au point 7) du même article 3 de la loi du 18 juillet 2014 on rend punissable ceux qui ont sciemment facilité, par tout moyen, la justification mensongère de la nature, de l'origine de l'emplacement, de la disposition, du mouvement ou de la propriété des biens visés à l'article 32-1 du code pénal, alinéa 1 premier sous 1), forment l'objet ou le produit, direct ou indirect, des infractions y visées.

Suit une longue, très longue liste d'infractions qui peuvent, en application de la disposition visée ci-avant, faire l'objet d'une mesure de repérage, à condition que l'origine des biens ait été trafiquée par un des moyens énumérés ci-avant.

Ceci n'est pas sans rappeler le fameux cheval de Troie.

Ce qui semble a priori important et impressionnant ce n'est pas le contenu mais le contenant!

Or, l'inverse est vrai.

Le fait à la base de bien matériel ou immatériel ce qui a ensuite été trafiqué quant à son origine est infiniment plus grave que le fait que par une manipulation informatique l'origine réelle du bien a illicitement été trafiqué.

Il ne semble d'ailleurs guère logique de ne pas permettre un repérage pour de nombreuses infractions, mais de le permettre si elles ont ensuite fait l'objet d'un acte de cybercriminalité.

Il résulte de l'examen de l'article visé qu'en fin de compte il ne saurait guère y avoir d'infractions ayant fait l'objet depuis l'entrée en vigueur de la loi du 30 mai 2005 d'une mesure de repérage qui ne figure pas dans l'énumération. La loi serait-elle, sur ce point, un coup d'épée dans l'eau?

Le soussigné fait encore siennes les observations purement juridiques contenues dans l'avis de la Cour Supérieure de Justice.

Ad article 2 point 4)

Aux termes de cette disposition „*les données visées*“ sont conservées sur le territoire de l'Union européenne.

Il est certes exact que la Cour de justice considère dans son arrêt que les données conservées ne sauraient quitter le territoire de l'Union européenne, mais ceci en raison du fait que la directive visée ne contient aucun contrôle avant la transmission de ces données à un territoire situé en dehors de l'Union européenne.

Or, à titre d'exemple, le Grand-Duché de Luxembourg s'apprête à ratifier le „*Memorandum of understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information*“ signé à Luxembourg le 20 juin 2012, qui prévoit la possibilité d'échanger les données telles que celles visées au projet.

Le projet de ratification prévoyant des mécanismes de contrôle, le texte proposé règle la situation pour notre pays.

Il y a donc lieu de reformuler la disposition visée.

Il s'entend d'ailleurs que dans un domaine comme le terrorisme l'échange de données au-delà des pays de l'Union européenne, est indispensable.

Aurait-on oublié, à titre d'exemple, que les auteurs des attentats du 11 septembre 2001 aux Etats-Unis vivaient avant les attentats, de manière cachée, en Allemagne?

Interdire de manière absolue le résultat d'un repérage n'est ni cohérent, ni raisonnable au regard du grave problème actuel du terrorisme.

Ad articles points 1) et 2)

Les dispositions ne donnent pas lieu à observation étant donné qu'elles tendent, à bon droit, à apporter des précisions à notre droit allant dans le sens préconisé par la Cour de justice dans l'arrêt visé.

Il se pose toutefois un autre problème assez délicat.

En effet à l'heure actuelle se trouve également dans la procédure législative le projet de loi n° 6675 portant notamment organisation du Service de Renseignement de l'Etat.

Or, aux termes de ce projet (tant du projet initial que du texte amendé présenté par le Gouvernement suite à l'avis du Conseil d'Etat):

„Le SRE est autorisé à procéder au repérage de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications“;

„en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou le fournisseur d'un service de télécommunications. La durée de cette mesure de recherche ne pourra se reporter qu'à une période maximale de six mois (...), sans préjudice de renouvellement (article 10, paragraphe (2), devenu article 7, paragraphe (2))“.

Selon l'article 67-1, paragraphe (1) alinéa 5 le juge d'instruction peut ordonner une mesure de repérage pour une durée d'un mois, également renouvelable.

La question qui mérite examen est celle de savoir si de par les renouvellements successifs les données ne sont pas retenues sur une période très longue, ce qui a, le cas échéant, pour conséquence que toutes les données collectées seront retenues très longtemps.

Il ne faut pas non plus perdre de vue que dans le genre de criminalité visé, on procède par algorithmes, c'est-à-dire, si on part de l'utilisateur. „A“, qu'on croit mêlé au terrorisme, on veut également savoir avec qui son correspondant „B“, est en relation, lequel est un contact régulier de „C“, etc., etc., pour voir finalement s'il y a également des relations entre, par exemple, „F“, „E“ et „A“, de sorte que toutes ces personnes sont soupçonnées d'être mêlées au terrorisme.

Pour cette raison il y a lieu de retenir toutes ces données puisqu'on recherche bien tous les contacts inconnus de „A“.

Pour cette raison on risque de retenir au-delà d'un délai de 6 mois une quantité énorme de données.

*

VI) OBSERVATIONS FINALES

En l'espèce il s'agit d'une importante question de politique criminelle, le concept étant pris en l'espèce au sens plein du mot, à savoir, pour reprendre la définition de Madame la Professeure Mireille Delmas-Marty:

„... elle (la politique criminelle) comprend l'ensemble des procédés par lesquels le corps social organise les réponses à la criminalité.

Son but essentiel est le maintien de l'ordre social. Elle consiste en des mesures préventives (éducation, famille, emploi, etc.) et des mesures répressives (emprisonnement, etc.). C'est un art difficile qui recherche l'équilibre entre l'efficacité de ces mesures et les effets pervers causés par elles, en particulier les atteintes aux droits et libertés fondamentaux des citoyens.“.

Il s'agit de faire un choix politique, notion prise au sens noble du terme. Ce choix s'opère entre les impératifs non conciliables de la liberté (entendue dans le présent contexte comme respect du droit à la vie privée) et de la sécurité.

Soit on cherche à élucider le plus grand nombre possible d'infractions⁵, soit l'on se limite, par respect, pour la protection de la vie privée, aux seules infractions portant atteinte aux valeurs essentielles pour permettre une vie commune.

La question est d'autant plus importante que le procédé visé est à la fois fort efficace pour trouver les auteurs d'infractions qu'invasive pour la vie privée des citoyens.

Une certaine modération semble se recommander pour les raisons exposées par la Cour de justice dans son arrêt „Digital Rights“.

Il s'entend que plus la liste des infractions se limite à des infractions réellement graves moins il y a lieu d'attacher une importance majeure aux problèmes de la durée de conservation des données.

Le Procureur général d'Etat,

Robert BIEVER

⁵ Sauf évidemment les infractions mineures, telles les contraventions.

CTIE – Division Imprimés et Fournitures de bureau

6763/05

N° 6763⁵

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

AVIS DE LA COMMISSION CONSULTATIVE DES DROITS DE L'HOMME DU GRAND-DUCHE DE LUXEMBOURG

(22.7.2015)

Conformément à l'article 2(1) de la loi du 21 novembre 2008 portant création d'une Commission consultative des droits de l'Homme au Grand-Duché de Luxembourg, la Commission consultative des droits de l'Homme (CCDH) a été saisie par le Gouvernement pour émettre un avis sur le projet de loi 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

*

I) CONSIDERATIONS GENERALES

Par son arrêt du 8 avril 2014¹, la Cour de justice de l'Union européenne (CJUE) a invalidé la directive 2006/24/CE relative à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, en s'appuyant sur les dispositions de la Charte des droits fondamentaux de l'Union européenne.

Il s'agit d'une décision clé, qui ne s'oppose pas seulement à la conservation générale et indifférenciée des données dans le cadre de la fourniture de services de communications électroniques, mais qui a aussi un impact sur de nombreuses autres mesures de conservation des données dans l'Union européenne².

Au Luxembourg, la directive 2006/24/CE a été transposée 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 criminelle³ et cette loi du 30 mai 2005 a encore été modifiée par la loi du 28 juillet 2011.⁴

Avant l'adoption de cette loi de 2010, la CCDH a adressé ses observations au législateur dans son avis 02/2010⁵.

1 CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12

2 Pour plus d'informations, voir: Prof. Dr. Franziska Boehm and Prof. Dr Mark D. Cole, Data Retention after the Judgement of the Court of Justice of the European Union (30.6.2014), disponible sur http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/Data/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

3 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. Mémorial A, n° 122, 29 juillet 2010

4 Projet de loi 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

5 CCDH avis 02/2010 sur le projet de loi 6113

Dans son arrêt dit „Digital Rights“, la CJUE a jugé que la directive 2006/24 comporte „une ingérence dans ces droits fondamentaux d’une vaste ampleur et d’une gravité particulière dans l’ordre juridique de l’Union sans qu’une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu’elle est effectivement limitée au strict nécessaire“ (point 65). Elle a en outre posé plusieurs exigences relatives aux mesures de sécurité nécessaires pour assurer la protection des données conservées.

Le présent projet de loi a pour objectif d’adapter la législation luxembourgeoise à ces exigences.

Alors que la directive européenne a été invalidée par la CJUE, les législations nationales restent en place et continuent à être appliquées. Voilà pourquoi la CCDH salue l’initiative du Gouvernement luxembourgeois de réagir comme un des premiers pays à cet arrêt de la CJUE en modifiant la législation actuelle, sans attendre les réactions au niveau de l’Union européenne.

Afin d’offrir une protection plus élevée aux citoyens, il n’en demeure pas moins qu’une position unifiée au niveau européen reste indispensable. A ce titre, la CCDH rappelle au Gouvernement l’engagement qu’il a pris de mettre la question sur l’agenda européen lors de la présidence luxembourgeoise du Conseil de l’Union européenne⁶ à défaut d’initiative de la part de la Commission européenne.⁷

Cependant, la CCDH regrette que le projet de loi se limite à des modifications ponctuelles et n’aborde pas du tout la question principale du maintien ou de l’abandon du principe même de la rétention des données, qui a pourtant été le sujet de nombreux débats en Europe.

1. Nécessité et utilité de la rétention des données

La conservation des données „concerne de manière globale l’ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s’applique donc même à des personnes pour lesquelles il n’existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves“. (point 58)

Elle place ainsi toute la population sous une sorte de soupçon généralisé et constitue une ingérence grave dans l’exercice du droit au respect de la vie privée et de la correspondance de toute personne. Or, une telle ingérence ne peut être justifiée que si elle est nécessaire, appropriée et proportionnée.

La Cour est arrivée à la conclusion que la directive poursuit le but légitime de la prévention des infractions et de la lutte contre la criminalité, mais que „le législateur de l’Union a excédé les limites qu’impose le respect du principe de proportionnalité“ (point 69).

La question de la nécessité, voire de l’utilité des mesures générales de conservation des données, n’a pas vraiment été analysée en profondeur dans l’arrêt „Digital Rights“. La CJUE note simplement que „la conservation de telles données peut être considérée comme apte à réaliser l’objectif poursuivi par ladite directive“ (point 49).

Or, comme le souligne la professeure Marie-Laure Basilien-Gainche „si l’on peut saluer le fait que le juge de Luxembourg n’ait pas considéré l’outil indispensable, on peut toutefois déplorer qu’il n’interroge pas un instant la prétendue utilité – pourtant sujette à caution – de la conservation des données électroniques pour lutter contre la criminalité organisée et le terrorisme“⁸.

6 2e semestre 2015

7 <http://www.europaforum.public.lu/fr/actualites/2015/02/gouv-chd-retention-donnees-cjue/index.html>

8 Marie-Laure Basilien-Gainche, „Une prohibition européenne claire de la surveillance électronique de masse“, La Revue des droits de l’homme [En ligne], Actualités Droits-Libertés, mis en ligne le 14 mai 2014, consulté le 12 mai 2015.
URL: <http://revdh.revues.org/746>

Ce sujet a pourtant été vivement discuté par de nombreux experts en matière de protection des données, et ceci aussi bien avant⁹ qu'après¹⁰ l'adoption de la directive 2006/24/CE.

Un point qui est souvent relevé est le manque de preuves limpides pour démontrer la nécessité de la conservation systématique et obligatoire des données électroniques. Ainsi, le rapport d'évaluation concernant la directive 2006/24/CE publié en 2011 par la Commission européenne¹¹, qui est arrivé à la conclusion que „la conservation de données est très utile aux systèmes de justice pénale et aux services répressifs de l'UE“, a été fortement critiqué¹² par le Contrôleur européen de la protection des données, qui a estimé que „la Commission se base principalement sur des déclarations des Etats membres sur leur perception de la conservation des données comme étant un outil nécessaire aux fins de la répression. Ces déclarations, cependant, indiquent plutôt que les Etats membres concernés sont heureux d'avoir des règles de l'UE sur la conservation des données“¹³, mais que „les informations quantitatives et qualitatives fournies par les Etats membres ne sont pas suffisantes pour confirmer la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données“¹⁴.

Dans le même ordre d'idées, il y a lieu de soulever l'exemple de l'Allemagne, qui est un des pays où la loi nationale transposant la directive 2006/24/CE a été déclarée inconstitutionnelle¹⁵.

Suite à cette décision de la Cour constitutionnelle, le ministre allemand de la Justice a décidé d'abandonner la conservation des données et a publié un rapport, réalisé par le Max-Planck Institut¹⁶, sur les conséquences de la suppression de cette conservation des données. Ce rapport est arrivé à la conclusion que l'absence d'une législation prévoyant la rétention des données n'a pas eu comme résultat une chute du nombre d'enquêtes criminelles résolues.

2. Mesures alternatives

Dans le cadre de cette discussion sur la nécessité de la conservation des données, il faut aussi considérer d'autres mesures utiles à prendre en compte à des fins d'enquête qui pourraient s'avérer comme des alternatives, car moins intrusives dans la vie privée. Le principal moyen alternatif qui est souvent invoqué est la conservation rapide des données (gel immédiat ou gel rapide). Cette méthode prévoit de „conserver temporairement ou de „geler“ certaines données de trafic des télécommunications et de localisation portant uniquement sur des personnes déterminées soupçonnées d'activités criminelles, qui peuvent par la suite être mises à la disposition des autorités répressives avec une autorisation judiciaire“.¹⁷

9 Groupe de travail „ARTICLE 29“ sur la protection des données. Avis 4/2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE (COM(2005)438 final du 21.9.2005), disponible sur http://www.cnpd.public.lu/fr/publications/groupe-art29/wp113_fr.pdf

Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE [COM(2005) 438 final], JO C 298 du 29.11.2005

10 Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)(2011/C 279/01);

Feiler, L., „The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection“, European Journal of Law and Technology. Vol. 1, Issue 3, 2010: Voir aussi la lettre datée du 22 juin 2010 d'un groupe important d'organisations de la société civile aux commissaires Malmström, Reding et Kroes,

<http://www.vorratsdatenspeicherung.de/content/view/363/158/lang.en>

11 Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE) (COM(2011) 225 final)

12 Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE) (2011/C 279/01)

13 Point 41 du texte p. 5

14 Point 44 du texte p. 6

15 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, jugement du 2 mars 2010 disponible sur

http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

16 Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung, http://vds.brauchts.net/MPI_VDS_Studie.pdf

17 Définition donnée dans l'avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE) (2011/C 279/01), point 54

Cette conservation rapide des données informatiques a été introduite en droit luxembourgeois par la loi du 18 juillet 2014¹⁸, par laquelle le Luxembourg a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité, et par son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

La conservation rapide des données „ne garantit pas la possibilité de remonter en amont de l'injonction, pas plus qu'elle ne permet de recueillir des preuves sur les mouvements des victimes ou des témoins d'une infraction, par exemple“¹⁹ et elle n'est utile que dans des situations où un suspect a été identifié. Cette méthode ne permet donc pas d'obtenir autant d'informations que le système général de la conservation des données, mais c'est exactement à cause de sa nature plus ciblée qu'elle est souvent jugée moins attentatoire aux droits fondamentaux.²⁰ Avant d'exclure cette méthode, parce qu'elle ne constitue pas une alternative exactement équivalente, il serait opportun de voir si elle pourrait produire des résultats comparables.

La CCDH estime qu'il faudrait évaluer si la conservation des données est non seulement utile pour les enquêtes criminelles, mais effectivement un outil absolument indispensable pour la lutte contre le terrorisme et la criminalité organisée et si des résultats comparables pourraient être obtenus avec des alternatives moins intrusives dans la vie privée de la population totale. Ces questions mériteraient indubitablement une discussion approfondie au Luxembourg, à l'instar d'autres pays européens comme l'Allemagne.

En attendant les développements futurs au niveau national aussi bien qu'au niveau européen, il est essentiel de limiter le champ d'application de la conservation des données au strict minimum et d'instaurer des contrôles suffisants permettant de protéger efficacement les données à caractère personnel contre les risques d'abus et les utilisations illicites.

*

II) ANALYSE DU PROJET DE LOI PAR LA CCDH

1. Liste limitative d'infractions graves

Dans son article 1er, le projet de loi sous avis propose de remplacer à l'article 67-1 du Code d'instruction criminelle le seuil de peine des infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs (infractions prévoyant une peine privative de liberté dont le maximum est égal ou supérieur à un an) par une liste précise d'infractions.

La CCDH avait déjà recommandé dans son avis 02/2010²¹ sur le projet de loi 6113 d'opter pour une liste d'infractions bien concise au lieu de la définition d'un seuil minimal de peine prévue.

La Commission nationale pour la protection des données (CNPD) avait aussi opté en faveur d'une liste d'infractions.²²

Alors qu'en 2010, le législateur n'avait pas retenu cette recommandation, les auteurs du présent projet de loi ont choisi d'intégrer une liste d'infractions dans l'article 67-1 du Code d'instruction criminelle.

18 Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, Mémorial A n° 133, 25 juillet 2014

19 Rapport d'évaluation concernant la directive sur la conservation des données, p. 6

20 Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données

21 CCDH avis 02/2010 sur le projet de loi 6113

22 Avis de la Commission nationale pour la protection des données sur le projet de loi et sur le projet de règlement grand-ducal déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics, 26 avril 2010

http://www.cnpd.public.lu/fr/decisions-avis/2010/retention-donnes/avis_CNPD_projet_loi_6113.pdf

Or, il s'agit en l'espèce d'une liste assez extensive qui comprend 33 infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs.

Cette liste contient entre autres des infractions comme le trafic illicite de biens culturels, les infractions contre l'environnement, l'incendie volontaire, le harcèlement et les atteintes à la vie privée, les homicides et coups et blessures volontaires.

Il convient de rappeler que dans son arrêt „Digital Rights“, la CJUE a souligné que la conservation des données, telle que prévue par la directive 2006/24/CE, comporte une ingérence dans les droits fondamentaux des citoyens européens „sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire“ (point 65). Et elle a noté qu'il faut prévoir des limitations à l'utilisation de ces données conservées „concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence“ (point 60).

Dans son avis en 2010, la CCDH avait déjà proposé de se limiter aux infractions suivantes:

- Les actes de terrorisme prévus par les articles 135-1 à 135-16 du Code pénal,
- L'association de malfaiteurs et le crime organisé, tels que prévus par les articles 322 et suivants du Code pénal, ainsi que la circonstance aggravante de l'association de malfaiteurs prévue spécifiquement en matière de trafic de stupéfiants par la loi modifiée du 19 février 1973, concernant la lutte contre la toxicomanie.

Comme le projet de loi ainsi que les textes précédents (projet de loi 6113 et la directive 2006/24/CE) se placent dans un contexte de lutte contre le terrorisme et la criminalité organisée, la CCDH est d'avis que les infractions qui se trouvent sur la liste sous avis ne sont pas toutes „suffisamment graves pour justifier une telle ingérence“. Par conséquent, il vaudrait mieux limiter l'accès aux données conservées pour les infractions qui se situent clairement dans ce contexte et raccourcir cette liste pour ne garder que le strict nécessaire.

2. La sécurité et la protection des données

Dans l'arrêt précité, la CJUE émet plusieurs exigences pour les règles visant la sécurité des données conservées par les fournisseurs de services de communication électroniques, sachant que ces règles doivent permettre „d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que tout accès et toute utilisation illicites de ces données“ (point 66).

a) Effacement des données à l'expiration du délai de rétention

La CCDH est satisfaite de constater que les auteurs du texte tiennent compte des exigences exprimées au point 67 de l'arrêt en proposant au point 2) de l'article 2 du projet de loi de modifier l'article 5 (1) (b) de la loi du 30 mai 2005 afin de préciser que les données retenues doivent être effacées irrémédiablement et sans délai à l'expiration du délai de rétention. Il ne sera donc plus possible de sauvegarder ces données sous une forme anonymisée après la fin de la durée de rétention.

b) Conservation des données sur le territoire de l'Union européenne

Le point 4) de l'article 2 du projet de loi prévoit de modifier l'article 5-1 de la loi modifiée du 30 mai 2005 en créant l'obligation de conserver les données concernées par les articles 5 et 9 sur le territoire de l'Union européenne. Il s'agit d'une exigence exprimée au point 68 de l'arrêt de la CJUE, qui l'estime nécessaire afin de garantir le contrôle par une autorité indépendante. Ce contrôle constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel.

Or, les coûts de stockage des données pour les fournisseurs, surtout ceux d'une taille moyenne et petite, n'étant pas négligeables, il a souvent été proposé de réfléchir à accorder des compensations

financières étatiques aux fournisseurs.²³ Dans ce contexte, il est important d'assurer un contrôle effectif du respect des obligations imposées aux fournisseurs.

La CCDH regrette de constater que la question de la sécurité des données n'est abordée que par renvoi à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à un règlement grand-ducal qui n'a d'ailleurs pas été soumis à l'avis de la CCDH.

Elle estime que les mesures de sécurité principales devraient être inscrites dans le présent projet de loi.

c) Augmentation des sanctions en cas de la violation des obligations

Les points 3) et 7) de l'article 2 du projet de loi proposent de modifier les articles 5(6) et 9(6) de la loi du 30 mai 2005 en vue d'augmenter les peines d'emprisonnement prévues. Celles-ci seront augmentées de „huit jours à un an“ à „six mois à deux ans“.

Le commentaire précise que le but de cette modification est „d'augmenter le caractère dissuasif de cette peine et de souligner ainsi l'importance accordée à la protection de ces données“.

Il ne s'agit en l'espèce pas d'une revendication formelle de la CJUE, mais d'une initiative du Gouvernement.

Dans son avis en 2010, la CCDH a déjà insisté sur l'importance de sanctions (y compris de sanctions administratives et pénales) efficaces, proportionnées et dissuasives.

Elle est satisfaite de constater que la loi de 2011 a introduit des sanctions administratives (avertissement et amende administrative) dans l'article 3 (3) de la loi de 2005, permettant ainsi à la CNPD de réagir en cas de manquement à l'obligation de notification des violations de données de la part du fournisseur.

Pourtant, elle estime qu'il ne suffit pas d'alourdir les sanctions afin de garantir la sécurité et la protection des données, comme le réclame la CJUE. Il est essentiel de garantir leur mise en oeuvre effective en cas de violation de la loi.

D'ailleurs, afin de garantir un contrôle efficace de la protection des données, il importe d'accorder les moyens nécessaires à la CNPD, qui est responsable d'assurer le respect des dispositions de la loi modifiée du 30 mai 2005.

La CCDH entend formuler les recommandations suivantes:

1. Une évaluation de la nécessité absolue de la conservation des données doit être faite et des méthodes alternatives doivent être considérées.
2. La liste des infractions doit se limiter au strict nécessaire et inclure seulement des infractions qui se situent dans le contexte de la lutte contre le terrorisme et la criminalité organisée.
3. Des sanctions efficaces, proportionnées et dissuasives doivent effectivement être mises en oeuvre.
4. La CNPD doit obtenir les moyens nécessaires pour effectuer un contrôle régulier du respect de la loi.

²³ Cecilia Malmström, „Taking on the Data Retention Directive“, SPEECH/10/723, European Commission conference, Brussels, 3 December 2010; SURVEILLE, Comparative law paper on data retention regulation in a sample of EU Member States, 30.4.2013

Voir aussi la lettre datée du 22 juin 2010 d'un groupe important d'organisations de la société civile aux commissaires Malmström, Reding et Kroes.

CTIE – Division Imprimés et Fournitures de bureau

6763/06

N° 6763⁶

CHAMBRE DES DEPUTES

Session ordinaire 2015-2016

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

**AVIS DE L'ORDRE DES AVOCATS DU BARREAU
DE LUXEMBOURG**

(13.10.2015)

Le Conseil de l'Ordre a été invité à exprimer son avis sur un projet de loi ayant pour objet l'adaptation du dispositif légal national relatif à la conservation des données de communications électroniques à des fins de poursuite pénale.

Le Conseil de l'Ordre a pris connaissance de l'avis de la Chambre de Commerce du 13 février 2015, de l'avis de la Commission Nationale pour la Protection des Données du 19 juin 2015, de l'avis du Conseil d'Etat du 10 juillet 2015 et de l'avis de la Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg du 22 juillet 2015.

Le projet de loi fait suite à l'arrêt *Digital Rights*¹ rendu par la Cour de Justice de l'Union Européenne (CJUE) qui a jugé invalide la Directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

Fruit du contexte post 11 septembre 2001, cette directive imposait notamment aux fournisseurs de services de communication électroniques de conserver, pour une durée allant de six à vingt-quatre mois, des données de trafic permettant d'identifier l'émetteur et le destinataire d'une communication, sa durée et localisation pour la recherche et la constatation d'infractions pénales graves. En revanche, elle n'autorise pas la conservation du contenu de la communication et des informations consultées. Or, „*ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.*“²

C'est donc dans son respect des droits fondamentaux, du droit au respect de la vie privée (article 7 de la Charte des Droits Fondamentaux de l'Union Européenne (la Charte)) et de celui de la protection des données à caractère personnel (article 8) que la validité de la Directive 2006/24/CE était mise en cause par la CJUE. Fondant son raisonnement sur la Charte des Droits Fondamentaux de l'Union Européenne la Cour a notamment jugé disproportionnée l'obligation de conservation des données qui s'applique de manière générale sans exiger un lien, fût-il indirect, entre la personne dont les données sont conservées et un risque d'infraction³ (point sur lequel nous reviendrons dans le présent avis).

1 CJUE (gr. Ch.) 8 avril 2014, aff. Jtes C-293/12 et C-594/12, *Digital Rights Ireland Ltd & Kärntern Landesregierung, Seitlinger, Tschohl et a.*

2 *ibid* point 27

3 *ibid* point 58

La CJUE fait également grief à la Directive 2006/24/CE de ne prévoir aucun critère permettant de délimiter l'accès des autorités nationales aux données⁴, ni aucune distinction entre les catégories de données, les personnes concernées ou quelque autre critère objectif quant à la durée de conservation⁵.

Le présent avis traitera dans un premier temps de la protection des personnes soumises selon les lois nationales au secret professionnel (I), puis émettra un avis sur le principe de collecte *a priori* et de conservation généralisées des données sans que la personne concernée ait participé directement ou indirectement à une infraction (II). Enfin le Conseil de l'Ordre analysera les autres dispositions prévues par le Projet de loi (III).

I. La protection du secret professionnel

Il est à noter que dans son arrêt *Digital Rights*, la CJUE fait expressément référence au secret professionnel pour lequel la Directive 2006/24/CE *aurait dû prévoir une exception*⁶. Le projet de loi ne répond pas à cette question fondamentale de préservation du secret professionnel en ne prévoyant aucune exception à la collecte et la rétention des données pour les personnes soumises à celui-ci.

Or, le secret professionnel de l'avocat repose sur de nombreuses normes impératives, qu'il s'agisse de prescriptions légales pénalement sanctionnées ou de règles déontologiques. Il est protégé par la Cour Européenne des Droits de l'Homme qui le définit comme „la base de la relation de confiance qui existe entre l'avocat et son client⁷ 8“ et érigé comme norme communautaire par la CJUE⁹. Le secret professionnel de l'avocat est d'ordre public et ceci dans l'intérêt du client. Il est général, absolu et illimité dans le temps¹⁰ et il participe à l'Etat de droit. Il couvre toutes les confidences que l'avocat a pu recevoir à raison de son état ou de sa profession. Sont ainsi couverts par le secret les informations reçues du client, celles reçues de tiers dans le cadre du dossier concernant ce client, mais également, et il convient de le rappeler pour la présente, le nom du client ainsi que l'agenda de l'avocat¹¹.

Le projet de loi vise la rétention des données relatives au trafic et à la localisation. Ces données désignent les informations liées à l'utilisation des réseaux et permettent d'identifier les interlocuteurs, leur localisation et la durée de leur communication. Si comme rappelé précédemment la conservation du contenu des communications électroniques et des informations consultées n'est pas visée ni par la loi de transposition de la Directive invalidée, ni par le présent Projet de loi commenté, il n'en demeure pas moins que les données relatives au trafic et à localisation collectées permettent d'identifier les interlocuteurs de l'avocat. Les déplacements précis, noms des personnes en correspondance avec l'avocat, donc de ses clients, lieux et dates de rencontre de l'avocat avec ses contacts sont autant d'éléments protégés par le secret professionnel de l'avocat.

Si le secret professionnel peut connaître des exceptions, celles-ci ne peuvent pas, à l'image de celles prévues pour les écoutes téléphoniques ou perquisitions¹², porter atteinte au secret de manière disproportionnée par rapport au but poursuivi et doivent s'accompagner de garanties procédurales particulières.

En ce sens le Conseil de l'Ordre se range derrière les avis du Conseil d'Etat du 10 juillet 2015 et de la Commission Nationale pour la Protection des Données (CNPD) du 19 juin 2015 et recommande l'insertion à l'article 67-1 du Code d'instruction criminelle d'une exception analogue à celle existant en matière d'écoutes téléphoniques qui dispose que „*les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes elles-mêmes de tenter de commettre ou d'avoir commis ou tenté de commettre l'infraction comme auteurs ou complices, ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le chef du service de renseignements.*“ (Article 88-4 du Code d'instruction criminelle).

4 *ibid* point 60

5 *ibid* point 63

6 *ibid* point 58: „En outre, elle (la Directive 2006/24/CE) ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel“

7 CEDH Cour EDH, 5e Sect. 24 juillet 2008, André et autres c. France, Req. n° 18603/03, point 41

8 Article 7.1.2 du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg

9 CJCE, 18 mai 1982, A.M. & S. c/ Commission des Communautés européenne, Aff. 155/79, Rec, p. 1575.

10 Article 7.1.1 du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg

11 Article 7.1.3. du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg

12 CEDH, 16 décembre 1992, Niemietz c. Allemagne.

Le Conseil de l'Ordre seconde la proposition du Conseil d'Etat d'insérer entre l'actuel paragraphe 3 de l'article 67-1 du Code d'instruction criminelle et le paragraphe 4 projeté, qui deviendrait alors le paragraphe 5, un paragraphe 4 s'inspirant du paragraphe 4 de l'article 88-1 du Code d'instruction criminelle, libellé comme suit:

„(4) Les mesures visées à l'alinéa (1) 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.“

Toujours afin d'assurer la protection du secret professionnel, le Conseil de l'Ordre est d'avis que la modification suivante devrait être apportée au paragraphe 2 de l'article 67-1 du Code d'instruction criminelle, comme suit:

„(2) Chaque opérateur de télécommunications et chaque fournisseur d'un service de télécommunications communique les informations qui ont été demandées dans les meilleurs délais. Toutefois, les informations qui relèvent du secret professionnel, au sens de l'article 458 du Code pénal, et notamment celles relatives au destinataire des appels, ne peuvent être communiquées, sauf si le dépositaire d'un tel secret est lui-même suspecté d'avoir commis l'infraction.“

Enfin, le Conseil de l'Ordre est également favorable à la proposition de la CNPD d'insérer une exception analogue pour les personnes soumises au secret professionnel à l'article 10 paragraphe (2) du projet de loi n° 6675 portant organisation du Service de Renseignement de l'Etat¹³. Cet article autorise le Service de Renseignement de l'Etat à procéder au repérage de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de télécommunications. Le Conseil de l'Ordre estime que le secret professionnel doit être protégé dans cette législation.

II. La problématique de la conservation a priori indifférenciée et massive de données personnelles

La CJUE, dans son arrêt *Digital Rights* reconnaît l'ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte que constitue la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci. Si la Cour juge l'ingérence justifiée en ce qu'elle répond à un objectif d'intérêt général, elle la considère cependant non proportionnée notamment par ses reproches aux points 58 et 59.

La Cour reproche dans un premier temps à la Directive 2006/24 d'être dirigée contre l'ensemble des utilisateurs des services de communication sans qu'un lien direct ou indirect avec la commission d'une infraction ne soit exigé.

Le point 58 de l'arrêt *Digital Rights* affirme en ce sens que: *„la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves“*.

Dans un deuxième temps la CJUE fait grief à la Directive 2006/24 de ne faire aucun lien entre les données conservées et une menace pour la sécurité publique et de ne prévoir aucune limite temporelle, géographique ou humaine à cette collecte.

Le point 59 de l'arrêt *Digital Rights* affirme en ce sens que: *„D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une*

¹³ *Projet de loi n° 6675 1) portant organisation du Service de Renseignement de l'Etat; 2) modifiant la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat, la loi du 31 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, le Code d'Instruction criminelle, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, et la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Ledit projet de loi a été déposé à la Chambre des Députés comme projet de loi n° 6675 en date du 2 avril 2014.*

zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves".

Le Conseil de l'Ordre regrette que si le projet de loi prévoit notamment des mesures limitant l'accès à ces données et relatives à la durée et à la localisation de la conservation, il ne répond pas formellement à ces critiques relatives à la conservation a priori, généralisée et indiscriminée des données relatives au trafic et à la localisation. Par conséquent, il n'est pas exclu que le Projet continue à se voir critiquer en justice pour ne pas avoir pris en considération l'entièreté des critiques de la CJUE.

Les Professeurs de droit Dr. Franziska Boehm de l'Université de Münster et Dr. Mark D. Cole de l'Université de Luxembourg concluent, dans leur rapport *Conservation des données après l'arrêt de la Cour de Justice de l'Union Européenne*¹⁴, que la conservation généralisée des données de personnes non suspectes pour une utilisation future à des fins répressives est contraire aux articles 7 et 8 de la Charte des Droits Fondamentaux de l'Union Européenne dès lors qu'il n'est pas possible d'établir un lien entre les données conservées et une menace à la Sécurité Publique¹⁵. La lutte contre le terrorisme et la criminalité organisée sont des combats louables en cette période de tension et de menaces internationales. Cependant, elle ne peut justifier des atteintes inutiles, inadéquates et inappropriées aux droits fondamentaux des citoyens européens. D'autres auteurs, dont Bernard Glandz¹⁶ et Christofi, voient dans les développements de l'arrêt *Digital Rights* le rejet de toute collecte massive de données et la nécessité de remettre en cause le travail législatif¹⁷ dans son entièreté.

Le Conseil de l'Ordre rejoint donc l'avis de la Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg en ce qu'il est regrettable que les rédacteurs du Projet de loi n'abordent pas les justifications du maintien de la conservation généralisée des données et ne répondent pas aux critiques de la CJUE visées aux points 57 et 58 de l'arrêt *Digital Rights*.

Il convient de s'interroger sur l'adéquation d'une telle mesure avec la recherche et la poursuite des infractions. La Commission consultative des Droits de l'Homme du Grand-Duché de Luxembourg fait état de l'exemple allemand dont le Tribunal constitutionnel fédéral a déclaré inconstitutionnelle la loi nationale transposant la Directive 2006/24/CE. Suite à cette décision, le Ministre allemand de la Justice a décidé d'abandonner la conservation des données et a publié un rapport, réalisé par le Max-Planck Institut, sur les conséquences de la suppression de cette conservation des données. Ce rapport est arrivé à la conclusion que l'absence d'une législation prévoyant la rétention des données n'a pas eu comme résultat une chute du nombre d'enquêtes criminelles résolues.

Le Conseil de l'Ordre rejoint également l'avis de la Commission consultative des Droits de l'Homme qui préconise une analyse approfondie des mesures alternatives à cette obligation de conservation généralisée comme la collecte rapide (dite gelée) des données qui concerne seulement les personnes soupçonnées d'avoir directement ou indirectement participé à la commission d'une infraction telle que déjà prévue intégrée dans notre législation par la loi du 18 juillet 2014 sur la Cybercriminalité¹⁸.

14 Dr. Franziska Boehm, Dr. Mark D. Cole, *Data Retention after the Judgment of the Court of Justice of the European Union*, Münster/Luxembourg, 30 juin 2014.

15 „The study has demonstrated the impact of the Data Retention Directive Judgment on data protection and privacy in the Law Enforcement sector and on other data retention measures. Essential is that blanket retention of data of unsuspecting persons for the later use for Law Enforcement is not in line with Article 7 and 8 of the Charter of Fundamental Rights of the European Union since it is not possible to establish a link between the data retained and a threat to public security“.

16 Christophe Bernard-Glandz, *Les arrêts Digital Rights Ireland et Google Spain, ou le printemps européen de la protection des données*, C.D.E. 2014/3, pp. 685-717

17 A. Christofi, „Arrêt Digital Rights Ireland“, *Revue du droit de l'Union européenne*, 2014, pp. 399-406.

18 Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

III. Autres Dispositions

Pour les autres dispositions traitant notamment de la durée de conservation, de la conservation des données sur le Territoire Européen, de l'obligation de destruction à l'expiration de la durée de conservation légale et limitant l'accès des autorités compétentes aux cas de commission d'infraction prévues dans une liste exhaustive de 33 infractions, le Conseil de l'Ordre se range à l'avis du Conseil d'Etat sans y apporter d'autres commentaires.

13 octobre 2015

(signature)

CTIE – Division Imprimés et Fournitures de bureau

6763/07

N° 6763⁷

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

ARRETE GRAND-DUCAL DE RETRAIT DU ROLE DES AFFAIRES DE LA CHAMBRE DES DEPUTES

(29.3.2023)

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

Sur le rapport de Notre Ministre de la Justice et après délibération du Gouvernement en Conseil ;

Arrêtons :

Article unique.— Notre Ministre de la Justice est autorisée à déposer en Notre nom à la Chambre des Députés le projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Palais de Luxembourg, le 29 mars 2023

La Ministre de la Justice,
Sam TANSON

HENRI

*

Impression: CTIE – Division Imprimés et Fournitures de bureau



Commission juridique

Procès-verbal de la réunion du 09 mars 2016

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 24 février 2016
2. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques
 - Désignation d'un rapporteur
 - Continuation de l'examen de l'avis du Conseil d'Etat
3. 6908 Projet de loi sur la reconnaissance du mariage au Grand-Duché de Luxembourg et modifiant le Code civil
 - Rapporteur: Madame Viviane Loschetter
 - Présentation et adoption d'un projet de rapport
4. 6820 Projet de loi portant modification : 1) de la loi du 29 mars 2013 relative à l'organisation du casier et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne, 2) du Code d'instruction criminelle, 3) du Code pénal
 - Rapporteur: Madame Josée Lorsché
 - Examen des avis (*cf. documents transmis par courrier électronique en date du 28 janvier 2016*)
 - Présentation et adoption d'une proposition d'amendements parlementaires
5. Divers

*

Présents : M. Marc Angel, Mme Simone Beissel, M. Eugène Berger, M. Alex Bodry, M. Franz Fayot, M. Léon Gloden, Mme Josée Lorsché, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth

Mme Nancy Carier, Mme Claudine Konsbruck, M. Luc Reding, du Ministère de la Justice

Mme Marie-Jeanne Kappweiler, Avocat général

M. Laurent Besch, M. Christophe Li, de l'Administration parlementaire

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission

*

1. Approbation du projet de procès-verbal de la réunion du 24 février 2016

Le projet du procès-verbal de la réunion du 24 février 2016 a été approuvé unanimement par les membres de la Commission.

2. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Désignation d'un rapporteur

Les membres de la Commission juridique ont désigné Mme Viviane Loschetter comme rapportrice du projet de loi 6763.

Remarques introductives

Mme la Rapportrice résume les problématiques discutées lors de la réunion jointe entre la Commission juridique et la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace, en date du 21 octobre 2015. Pour le détail, il est prié de se reporter au procès-verbal de ladite réunion jointe (P.V. J01 et P.V. ERMCE 01).

Le représentant du Ministre de la Justice donne à considérer qu'une solution européenne, en matière de rétention de données, n'est probablement pas envisageable dans le futur proche. Il explique qu'aucune proposition de directive visant à remplacer la directive invalidée 2006/24/CE n'a été présentée jusqu'à présent. Un groupe de travail spécial en matière de conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuites des infractions graves, a été créé au sein du Conseil de l'Union européenne, dans le cadre de la Présidence du Conseil de l'Union européenne par les Pays-Bas. L'orateur énonce que le Ministère de la Justice préconise une solution européenne, cependant, malgré qu'il est difficile à l'heure actuelle de trouver un compromis au sein des différents Etats membres de l'Union européenne.

Examen de l'avis du Conseil d'Etat

Le représentant du Ministre de la Justice donne à considérer qu'il s'agit d'une matière très technique ayant trait aux technologies de l'information et de la communication. Il énonce que des changements mineurs, au niveau du vocabulaire utilisé, risque d'avoir des répercussions considérables sur l'ensemble du projet de loi.

Nouvel article 2 (article 1^{er} initial) – modification de l'article 67-1 du Code d'instruction criminelle

- Infractions pouvant justifier un accès aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs - liste d'infractions

Le représentant du Ministre de la Justice rappelle que le Conseil d'Etat a, à juste titre, soulevé que le choix entre un seuil des peines ou une liste exhaustive des infractions, pouvant justifier l'accès des autorités judiciaires aux données personnelles de communication (métadonnées) retenues par les opérateurs de télécommunications, constitue essentiellement un choix politique et que la Commission juridique s'est prononcée en faveur de l'établissement d'une liste exhaustive des infractions. Cette discussion a déjà été menée lors de la réunion du 21 octobre 2015.

Le Conseil d'Etat propose d'insérer une notion générique de « *toutes les infractions qualifiées de crime par la loi* » pour ne maintenir dans la liste que des infractions qualifiées de délits que les auteurs jugent opportun d'y insérer.

L'orateur rappelle également que le projet de loi sous examen vise à légiférer sur les conditions selon lesquelles les autorités judiciaires peuvent avoir recours aux données personnelles de communication (métadonnées) retenues par les fournisseurs et opérateurs de télécommunications.

Le représentant du Ministre de la Justice explique, suite à une question posée par un représentant du groupe politique CSV relative à l'origine de la liste exhaustive contenue dans le projet de loi, que la liste exhaustive proposée telle qu'elle figure actuellement sous l'article 2, point 2 (insertion d'un nouveau paragraphe 4 à l'article 67-1 du Code d'instruction criminelle), est issue de l'annexe D de la directive européenne 2014/41/UE du 3 avril 2014.

Le représentant du Ministre de la Justice se réfère à l'avis du Conseil d'Etat et estime qu'il serait judicieux de créer une liste spécifique dans le cadre de ce projet de loi et de ne pas se fonder sur une liste préexistante figurant dans le Code d'instruction criminelle. Il justifie cette démarche par le fait que la finalité de cette liste différera des listes préexistantes. Il énonce qu'il serait utile, dans le cadre de la coopération judiciaire internationale, de se fonder sur une liste émanant de ladite directive européenne.

Il échet de noter que la liste ne contient pas toutes les infractions (ni tous les crimes) inscrites dans notre Code pénal.

Madame la Rapportrice énonce que pour certains crimes, dont la gravité n'est pas contestée, la question de l'opportunité à insérer le crime sur ladite liste se pose.

Le représentant du Parquet général énonce que pour beaucoup de crimes, il serait utile, dans le cadre des enquêtes, à pouvoir recourir aux métadonnées afférentes.

Madame la Rapportrice constate, en ce qui concerne les crimes, que la question de la détermination des faits criminels devant figurer dans ladite liste, en combinaison avec une énumération exhaustive des délits, n'est pas encore résolue.

Le représentant du Ministre de la Justice propose, au sujet des délits à retenir dans la liste et par rapport à la suggestion du Conseil d'Etat, d'en discuter avec les représentants du Parquet général. La liste définitive sera soumise, pour discussion et approbation, aux membres de la Commission juridique. [ministère de la Justice]

- La protection des données de personnes soumises à un régime de protection spéciale en raison de leur secret professionnel

Le représentant du Ministre de la Justice résume la problématique soulevée par le Conseil d'Etat en matière d'accès par les autorités judiciaires aux données retenues relatives à des communications couvertes par le secret professionnel. A priori, une disposition excluant du

champ d'application du présent projet de loi les personnes soumises au secret professionnel lui semble possible.

Il précise que les métadonnées faisant l'objet d'une retenue par les fournisseurs et opérateurs de télécommunication ne permettent pas de connaître le contenu des communications échangées.

Un membre du groupe politique CSV s'interroge comment les autorités judiciaires peuvent faire abstraction, par exemple dans le cadre d'un échange de courriels, du fait que cet échange de courriels pourrait se dérouler par exemple entre un avocat, personne couverte par le secret professionnel, et son mandant. Il y voit un risque pour la garantie du caractère confidentiel des conversations entre un avocat et son mandant.

Le représentant du Ministre de la Justice rappelle d'abord qu'il est question de métadonnées et non pas du contenu des communications. Il estime cependant qu'il serait opportun, par analogie à la mise en œuvre des « *écoutes téléphoniques* » (articles 88-3 et 88-4 du Code d'instruction criminelle), de se renseigner également auprès des autorités judiciaires à ce sujet et de présenter des explications supplémentaires lors d'une prochaine réunion.
[Ministère de la Justice]

- Blanchiment d'argent

Le représentant du Ministre de la Justice note que la critique du Conseil d'Etat relative à la non inscription du blanchiment de fonds provenant du trafic de stupéfiants semble erronée, comme la liste telle que proposée par le projet de loi, contient dans son nouvel article 2 (article 1^{er} initialement) point 12 une disposition spécifique au « *blanchiment des produits du crime et recel* ».

Nouvel article 1^{er} (article 2 initial) – modification de la loi du 30 mai 2005

Point 2) – article 5, paragraphe 1^{er}, point (b) - Suppression de manière irrémédiable des données de télécommunication retenues

Le représentant du Ministère de la Justice précise que les données en question sont supprimées de manière irrémédiable après l'écoulement du délai légal.

Point 3) – modification de l'article 5, paragraphe 6 - Dispositions pénales

Le représentant du Ministre de la Justice énonce que cette disposition, en ce qu'elle prévoit des peines d'emprisonnement plus sévères, en cas de violation des dispositions inscrites à l'article 5 de la loi du 30 mai 2005, se justifie par l'importance accordée à la protection des données à caractère personnel.

Mme la Rapportrice propose de maintenir ce régime et renvoi à sa fonction dissuasive.

Un membre du groupe politique CSV estime qu'un accès non-autorisé auxdites données, suivi d'une diffusion de ces données, pourrait s'avérer dramatique pour la victime. Dans ce cas, il faudrait éventuellement aggraver la sanction pénale.

Il pose une question quant à la différence des sanctions pénales prévues par la loi modifiée du 2 août 2002 relative à la protection des données et celles inscrites dans la loi modifiée du 30 mai 2005 relative à la protection de la vie privée dans le secteur des télécommunications.

Il estime qu'il serait utile de prendre d'abord connaissance des infractions sanctionnées pénalement par une peine d'emprisonnement de « huit jours à un an », avant de prévoir des sanctions supplémentaires.

Le représentant du Ministre de la Justice propose d'établir un tableau synoptique reprenant les agissements qui sont sanctionnés pénalement dans le cadre de ces deux lois. [Ministère de la Justice]

Echange de vues

Nécessité d'un règlement grand-ducal

- ❖ Le représentant du Ministre de la Justice explique que certains détails qui sont de nature technique, seront réglés par voie d'un règlement grand-ducal. Il rappelle qu'il est courant dans le domaine des télécommunications de régler certaines questions de détails par voie réglementaire. Il énonce que cette procédure présente l'avantage à ce que la loi ne devrait pas être modifiée à chaque fois, suite aux évolutions technologiques fréquentes dans le domaine des télécommunications.

Il énonce qu'il s'agit essentiellement de questions liées au mode de stockage de ces données sur des serveurs informatiques et à l'emplacement de ces serveurs. Il fait référence à la réglementation applicable en matière de vidéosurveillance par la Police (VISUPOL).

- ❖ Madame la Rapportrice demande à ce que le projet d'un règlement grand-ducal afférent soit présenté à la Commission juridique une fois que le texte de loi soit finalisé.

Durée de rétention

- ❖ Madame la Rapportrice soulève le volet relatif à la durée de la rétention de ces données. Elle rappelle que l'article 5, paragraphe 1^{er} de la loi modifiée du 30 mai 2005 prévoit actuellement une durée de rétention de 6 mois. Elle pose la question de l'opportunité d'une diminution de cette durée à 3 mois, en soulignant que d'autres Etats membres de l'Union européenne ont déjà modifié leurs lois nationales dans ce sens.
- ❖ Le représentant du Ministre de la Justice donne à considérer que la durée de rétention des données est intimement liée à la procédure pénale applicable. Il rappelle que la loi nationale prévoit que seul le juge d'instruction, magistrat indépendant, peut autoriser un accès aux données de communication retenues, ce qui constitue une garantie procédurale supplémentaire. Il déconseille à diminuer la durée de rétention, en expliquant que lors des discussions internes préalablement menées entre le Ministre de la Justice, les autorités judiciaires et les autorités policières, les dernières se seraient prononcées favorablement à un maintien de la durée de rétention de 6 mois.
- ❖ Un membre du groupe politique DP énonce que de son expérience, les délais parfois nécessaires pour réaliser un échange d'informations entre les différentes autorités et administrations luxembourgeoises peuvent être très longs. Un délai de rétention de 3 mois lui paraît trop bref.
- ❖ Un membre du groupe politique DP énonce que la vaste majorité des utilisateurs n'ont commis aucune infraction. Il serait difficilement compréhensible pour ces personnes pourquoi leurs données à caractère personnel seraient stockées pendant une durée excédant 6 mois. Il renvoie à la problématique de la conciliation entre l'impératif du respect du droit à la vie privée et l'impératif de la sécurité publique.

- ❖ Un membre du groupe politique CSV s'exprime en faveur du maintien du délai de 6 mois, tout en précisant que le principe de proportionnalité doit être respecté. Il estime que la Commission nationale pour la protection des données (CNPD) devrait jouer le rôle d'un contrôleur et partant disposer des moyens et compétences nécessaires pour assurer sa mission légale.

Il indique également que la tenue et l'exploitation des bases de données régissant des bases de données détenues par la Police Grand-ducale ne seraient actuellement pas conformes aux exigences de la loi du 2 août 2002 relative à la protection des données. Il demande à ce que la CNPD soit investie du pouvoir de contrôler la banque de données mise en œuvre par les autorités policières.

- ❖ Le représentant du Parquet général donne à considérer que dans le cadre des enquêtes complexes, un délai de rétention des données de 3 mois peut s'avérer trop court (pour assurer la manifestation de la vérité).
- ❖ Un membre du groupe politique LSAP rappelle que l'arrêt rendu par la Cour de justice de l'Union européenne du 8 avril 2014 (affaires jointes C-293/12 C-594/12) dit « Digital rights » ne donne aucune indication quant à une durée de stockage raisonnable.
- ❖ Le représentant du Ministre de la Justice énonce que l'arrêt de la Cour de justice s'apprête à des interprétations très divergentes en matière de légitimité de rétention des données personnelles.
- ❖ Un membre du groupe politique CSV estime qu'il serait utile de prendre connaissance des législations étrangères en matière de durée de stockage de données personnelles et des aspects procéduraux.

La continuation de l'examen du projet de loi figurera à l'ordre du jour d'une prochaine séance de la Commission juridique, une fois que le Ministère de la Justice a recueilli les informations requises.

3. 6908 Projet de loi sur la reconnaissance du mariage au Grand-Duché de Luxembourg et modifiant le Code civil

Présentation du projet de rapport

Madame la Rapportrice présente succinctement son projet de rapport. Elle donne à considérer qu'il ne s'agit pas d'une modification d'une loi existante, mais d'une loi nouvelle.

Vote

Le projet de rapport, recueille l'accord majoritaire (13) des membres de la Commission avec une abstention (représentant de la sensibilité politique ADR).

Temps de parole

Les membres de la Commission proposent le modèle de base pour les débats en séance plénière.

4. 6820 Projet de loi portant modification : 1) de la loi du 29 mars 2013 relative à l'organisation du casier et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne, 2) du Code d'instruction criminelle, 3) du Code pénal

Ce point est reporté.

5. Divers

1) *Demande du groupe politique CSV du 3 mars 2016 et demande de la sensibilité politique ADR du 8 mars 2016*

- ❖ Madame la Présidente prend acte des courriers du groupe politique CSV et de la sensibilité politique ADR et propose de mettre les projets de loi 6568, 5867 et les propositions de loi 5553 et 6797 à l'ordre du jour d'une réunion de la Commission juridique dont la date reste à être déterminée.
- ❖ Un représentant de la sensibilité ADR réaffirme son souhait de mettre notamment la proposition de loi 6797 à l'ordre du jour de la Commission juridique.
- ❖ Un représentant du groupe politique CSV souligne l'importance de mettre les projets de loi 6568 et 5867 à l'ordre du jour de la Commission. Il indique que les projets de loi 6568 et 5867 présentent un intérêt majeur pour un grand nombre de citoyens et que, dans le contexte de la réforme fiscale annoncée par le Gouvernement, le volet relatif à l'autorité parentale conjointe aurait des incidences de nature pécuniaire pour de nombreux couples parents.
- ❖ Les membres de la Commission juridique conviennent de convoquer une réunion de la commission en date du 15 mars 2016 de 14h15 à 16h30, à l'ordre du jour de laquelle figureront les projets de loi 6568 et 5867 ainsi que les propositions de loi 5553 et 6797.

2) *Dissolution de la Sous-commission « Création d'un droit européen des contrats pour les consommateurs et les entreprises de la Commission juridique »*

- ❖ Les membres de la commission décident de dissoudre la Sous-commission « Création d'un droit européen des contrats pour les consommateurs et les entreprises de la Commission juridique », comme son objet est devenu caduc. Un courrier en ce sens sera envoyé aux membres de la Conférence des Présidents.

3) *Projet de loi 5730*

- ❖ M. le Rapporteur du projet de loi 5730 « portant modernisation de la loi modifiée du 10 août 1915 concernant les sociétés commerciales et modification du Code civil et de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises » propose de présenter le 23 mars 2016 son projet de rapport, après avoir analysé les différents avis complémentaires lors de la réunion du 14 mars 2016 de la Sous-commission.

4) *Projet de loi 6624*

- ❖ M. le Rapporteur indique vouloir présenter, lors de la réunion du 16 mars 2016, le projet de rapport du projet de loi 6624 réformant le régime de publication légale relatif aux sociétés et associations.

5) *Projet de loi 6777*

- ❖ Un membre du groupe politique LSAP propose d'entamer l'examen parlementaire du projet de loi 6777 ayant pour objet d'instituer la société à responsabilité limitée simplifiée.

6) *Projets de loi 6759 et 6762 (examen parlementaire en cours)*

- ❖ Un représentant du groupe politique CSV énonce qu'il est important d'avancer dans le cadre de l'établissement d'un avis juridique, tel que demandé, relatif à la confidentialité des documents parlementaires.
- ❖ Madame la Présidente rappelle que la Conférence des Présidents a décidé que l'établissement d'un tel avis juridique relève de la compétence du Bureau.

En ce qui concerne le projet de loi 6759 et son annexe, elle indique que le Gouvernement a demandé un avis à la Commission nationale pour la protection des données et un avis au Conseil d'Etat. Elle propose d'attendre la communication de ces deux avis.

Cette proposition recueille l'accord unanime des membres de la Commission juridique.

Le secrétaire-administrateur,
Laurent Besch

La Présidente,
Viviane Loschetter

Le secrétaire-administrateur (stagiaire)
Christophe Li

01



Session ordinaire 2015-2016

LB/pk

P.V. J 01
P.V. ERMCE 01

Commission juridique

et

Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

Procès-verbal de la réunion du 21 octobre 2015

Ordre du jour :

1. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques
- Echange de vues suite à l'avis du Conseil d'Etat du 10 juillet 2015

2. **Uniquement pour les membres de la Commission juridique:**

6759 Projet de loi portant approbation du " Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information ", signé à Luxembourg le 20 juin 2012
- Désignation d'un rapporteur
- Examen de l'avis du Conseil d'Etat

3. 6762 Projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012
- Désignation d'un rapporteur
- Examen de l'avis du Conseil d'Etat

4. Divers

*

Présents : M. Mars Di Bartolomeo remplaçant M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Alex Bodry, M. Franz Fayot, M. Léon Gloden, Mme Josée Lorsché, Mme Viviane Loschetter, Mme Octavie Modert, M. Laurent Mosar,

Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth, membres de la Commission juridique

Mme Diane Adehm, M. André Bauler, Mme Simone Beissel, M. Eugène Berger, Mme Tess Burton, M. Yves Cruchten, Mme Octavie Modert, M. Roger Negri, M. Marcel Oberweis, M. Roy Reding, M. Serge Wilmes, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

M. Luc Reding, du Ministère de la Justice

M. Laurent Besch, de l'Administration parlementaire

Excusés : M. Marc Angel, M. Paul-Henri Meyers, membres de la Commission juridique

M. Claude Adam, Mme Taina Bofferding, Mme Martine Hansen, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission juridique
Mme Simone Beissel, Président de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

*

1. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Mme la Présidente rappelle que la présente réunion jointe fait suite à celle ayant eu lieu le mercredi 16 juillet 2014 (cf. P.V. J 26 / P.V. ERMCE 31) et le mercredi 2 juillet 2014 (cf. P.V. J 24 / P.V. ERMCE 28) à l'ordre du jour desquelles a figuré un échange de vues ayant porté sur

- l'arrêt de la Cour (grande chambre) du 8 avril 2014. «*Digital Rights Ireland Ltd (C-293/12) contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung (C-594/12)*», et
- l'arrêt de la Cour (grande chambre) du 13 mai 2014 «*Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*».

Le projet de loi sous examen a été présenté aux membres de la Commission juridique lors de la réunion du 11 février 2015 (cf. P.V. J 14) à qui le projet de loi a été renvoyé pour compétence.

Explications de Monsieur le Ministre de la Justice

Pour le détail, il est prié de se reporter au point 3 du procès-verbal n°14 de la réunion de la commission du 11 février 2015 et à l'exposé des motifs.

Monsieur le Ministre de la Justice accueille favorablement l'avis du Conseil d'Etat en ce que ce dernier a approuvé l'approche générale inhérente au projet de loi.

L'orateur précise que la situation, sur le plan légal, diffère d'un pays membre à l'autre suite à l'annulation de la directive 2006/24/CE du 15 mars 2006 du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (dénommée ci-après la directive 2006/24/CE).

En effet, l'annulation de ladite directive par la Cour de Justice de l'Union européenne n'entraîne pas, comme telle, la caducité des législations nationales de transposition. Or, comme le précise le Conseil d'Etat dans son avis du 10 juillet 2015, les législations nationales ayant transposé ladite directive s'exposent, pour autant qu'elles aient suivi les dispositions de ladite directive, au reproche du non respect des mêmes droits fondamentaux que ceux visés à l'arrêt du 8 avril 2004 de la Cour de Justice de l'Union européenne.

L'orateur précise que la validité de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques n'a pas encore été mise en cause devant les juridictions luxembourgeoises.

Monsieur le Ministre de la Justice informe les membres de la commission que le projet de loi tient également compte d'une exigence posée dans le cadre de l'arrêt de la Cour de Justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximilian Schrems / Data Protection Commissioner*» (affaire C-362/14) en ce qu'il est proposé de reformuler le libellé de l'article 5-1 de la loi modifiée précitée du 30 mai 2005 qui oblige, dans son paragraphe 1^{er}, que les données doivent être conservées sur le territoire de l'Union européenne.

L'orateur informe les membres de la commission que ledit arrêt et ses conséquences figureront à l'ordre du jour de la réunion des 3 et 4 décembre 2015 du Conseil JAI.

Examen de l'avis du Conseil d'Etat

Observation préliminaire

Le Conseil d'Etat fait observer que «[...] l'article 67-1 du Code d'instruction criminelle ne fait que poser les conditions d'accès aux données que les fournisseurs et opérateurs sont obligés de retenir en vertu de la loi du 30 mai 2005. Le Conseil d'Etat propose dès lors d'intervertir les articles du projet, l'article 1^{er} devenant l'article 2 et l'article 2 devenant l'article 1^{er}.».

La commission unanime fait sienne cette suggestion.

Nouvel article 2^e (article 1^{er} initial) – modification de l'article 67-1 du code d'instruction criminelle

Accès aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs

Le Conseil d'Etat souligne, en ce qui concerne les deux critiques soulevées par la Cour de Justice de l'Union européenne, à savoir (i) le défaut de précision suffisante quant aux infractions pouvant justifier un accès aux données retenues et (ii) le défaut de limitations

quant au nombre de personnes pouvant effectuer un accès auxdites données, que la loi nationale «[...] prévoit ainsi des règles procédurales précises déterminant tant les accès que les recours contre ceux-ci. De même, le cercle des personnes pouvant recourir à cette mesure est déterminé par les dispositions sur l'organisation judiciaire, et est dès lors non seulement restreint, mais encore fermé.».

La loi luxembourgeoise a de sorte mis en place une espèce de filtre de nature restrictive au niveau de l'accès aux données ayant fait l'objet d'une collecte et d'un stockage.

Au sujet d'un régime de protection spéciale des données de personnes soumises à un régime de protection spéciale en raison de leur secret professionnel, le Conseil d'Etat soulève que l'article 67-1 du Code d'instruction criminelle reste muet sur ce point.

Il propose dès lors à insérer un paragraphe 4 nouveau à l'article 67-1 du Code d'instruction criminelle libellé comme suit:

«(4) Les mesures visées à l'alinéa (1) 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.»

Monsieur le Ministre de la Justice fait observer que les législations étrangères ne prévoient pas de régime d'exception à ce sujet comme une telle exception n'est guère compatible avec le principe même de la rétention de données. L'orateur rappelle que les données à caractère personnel détenues par des personnes tenues au respect du secret professionnel bénéficient de garanties suffisantes en ce que l'accès aux données collectées et stockées est conditionné et nécessite l'intervention obligatoire d'un juge d'instruction, magistrat indépendant. Ainsi, la protection des personnes liées par le secret professionnel à cet effet est entourée des garanties suffisantes.

Les membres de la commission unanimes décident d'insérer l'ajout tel que proposé par le Conseil d'Etat dont le libellé univoque vise à clarifier la situation d'une personne liée par le secret professionnel dans le cadre de l'application de l'article 67-1 du Code d'instruction criminelle.

Infractions pouvant justifier un accès aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs - liste d'infractions

Les auteurs du projet de loi proposent de remplacer la mention d'un seuil de peine déterminant les infractions pour lesquelles les autorités judiciaires peuvent accéder aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs par une liste d'infractions.

Le Conseil d'Etat rappelle que dans le cadre du projet de loi 6113 devenu 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 (Mémorial A, n122 du 29 juillet 2010), il «[...] avait à l'époque exprimé sa préférence pour un seuil de peine.».

Il renvoie à l'article 4 de la directive 2006/24/CE qui dispose que «Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans

son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.».

Le Conseil d'Etat «n'en déduit pas la nécessité absolue pour le législateur national de devoir revenir sur sa décision initiale de procéder à une limitation par le recours à un seuil de peine. Tout au plus, mais il s'agit là d'un choix politique qui ne convient pas au Conseil d'État, pourrait-on vérifier si le seuil actuel d'un an 15 doit être maintenu, ou bien s'il doit être porté à un niveau plus élevé, ainsi que cela avait été notamment discuté dans le cadre de la loi précitée du 24 juillet 2010.».

Il continue en s'interrogeant sur la nécessité de créer une nouvelle liste qui, selon lui, «[...] viendrait s'ajouter à celles figurant déjà actuellement aux différents codes, à l'exemple de l'article 506-1 du Code pénal et des articles 66-2 et 66-3 du Code d'instruction criminelle.».

Le Conseil d'Etat propose, dans le cas de figure où la liste d'infraction sera maintenue, «[...] afin d'éviter que la liste ne se révèle incomplète pour ce qui des infractions qualifiées de crime, d'en retirer tous les crimes spécifiquement mentionnés et de remplacer ces mentions individuelles par la mention générique de „toutes les infractions qualifiées de crime par la loi“ pour ne maintenir pour le surplus dans la liste que les infractions qualifiées de délit que les auteurs jugeront opportun d'y insérer.».

Il continue en suggérant, «[...] afin de respecter les critères de précision et de prévisibilité requis pour toute loi pénale, de remplacer les références à des infractions, voire à des groupes d'infractions, génériques par des références à des articles précis du Code pénal, ou à des lois spéciales, ainsi que cela est déjà pratiqué à l'article 506-1 du Code pénal. Cet exercice pourrait être mis à profit pour énumérer les infractions en question dans un ordre logique suivant, pour celles tirées du Code pénal, une suite numérique et, pour celles tirées des lois spéciales, une suite chronologique.».

Il fait également observer que l'infraction de blanchiment de fonds provenant du trafic de stupéfiants ne figure pas dans la liste d'infractions proposée. Or, il convient de renvoyer au point 12) de ladite liste qui vise l'infraction du blanchiment des produits du crime et recel.

Monsieur le Ministre de la Justice propose de vérifier si la liste des infractions telle que proposée nécessite des adaptations. [Ministère de la justice]

Les membres de la commission décident d'y revenir le moment venu.

Nouvel article 1^{er} (article 2^e initial) – modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Point 1) – modification de l'article 5, paragraphe 1^{er}, point (a)

Le Conseil d'Etat propose de supprimer l'ajout «d'une des infractions prévues à l'article 67-1 (4) du Code d'instruction criminelle» appelé à remplacer le bout de phrase «d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement» qu'il avait à l'époque proposé, dans son avis du 22 juin 2010 relatif au projet de loi 6113 (cf. doc. parl. 6113^o, page 3), de supprimer.

En effet, cela relève du Code d'instruction criminelle et comme les opérateurs devront de toute façon tout conserver, ne sachant *a priori* ni aux fins de recherche de quelles infractions

serviront les données ni quelle donnée sera utile à cette même fin, le Conseil d'Etat estime que ledit ajout peut être supprimé.

Point 2) – article 5, paragraphe 1^{er}, point (b)

Le libellé modifié, en ce qu'il est proposé de préciser que

- (i) l'effacement des données relatives au trafic concernant les abonnés et les utilisateurs doit être irrémédiable et sans délai, et
- (ii) la suppression de la possibilité d'une sauvegarde des données précitées sous une forme anonymisée,

ne donne pas lieu à observation de la part du Conseil d'Etat.

Point 3) – modification de l'article 5, paragraphe 6

Le Conseil d'Etat indique pouvoir «*suivre le raisonnement indiqué dans l'exposé des motifs, il tient cependant à faire remarquer que cette modification instaure un déséquilibre entre la disposition pénale inscrite à l'article 5, paragraphe 6, et celles inscrites à d'autres endroits de la même loi, alors pourtant que les droits protégés par ces autres dispositions sont de valeur égale.*».

Point 4) – modification de l'article 5-1

Le Conseil d'Etat suggère de supprimer à la seconde phrase du paragraphe 2, le terme de «*pleine*» pour ne pas apporter une plus-value législative quelconque. Le texte se lira dès lors comme suit: «*[...] afin d'assurer l'intégrité et la confidentialité de ces données.*».

Le Conseil d'Etat déplore par ailleurs que le règlement grand-ducal visé à l'article 5-1, paragraphe 2, reformulé, n'ait pas été joint au projet de loi, ce qui, en cas de retard dans la mise en place des détails techniques appelés à régir l'intégrité et la confidentialité des données retenues, risque d'entraîner l'inapplicabilité pratique des principes établis par la loi.

Le représentant du Ministère de la Justice informe les membres de la commission qu'une concertation portant sur les modalités de mise en œuvre du cadre légal modifié avec les représentants des fournisseurs et opérateurs a lieu.

Points 5), 6) et 7) – modification de l'article 9, paragraphe 1^{er}, point (a); paragraphe 1^{er}, point (b); paragraphe 6

Le Conseil d'Etat renvoie, comme les points 5), 6) et 7) «*[...] ne font qu'apporter à l'article 9 (rétention des données de localisation autres que les données relatives au trafic) de la loi précitée du 30 mai 2005 des modifications identiques à celles proposées pour l'article 5 [...]*» à ces observations soulevées au sujet des modifications proposées, à l'endroit de l'article 5 (cf. points 1) à 4) ci-avant).

Avis de la Commission nationale pour la protection des données du 16 juin 2015

Les membres de la commission procèdent à un aperçu des points soulevés dans l'avis sous rubrique.

Echange de vues

- ❖ Mme la Rapportrice propose, une fois que le Ministère de la Justice ait finalisé ses vérifications, de revenir sur deux points, à savoir (i) la liste d'infractions et (ii) la durée de conservation des données relatives au trafic.
- ❖ Un représentant du groupe politique LSAP s'interroge sur les éventuelles modifications du cadre légal afférent luxembourgeois suite à l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximilian Schrems / Data Protection Commissioner*» (affaire C-362/14).

Monsieur le Ministre de la Justice explique que par ledit arrêt, l'accord dit «*Safe Harbour*» régissant les flux de données personnelles commerciales entre l'Europe et les Etats-Unis depuis 2000 a été invalidé. Or, cela ne signifie pas que les mesures d'adéquation nationales soient *ipso facto* déclarées comme étant invalides.

Il informe les membres de la commission que la Commission européenne, mandatée par les Etats membres à cet effet, est en train de négocier un nouvel accord.

Cet arrêt du 6 octobre 2015 a par contre une autre percée, à savoir le rétablissement de la compétence exclusive, en tant qu'autorité nationale indépendante, des autorités nationales respectives de protection des données à caractère personnel pour le volet du transfert des données visées.

L'orateur précise que cet arrêt n'a pas pour conséquence de devoir procéder à des adaptations du cadre légal national dans l'attente de la finalisation du paquet européen relatif à la protection des données à caractère personnel.

- ❖ Le représentant de la sensibilité politique déi Lénk, en sa qualité d'observateur, estime que l'absence d'un quelconque moyen de recours a également été sanctionnée par la Cour de Justice de l'Union européenne dans son arrêt précité du 6 octobre 2015.

Au sujet du projet de loi 6763, il informe favoriser l'établissement d'une liste d'infractions en lieu et place de la fixation d'un seuil de peine. Il critique le fait que les documents classifiés soient exclus du champ d'application matériel de la loi modifiée du 30 mai 2005 précitée.

L'orateur renvoie à l'avis intitulé «*Data Retention after the Judgement of the Court of Justice of the European Union*» du 30 juin 2014 rédigé par Monsieur le professeur Dr. Mark D. Cole de l'Université de Luxembourg et Madame le professeur Dr. Franziska Boehm de l'Université de Münster.

Il demande à ce qu'un échange de vues soit organisé avec les auteurs dudit avis.

Monsieur le Ministre de la Justice précise les documents classifiés sont régis par un cadre légal spécifique et qu'il convient d'en discuter au sein de la commission parlementaire compétente.

Mme la Présidente informe les membres de la commission que ledit avis a été communiqué aux membres des deux commissions parlementaires. L'oratrice souligne que les conclusions écrites dudit expert ne sont pas univoques.

*

La continuation de l'examen du projet de loi figurera à l'ordre du jour de l'une des prochaines réunions de la commission une fois que le Ministère de la Justice aurait finalisé ses vérifications.

2. Uniquement pour les membres de la Commission juridique:

6759 Projet de loi portant approbation du " Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information ", signé à Luxembourg le 20 juin 2012

Le représentant de la sensibilité politique déi Lénk (observateur) estime qu'il convient de retirer le projet de loi de l'ordre du jour de la commission comme il n'est pas assuré que le niveau de protection des données à caractère personnel échangées dans le cadre de la coopération renforcée, qui vise l'échange d'informations concernant des personnes faisant l'objet d'enquêtes pénales en matière de terrorisme au Luxembourg ou aux Etats-Unis, soit conforme au niveau européen. Ceci s'impose d'autant plus depuis l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximillian Schrems / Data Protection Commissionner*» (affaire C-362/14).

Une traduction française de l'accord intitulé «*Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information*» est distribuée séance tenante aux membres de la commission.

Désignation d'un rapporteur

La commission unanime désigne Mme la Présidente comme rapporteur du projet de loi.

Examen de l'avis du Conseil d'Etat

Il convient de préciser que le Conseil d'Etat a avisé le texte de loi proposé tel qu'amendé par le Gouvernement.

Observation méthodologique: le terme «*Accord*» vise le «*Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information*» qui est approuvé par le projet de loi sous examen.

Article 1^{er}

Le Conseil d'Etat fait observer, en renvoyant à l'article VIII de l'Accord, que tout amendement de l'Accord doit obligatoirement être soumis, conformément aux dispositions de l'article 37 de la Constitution, pour approbation à la Chambre des Députés et ce avant le délai d'entrée en vigueur de la disposition amendée. Il s'agit d'éviter que celle-ci puisse produire des effets au niveau international à l'égard du Luxembourg avant toute approbation parlementaire.

Article 2

La disposition sous référence ne donne pas lieu à observation.

Article 3

Paragraphe 1^{er}

Le contrôle et l'approbation judiciaire de la transmission d'informations concernant une personne faisant l'objet d'une enquête pénale en matière de terrorisme au Luxembourg ou aux Etats-Unis sont centralisés et relèvent de la compétence exclusive du procureur général d'Etat.

L'accord préalable du procureur général d'Etat est requis pour toute transmission d'informations, sauf les deux exceptions prévues à l'endroit du paragraphe 2 de l'article 3 sous examen.

Il convient de préciser, comme le rappelle à juste titre le Conseil d'Etat, qu'il existe trois cas de figure où le procureur général d'Etat peut refuser l'autorisation de transmission, à savoir:

1. si la transmission est de nature à porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à des intérêts essentiels similaires du Grand-Duché de Luxembourg,
2. si la transmission est relative à une infraction aux lois militaires qui ne constitue pas une infraction de droit commun, et
3. si la transmission est relative à une infraction politique.

Par ailleurs, le procureur général d'Etat est obligé de refuser une autorisation de transmission à chaque fois qu'elle se rapporte à un fait pour lequel celle-ci n'est pas prévue par l'Accord ou que son objet dépasse le domaine d'application dudit Accord.

Il importe de noter que cela va de soi comme l'Accord a un objet précis, à savoir l'échange d'informations portant sur des faits de terrorisme à l'exclusion de documents ou de pièces à conviction. Ainsi, il s'agit d'éviter que les transmissions d'informations opérées dans ce cadre empiètent sur le domaine de l'entraide judiciaire.

Paragraphe 2

Le paragraphe 2 énonce les deux cas de figure où la transmission d'informations n'est pas soumise au contrôle et à l'approbation judiciaire.

Le Conseil d'Etat fait observer que «[...] le projet de loi souligne certes que, dans tous les cas, une telle transmission ne peut être que complémentaire à une transmission déjà autorisée par le procureur général d'Etat. Cependant, les données couvertes par le prédit article 34-1 sont très extensives et sont tirées de bases de données très variées. Le Conseil d'Etat s'interroge dès lors sur l'opportunité d'autoriser le point de contact à transmettre ces données sans autorisation ou contrôle préalable de la part du procureur général d'Etat ce, au vu notamment de l'absence de dispositions dans le MoU garantissant un niveau élevé de protection des données personnelles.

Dans son avis, le Parquet général avait pour sa part proposé de soumettre toute transmission de données nominatives de personnes suspectées d'actes de terrorisme à une autorisation préalable. Aux yeux du Conseil d'Etat tel devrait au moins être le cas lorsque le Luxembourg révèle l'identité d'une personne suspectée de tels actes qui n'est pas encore

connue par les autorités des États-Unis. Le Conseil d'État souligne que toute transmission sur base de l'article 3, paragraphe 2, du projet sous avis ne peut dès lors avoir lieu qu'à titre complémentaire, c'est-à-dire lorsque l'identité de la personne concernée a déjà fait l'objet d'une transmission autorisée par le procureur général d'État ou est déjà connue.».

Monsieur le Ministre de la Justice propose d'envoyer un courrier circonstancié au Conseil d'État et d'en tenir au courant les membres de la Commission juridique. [Ministère de la Justice]

Paragraphe 3

Le libellé proposé tient compte tant de toute transmission de demande envoyée d'un point de contact vers son homologue que d'une transmission spontanée à l'initiative d'un point de contact.

Le texte proposé ne donne pas lieu à observation de la part du Conseil d'État.

Paragraphe 4

L'usage restreint de l'information dont la transmission a été autorisée par le procureur général d'État peut être élargi sous la condition d'une autorisation spécifique émanant de ce dernier.

Cette disposition n'appelle pas d'observation de la part du Conseil d'État.

Article 4

Paragraphe 1^{er}

Le libellé, tel qu'amendé par le Gouvernement, désigne les autorités luxembourgeoises habilitées à présenter des demandes de transmission de données selon le cadre posé par l'Accord.

Paragraphe 2

Le paragraphe 2 précise que les informations transmises au point de contact luxembourgeois peuvent être utilisées par les autorités répressives luxembourgeoises de la même manière que celles obtenues par voie d'entraide judiciaire en matière pénale sous réserve des modalités indiquées par l'Accord.

Le Conseil d'État tient à préciser que «[...] l'accès à ces informations doit être limité sur une base „need-to-know“ et au seul personnel des agences et organes gouvernementaux pertinents. Cet article prohibe en son point a) l'utilisation de ces informations dans des procédures judiciaires, quasi-judiciaires, juridiques ou encore administratives. Elles ne peuvent pas non plus être divulguées à des gouvernements de pays tiers, à des organisations internationales ou à des personnes privées. Toute utilisation aux fins prévues par l'article 4 sous avis est prohibée à moins que les États-Unis d'Amérique ne donnent leur autorisation écrite à une telle utilisation. Il s'ensuit que l'article 4 ne peut s'appliquer qu'au seul cas où les autorités répressives luxembourgeoises ont obtenu la permission, par écrit, d'utiliser ces informations à ces fins. C'est dans ce cas unique que les informations peuvent

être utilisées de la même manière que celles obtenues par voie d'entraide judiciaire ainsi que le prévoit le paragraphe 2 de l'article 4 du projet de loi sous avis.».

Echange de vues

- ❖ Un membre du groupe politique DP estime opportun d'adopter, du moins dans un premier temps, une approche restrictive.

Le représentant du Ministère de la Justice explique qu'à raison de l'objet bien déterminé de l'Accord, la transmission d'informations ne peut qu'intervenir endéans un cadre bien délimité soumise à un contrôle judiciaire préalable et centralisé en les mains du procureur générale d'Etat.

- ❖ Un membre du groupe politique CSV donne à considérer qu'il faut veiller au niveau de la mise en œuvre de l'Accord que toute transmission d'informations soit conforme au principe de la spécialité.

Il convient d'éviter que des informations transmises en toute régularité puissent être détournées pour être utilisées à des fins tout autres et étrangères au cadre autorisé de l'Accord.

- ❖ Le représentant de la sensibilité politique déi Lénk (observateur) s'interroge sur d'éventuelles implications de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximillian Schrems / Data Protection Commissioner*» (affaire C-362/14) en ce qu'il a annulé l'accord dit «Safe Harbour» sur la mise en œuvre de l'échange de transmission tel que visé par le présent Accord.

Monsieur le Ministre de la Justice rappelle que l'accord «*Safe Harbour*» ne vise que les données commerciales, alors que le présent Accord ne vise que des données spécifiques à caractère pénal.

3. 6762 Projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012

Le représentant de la sensibilité politique déi Lénk (observateur) estime qu'il convient de retirer le projet de loi de l'ordre du jour de la commission comme il n'est pas assuré que le niveau de protection des données à caractère personnel échangées dans le cadre de la coopération renforcée, qui vise l'échange d'informations pénales entre les autorités de poursuites pénales luxembourgeoises et américaines, soit conforme au niveau européen. Ceci s'impose d'autant plus depuis l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximillian Schrems / Data Protection Commissioner*» (affaire C-362/14).

Désignation d'un rapporteur

La proposition de désigner Mme la Présidente comme rapporteur recueille l'accord unanime des membres de la commission.

Examen de l'avis du Conseil d'Etat

Il convient de préciser que le Conseil d'Etat a avisé le texte de loi proposé tel qu'amendé par le Gouvernement.

Observation méthodologique: le terme «*Accord*» vise l'«*Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave*» qui est approuvé par le projet de loi sous examen.

Intitulé

L'intitulé doit être modifié en ce que l'Accord a été signé le 3 février 2012 et non le 3 février 2011.

Article 1^{er}

Le Conseil d'Etat rappelle, en renvoyant à l'article 23 de l'Accord, que tout amendement audit Accord doit être soumis pour approbation à la Chambre des Députés. Il importe, eu égard aux dispositions de l'article 37 de la Constitution, que cette approbation parlementaire intervienne avant l'entrée en vigueur de l'amendement afférent et ce afin d'éviter qu'il produise des effets au niveau international à l'égard du Luxembourg.

Article 2

Le libellé proposé ne donne pas lieu à observation de la part du Conseil d'Etat.

Article 3

Paragraphe 1^{er}

Le libellé proposé (suite à l'amendement gouvernementale du 10 avril 2015) n'appelle pas d'observation de la part du Conseil d'Etat.

Paragraphe 2

Le Conseil d'Etat fait observer qu'aucune autorisation préalable de la part du procureur général d'Etat n'est requise pour les données dactyloscopiques et de profils ADN comme elles sont soumises à une consultation automatisée.

Il continue en soulignant que, pour les données issues des bases de données visées par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, aucune autorisation préalable de la part du procureur général d'Etat n'est requise et ce contrairement à ce qui est prévu à l'article 3, paragraphe 2 du projet de loi 6759 (cf. point 2. ci-avant). Il fait observer «*[...] que ce dernier prévoit que ces données ne peuvent être transmises que de manière complémentaire à une transmission autorisée préalablement par le procureur général d'Etat, une telle restriction n'est pas prévue par l'article 3 du projet de loi sous avis. Le Conseil d'Etat s'interroge sur les raisons de cette distinction, d'autant plus que*

la différenciation, opérée dans le commentaire des articles entre, d'une part, les données moins sensibles et, d'autre part, celles visées par ailleurs par l'Accord et qui renseignent sur la participation d'une personne à une infraction pénale, ne ressort pas du texte du projet de loi sous avis. Ce dernier ne précise pas que les données à transmettre sans autorisation sont des données moins sensibles et pas en relation avec une telle infraction grave. Il n'est donc pas exclu que les données à transmettre sur base de l'article 11 de l'Accord (transmission de données à caractère personnel et autres informations aux fins de la prévention d'infractions criminelles et terroristes graves) englobent toutes les données tirées des bases de données visées par l'article 34-1 susmentionné. A l'instar de ce que propose le Parquet général, le Conseil d'État estime cependant que les données à caractère personnel transmises sur base du prédit article 11 devraient être soumises à une autorisation préalable. Il pourrait s'accommoder d'une solution telle que prévue par le projet de loi portant approbation du MoU à savoir qu'une transmission complémentaire de données à caractère personnel peut se faire sans autorisation préalable pour les cas où une première transmission de données identifiant une personne a fait l'objet d'une telle autorisation.».

Paragraphe 3

Le libellé tel que proposé ne donne pas lieu à observation.

Paragraphe 4

Le Conseil d'Etat émet des observations quant à «[...] l'utilisation que les États-Unis d'Amérique peuvent faire des données qui leur ont été transmises. Ainsi, il prévoit que les données leur transmises par le Grand-Duché de Luxembourg sur base de l'article 11 de l'Accord, ne peuvent être utilisées sans le consentement préalable du procureur général d'État aux fins d'une enquête en matière pénale autre que celle dans le cadre de laquelle elles ont été transmises, pour la prévention d'une menace grave à la sécurité publique autre que celle dans le cadre de laquelle elles ont été transmises ou aux fins visées par l'article 13, paragraphes 1, sous c) et d), et 2.

Se posent ici cependant deux questions.

En premier lieu, outre les restrictions prévues par le paragraphe 4 et dont la conformité avec l'Accord sera analysée ci-dessous, le Luxembourg peut imposer, sur base de l'article 11, paragraphe 3, de l'Accord, d'autres conditions quant à l'utilisation qui pourra être faite de ces données. Or, le texte du projet de loi reste muet quant à la question qui déterminera, du côté luxembourgeois, de telles conditions. Est-ce que ce sera également le procureur général d'État? Le point de contact? Le projet de loi sous avis devra spécifier qui sera autorisé à imposer des conditions sur base de l'article 11 de l'Accord. L'article 11, paragraphe 3, prévoit encore que ces conditions sont imposées „dans le respect du droit national“. Le Conseil d'État s'interroge sur le contenu de ce renvoi et se demande s'il n'y a pas lieu de spécifier la matière visée.

En second lieu, le Conseil d'État s'interroge sur la conformité du paragraphe 4 de l'article 3 du projet de loi avec l'Accord soumis pour approbation, et notamment avec ses articles 11, paragraphe 3, et 13, paragraphes 1er et 2. Il semble en effet que les auteurs du projet de loi en question estiment qu'une lecture combinée de ces articles de l'Accord permet de soumettre à autorisation préalable du procureur général d'État l'utilisation des données dans les situations y reprises à savoir, globalement, à des fins ou dans des procédures autres que celles pour lesquelles elles ont été transmises. Or, une autre lecture de ces textes est possible et, aux yeux du Conseil d'État, plus appropriée.

En effet, l'article 11, paragraphe 3, de l'Accord prévoit certes que „[l]a Partie qui transmet les données peut, dans le respect de son droit national, imposer des conditions quant à l'utilisation qui en sera faite par la Partie destinataire. Si cette dernière accepte les données, elle sera liée par ces conditions“. Cependant, l'article 13, paragraphe 1er, de l'Accord prévoit que „chaque Partie peut traiter les données obtenues en vertu du présent Accord:

- a. aux fins de ses enquêtes en matière pénale;
- b. pour la prévention d'une menace grave à la sécurité publique;
- c. dans le cadre de ses procédures administratives ou judiciaires non pénales mais liées directement aux enquêtes visées à l'alinéa (a); ou
- d. pour toute autre finalité, mais uniquement avec le consentement préalable de la Partie ayant transmis les données.“

En outre, le paragraphe 2 du même article impose que „[l]es Parties ne procéderont à aucun transfert de données prévu aux termes de cet Accord à un quelconque État tiers, organisme international ou entité privée sans le consentement de la Partie ayant transmis les données et sans l'adoption de mesures de protection appropriées“.

Il ressort des dispositions précitées que l'utilisation des données transmises peut être soumise à consentement préalable uniquement dans les cas où la Partie qui les a reçues souhaite les utiliser „pour toute autre finalité“ ou les transférer à des entités tierces ou privées. Contrairement à ce que prévoient les auteurs au paragraphe 4, de l'article 3, du projet de loi soumis pour avis, l'utilisation des données en question aux fins d'enquêtes en matière pénale autres que celle dans le cadre de laquelle elles ont été transmises ou l'utilisation de ces données pour la prévention d'une menace grave à la sécurité autre que celle pour la prévention de laquelle elles ont été transmises, ne pourrait alors pas être soumise à un tel accord préalable, global et anticipé. L'article 13, paragraphes 1er et 2, de l'Accord limiterait ce consentement préalable aux deux cas bien précis précités. Certes, la première phrase de l'article 13, paragraphe 1er fait référence à l'article 11, paragraphe 3, de l'Accord, qui prévoit que la Partie qui transmet les données peut imposer des conditions. Or, ces conditions ne peuvent, à la lumière de ce qui précède, consister dans un accord préalable, imposé de manière tellement extensive que prévue par les auteurs du projet de loi.

Il résulterait dès lors de cette lecture que l'article 3, paragraphe 4, du projet de loi ne soit pas conforme aux articles 11, paragraphe 3, et 13, paragraphes 1er et 2, de l'Accord.

Cette interprétation recueillant la préférence du Conseil d'État, il sera nécessaire que les auteurs fournissent, à la lumière de ce qui précède, des explications additionnelles quant à leur interprétation de ces dispositions, avant que le Conseil d'État ne puisse se prononcer en définitive sur la dispense du second vote constitutionnel.»

Monsieur le Ministre de la Justice propose d'envoyer un courrier circonstancié au Conseil d'Etat et d'en tenir au courant les membres de la Commission juridique. [Ministère de la Justice]

Article 4

Paragraphe 1^{er}

Le libellé, tel qu'amendé par le Gouvernement, désigne les autorités luxembourgeoises habilitées à présenter des demandes de transmission de données selon le cadre posé par l'Accord.

Paragraphe 2

Le paragraphe 2 précise que les informations transmises au point de contact luxembourgeois peuvent être utilisées par les autorités répressives luxembourgeoises de la même manière que celles obtenues par voie d'entraide judiciaire en matière pénale sous réserve des modalités indiquées par l'Accord.

Echange de vues

- ❖ Un membre du groupe politique LSAP est d'avis que les deux interrogations soulevées par le Conseil d'Etat à l'endroit du paragraphe 3 de l'article 3 méritent d'être examinées plus amplement par la commission.

Monsieur le Ministre de la Justice propose d'y revenir une fois que le Conseil d'Etat s'est prononcé sur le courrier circonstancié lequel le ministère de la Justice propose de lui envoyer.

- ❖ Un membre du groupe politique CSV donne à considérer qu'il faut veiller, eu égard à la propension américaine de conférer une compétence universelle, au niveau de la mise en œuvre de l'Accord que toute transmission d'informations soit conforme au principe de la spécialité.

Il convient d'éviter que des informations transmises en toute régularité puissent être détournées pour être utilisées à des fins tout autres et étrangères au cadre autorisé de l'Accord.

- ❖ Un membre du groupe politique DP souligne qu'il importe d'adopter une approche restrictive.

Le représentant du Ministère de la Justice explique que l'architecture du système proposé repose sur deux phases distinctes.

Dans un premier temps, il y a un échange d'information par le biais de la recherche et de la comparaison automatisée d'empreintes digitales et de profils d'ADN dans les bases de données luxembourgeoise et américaine.

Dans le cas de figure d'une concordance, des informations à caractère personnel et non-personnel à des fins de prévention du terrorisme sont, dans une deuxième phase, transmises par le biais du point de contact respectif désigné. Cet échange d'informations se fait de manière non automatisée.

- ❖ Un membre du groupe politique CSV se demande si la Commission européenne, dans le cadre des négociations menées dans le cadre du TTIP (*Transatlantic Trade and Investment Partnership*) et du TISA (*Trade in Services Agreement*), même si les deux arrêts de la Cour de justice de l'Union européenne pré-mentionnés ne devraient pas être sans conséquence, parvient à imposer le maintien de certains niveaux standards propres à l'Union européenne.

Monsieur le Ministre de la Justice donne à considérer que la Commission européenne est bien consciente de l'impact de la jurisprudence récente de la juridiction européenne. Il estime partant qu'elle ne peut pas ne pas en tenir compte comme l'accord futur devra rencontrer l'approbation du Parlement européen qui affiche un regard très critique quant au TTISP et TISA.

4. Divers

1) Demande de convocation d'une réunion du groupe politique CSV du 21 août 2015 portant sur les solutions proposées en vue de rencontrer les problèmes liées à la mendicité

Un membre du groupe politique CSV déplore qu'à ce jour, deux mois après la notification de ladite demande de convocation, aucune réunion à ce sujet n'ait été convoquée.

L'orateur renvoie aux réunions du 16 septembre 2015 (cf. P.V. J 30) et à celle du 7 octobre 2015 (cf. P.V. J 32) où ce point a été abordé à chaque fois sur sa demande.

Il rappelle que cette demande de convocation a été faite suite aux déclarations faites tant par Monsieur le Premier Ministre, Ministre d'Etat, que par Monsieur le Ministre de la Sécurité intérieure.

L'orateur informe les membres de la commission que son groupe politique est d'accord, compte tenu des nombreux engagements de Monsieur le Ministre de la Sécurité, pris à raison de ses multiples responsabilités ministérielles, d'inviter Monsieur le Ministre de la Justice ainsi que des représentants du parquet général et de la Police Grand-ducale.

Les membres de la commission décident, compte tenu des disponibilités de Monsieur le Ministre de la Justice, de fixer cette réunion au mercredi 18 novembre 2015 de 13h00 à 14h00.

Cette réunion a été reportée, postérieurement à la tenue de la présente réunion, au **jeudi 19 novembre 2015 de 12h30 à 13h50**.

2) Réforme de la Cour de Justice de l'Union européenne – augmentation des postes de magistrats – accord de principe intervenu

Monsieur le Ministre de la Justice informe les membres de la commission qu'un accord de principe a pu être trouvé au niveau du Conseil JAI, du Parlement européen et de la Commission européenne. Il reste encore l'étape de validation au sein du COREP.

Ledit accord comporte l'obligation, par voie de déclaration politique, d'assurer la parité des sexes lors de la nomination future des magistrats par les Etats membres. Cette condition ne saura être consacrée sur le plan légal formel afin d'éviter à introduire un critère de nomination supplémentaire contraire aux dispositions des traités régissant l'Union européenne.

La Cour de Justice de l'Union européenne se voit renforcée au niveau des magistrats qui passeront de 28 magistrats à 56, y compris les 8 magistrats affectés au Tribunal de la fonction publique qui sera fusionné avec le Tribunal de 1^{ère} instance.

Ce renforcement se fera en trois étapes. Les Etats membres sont désignés par lots (trois lots successifs) pour procéder à la nomination d'un magistrat supplémentaire. En effet, chaque Etat membre a désormais droit à deux magistrats.

Le Luxembourg faisant partie des pays du premier lot, procédera prochainement à la nomination du magistrat supplémentaire. Cette décision dûment motivée sera prise en Conseil de Gouvernement (avant la fin de cette année) qui ne compte pas lancer une procédure d'appel à candidature, comme c'était le cas lors de la dernière nomination d'un

magistrat à la Cour de Justice de l'Union européenne. Cette façon de procéder avait essuyé à l'époque de nombreuses critiques.

Une fois ce renforcement complétée, toute nouvelle nomination par les Etats membres portera sur deux magistrats avec respect de la parité homme/femme.

En ce qui concerne la capacité d'accueil de la Cour de Justice de l'Union européenne, il convient de renvoyer au projet de loi 6825 relatif à la construction de la 5^e extension de la Cour de Justice de l'Union européenne dont le rapport a été adopté par la Commission du Développement durable en date du 15 octobre 2015. Cette 5^e extension comporte notamment la construction d'une 3^e tour adjacente aux deux tours préexistantes.

Le secrétaire-administrateur,
Laurent Besch

La Présidente de la Commission juridique,
Viviane Loschetter

La Présidente de la Commission de
l'Enseignement supérieur, de la Recherche,
des Médias, des Communications et de
l'Espace,
Simone Beissel

01



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Session ordinaire 2015-2016

LB/pk

P.V. J 01
P.V. ERMCE 01

Commission juridique

et

Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

Procès-verbal de la réunion du 21 octobre 2015

Ordre du jour :

1. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques
- Echange de vues suite à l'avis du Conseil d'Etat du 10 juillet 2015

2. **Uniquement pour les membres de la Commission juridique:**

6759 Projet de loi portant approbation du " Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information ", signé à Luxembourg le 20 juin 2012
- Désignation d'un rapporteur
- Examen de l'avis du Conseil d'Etat

3. 6762 Projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012
- Désignation d'un rapporteur
- Examen de l'avis du Conseil d'Etat

4. Divers

*

Présents : M. Mars Di Bartolomeo remplaçant M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Alex Bodry, M. Franz Fayot, M. Léon Gloden, Mme Josée Lorsché, Mme Viviane Loschetter, Mme Octavie Modert, M. Laurent Mosar,

Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth, membres de la Commission juridique

Mme Diane Adehm, M. André Bauler, Mme Simone Beissel, M. Eugène Berger, Mme Tess Burton, M. Yves Cruchten, Mme Octavie Modert, M. Roger Negri, M. Marcel Oberweis, M. Roy Reding, M. Serge Wilmes, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

M. Luc Reding, du Ministère de la Justice

M. Laurent Besch, de l'Administration parlementaire

Excusés : M. Marc Angel, M. Paul-Henri Meyers, membres de la Commission juridique

M. Claude Adam, Mme Taina Bofferding, Mme Martine Hansen, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission juridique
Mme Simone Beissel, Président de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace

*

1. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Mme la Présidente rappelle que la présente réunion jointe fait suite à celle ayant eu lieu le mercredi 16 juillet 2014 (cf. P.V. J 26 / P.V. ERMCE 31) et le mercredi 2 juillet 2014 (cf. P.V. J 24 / P.V. ERMCE 28) à l'ordre du jour desquelles a figuré un échange de vues ayant porté sur

- l'arrêt de la Cour (grande chambre) du 8 avril 2014. «*Digital Rights Ireland Ltd (C-293/12) contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung (C-594/12)*», et
- l'arrêt de la Cour (grande chambre) du 13 mai 2014 «*Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*».

Le projet de loi sous examen a été présenté aux membres de la Commission juridique lors de la réunion du 11 février 2015 (cf. P.V. J 14) à qui le projet de loi a été renvoyé pour compétence.

Explications de Monsieur le Ministre de la Justice

Pour le détail, il est prié de se reporter au point 3 du procès-verbal n°14 de la réunion de la commission du 11 février 2015 et à l'exposé des motifs.

Monsieur le Ministre de la Justice accueille favorablement l'avis du Conseil d'Etat en ce que ce dernier a approuvé l'approche générale inhérente au projet de loi.

L'orateur précise que la situation, sur le plan légal, diffère d'un pays membre à l'autre suite à l'annulation de la directive 2006/24/CE du 15 mars 2006 du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (dénommée ci-après la directive 2006/24/CE).

En effet, l'annulation de ladite directive par la Cour de Justice de l'Union européenne n'entraîne pas, comme telle, la caducité des législations nationales de transposition. Or, comme le précise le Conseil d'Etat dans son avis du 10 juillet 2015, les législations nationales ayant transposé ladite directive s'exposent, pour autant qu'elles aient suivi les dispositions de ladite directive, au reproche du non respect des mêmes droits fondamentaux que ceux visés à l'arrêt du 8 avril 2004 de la Cour de Justice de l'Union européenne.

L'orateur précise que la validité de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques n'a pas encore été mise en cause devant les juridictions luxembourgeoises.

Monsieur le Ministre de la Justice informe les membres de la commission que le projet de loi tient également compte d'une exigence posée dans le cadre de l'arrêt de la Cour de Justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximilian Schrems / Data Protection Commissionner*» (affaire C-362/14) en ce qu'il est proposé de reformuler le libellé de l'article 5-1 de la loi modifiée précitée du 30 mai 2005 qui oblige, dans son paragraphe 1^{er}, que les données doivent être conservées sur le territoire de l'Union européenne.

L'orateur informe les membres de la commission que ledit arrêt et ses conséquences figureront à l'ordre du jour de la réunion des 3 et 4 décembre 2015 du Conseil JAI.

Examen de l'avis du Conseil d'Etat

Observation préliminaire

Le Conseil d'Etat fait observer que «[...] l'article 67-1 du Code d'instruction criminelle ne fait que poser les conditions d'accès aux données que les fournisseurs et opérateurs sont obligés de retenir en vertu de la loi du 30 mai 2005. Le Conseil d'Etat propose dès lors d'intervertir les articles du projet, l'article 1^{er} devenant l'article 2 et l'article 2 devenant l'article 1^{er}.».

La commission unanime fait sienne cette suggestion.

Nouvel article 2^e (article 1^{er} initial) – modification de l'article 67-1 du code d'instruction criminelle

Accès aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs

Le Conseil d'Etat souligne, en ce qui concerne les deux critiques soulevées par la Cour de Justice de l'Union européenne, à savoir (i) le défaut de précision suffisante quant aux infractions pouvant justifier un accès aux données retenues et (ii) le défaut de limitations

quant au nombre de personnes pouvant effectuer un accès auxdites données, que la loi nationale «[...] prévoit ainsi des règles procédurales précises déterminant tant les accès que les recours contre ceux-ci. De même, le cercle des personnes pouvant recourir à cette mesure est déterminé par les dispositions sur l'organisation judiciaire, et est dès lors non seulement restreint, mais encore fermé.».

La loi luxembourgeoise a de sorte mis en place une espèce de filtre de nature restrictive au niveau de l'accès aux données ayant fait l'objet d'une collecte et d'un stockage.

Au sujet d'un régime de protection spéciale des données de personnes soumises à un régime de protection spéciale en raison de leur secret professionnel, le Conseil d'Etat soulève que l'article 67-1 du Code d'instruction criminelle reste muet sur ce point.

Il propose dès lors à insérer un paragraphe 4 nouveau à l'article 67-1 du Code d'instruction criminelle libellé comme suit:

«(4) Les mesures visées à l'alinéa (1) 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.»

Monsieur le Ministre de la Justice fait observer que les législations étrangères ne prévoient pas de régime d'exception à ce sujet comme une telle exception n'est guère compatible avec le principe même de la rétention de données. L'orateur rappelle que les données à caractère personnel détenues par des personnes tenues au respect du secret professionnel bénéficient de garanties suffisantes en ce que l'accès aux données collectées et stockées est conditionné et nécessite l'intervention obligatoire d'un juge d'instruction, magistrat indépendant. Ainsi, la protection des personnes liées par le secret professionnel à cet effet est entourée des garanties suffisantes.

Les membres de la commission unanimes décident d'insérer l'ajout tel que proposé par le Conseil d'Etat dont le libellé univoque vise à clarifier la situation d'une personne liée par le secret professionnel dans le cadre de l'application de l'article 67-1 du Code d'instruction criminelle.

Infractions pouvant justifier un accès aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs - liste d'infractions

Les auteurs du projet de loi proposent de remplacer la mention d'un seuil de peine déterminant les infractions pour lesquelles les autorités judiciaires peuvent accéder aux données à caractère personnel collectées et stockées par les fournisseurs et opérateurs par une liste d'infractions.

Le Conseil d'Etat rappelle que dans le cadre du projet de loi 6113 devenu 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 (Mémorial A, n122 du 29 juillet 2010), il «[...] avait à l'époque exprimé sa préférence pour un seuil de peine.».

Il renvoie à l'article 4 de la directive 2006/24/CE qui dispose que «Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans

son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.».

Le Conseil d'Etat «n'en déduit pas la nécessité absolue pour le législateur national de devoir revenir sur sa décision initiale de procéder à une limitation par le recours à un seuil de peine. Tout au plus, mais il s'agit là d'un choix politique qui ne convient pas au Conseil d'État, pourrait-on vérifier si le seuil actuel d'un an 15 doit être maintenu, ou bien s'il doit être porté à un niveau plus élevé, ainsi que cela avait été notamment discuté dans le cadre de la loi précitée du 24 juillet 2010.».

Il continue en s'interrogeant sur la nécessité de créer une nouvelle liste qui, selon lui, «[...] viendrait s'ajouter à celles figurant déjà actuellement aux différents codes, à l'exemple de l'article 506-1 du Code pénal et des articles 66-2 et 66-3 du Code d'instruction criminelle.».

Le Conseil d'Etat propose, dans le cas de figure où la liste d'infraction sera maintenue, «[...] afin d'éviter que la liste ne se révèle incomplète pour ce qui des infractions qualifiées de crime, d'en retirer tous les crimes spécifiquement mentionnés et de remplacer ces mentions individuelles par la mention générique de „toutes les infractions qualifiées de crime par la loi“ pour ne maintenir pour le surplus dans la liste que les infractions qualifiées de délit que les auteurs jugeront opportun d'y insérer.» Il continue en suggérant, «[...] afin de respecter les critères de précision et de prévisibilité requis pour toute loi pénale, de remplacer les références à des infractions, voire à des groupes d'infractions, génériques par des références à des articles précis du Code pénal, ou à des lois spéciales, ainsi que cela est déjà pratiqué à l'article 506-1 du Code pénal. Cet exercice pourrait être mis à profit pour énumérer les infractions en question dans un ordre logique suivant, pour celles tirées du Code pénal, une suite numérique et, pour celles tirées des lois spéciales, une suite chronologique.».

Il fait également observer que l'infraction de blanchiment de fonds provenant du trafic de stupéfiants ne figure pas dans la liste d'infractions proposée. Or, il convient de renvoyer au point 12) de ladite liste qui vise l'infraction du blanchiment des produits du crime et recel.

Monsieur le Ministre de la Justice propose de vérifier si la liste des infractions telle que proposée nécessite des adaptations. [Ministère de la justice]

Les membres de la commission décident d'y revenir le moment venu.

Nouvel article 1^{er} (article 2^e initial) – modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Point 1) – modification de l'article 5, paragraphe 1^{er}, point (a)

Le Conseil d'Etat propose de supprimer l'ajout «d'une des infractions prévues à l'article 67-1 (4) du Code d'instruction criminelle» appelé à remplacer le bout de phrase «d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement» qu'il avait à l'époque proposé, dans son avis du 22 juin 2010 relatif au projet de loi 6113 (cf. doc. parl. 6113^o, page 3), de supprimer.

En effet, cela relève du Code d'instruction criminelle et comme les opérateurs devront de toute façon tout conserver, ne sachant *a priori* ni aux fins de recherche de quelles infractions

serviront les données ni quelle donnée sera utile à cette même fin, le Conseil d'Etat estime que ledit ajout peut être supprimé.

Point 2) – article 5, paragraphe 1^{er}, point (b)

Le libellé modifié, en ce qu'il est proposé de préciser que

- (i) l'effacement des données relatives au trafic concernant les abonnés et les utilisateurs doit être irrémédiable et sans délai, et
- (ii) la suppression de la possibilité d'une sauvegarde des données précitées sous une forme anonymisée,

ne donne pas lieu à observation de la part du Conseil d'Etat.

Point 3) – modification de l'article 5, paragraphe 6

Le Conseil d'Etat indique pouvoir «*suivre le raisonnement indiqué dans l'exposé des motifs, il tient cependant à faire remarquer que cette modification instaure un déséquilibre entre la disposition pénale inscrite à l'article 5, paragraphe 6, et celles inscrites à d'autres endroits de la même loi, alors pourtant que les droits protégés par ces autres dispositions sont de valeur égale.*».

Point 4) – modification de l'article 5-1

Le Conseil d'Etat suggère de supprimer à la seconde phrase du paragraphe 2, le terme de «*pleine*» pour ne pas apporter une plus-value législative quelconque. Le texte se lira dès lors comme suit: «*[...] afin d'assurer l'intégrité et la confidentialité de ces données.*».

Le Conseil d'Etat déplore par ailleurs que le règlement grand-ducal visé à l'article 5-1, paragraphe 2, reformulé, n'ait pas été joint au projet de loi, ce qui, en cas de retard dans la mise en place des détails techniques appelés à régir l'intégrité et la confidentialité des données retenues, risque d'entraîner l'inapplicabilité pratique des principes établis par la loi.

Le représentant du Ministère de la Justice informe les membres de la commission qu'une concertation portant sur les modalités de mise en œuvre du cadre légal modifié avec les représentants des fournisseurs et opérateurs a lieu.

Points 5), 6) et 7) – modification de l'article 9, paragraphe 1^{er}, point (a); paragraphe 1^{er}, point (b); paragraphe 6

Le Conseil d'Etat renvoie, comme les points 5), 6) et 7) «*[...] ne font qu'apporter à l'article 9 (rétention des données de localisation autres que les données relatives au trafic) de la loi précitée du 30 mai 2005 des modifications identiques à celles proposées pour l'article 5 [...]*» à ces observations soulevées au sujet des modifications proposées, à l'endroit de l'article 5 (cf. points 1) à 4) ci-avant).

Avis de la Commission nationale pour la protection des données du 16 juin 2015

Les membres de la commission procèdent à un aperçu des points soulevés dans l'avis sous rubrique.

Echange de vues

- ❖ Mme la Rapportrice propose, une fois que le Ministère de la Justice ait finalisé ses vérifications, de revenir sur deux points, à savoir (i) la liste d'infractions et (ii) la durée de conservation des données relatives au trafic.
- ❖ Un représentant du groupe politique LSAP s'interroge sur les éventuelles modifications du cadre légal afférent luxembourgeois suite à l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximilian Schrems / Data Protection Commissioner*» (affaire C-362/14).

Monsieur le Ministre de la Justice explique que par ledit arrêt, l'accord dit «*Safe Harbour*» régissant les flux de données personnelles commerciales entre l'Europe et les Etats-Unis depuis 2000 a été invalidé. Or, cela ne signifie pas que les mesures d'adéquation nationales soient *ipso facto* déclarées comme étant invalides.

Il informe les membres de la commission que la Commission européenne, mandatée par les Etats membres à cet effet, est en train de négocier un nouvel accord.

Cet arrêt du 6 octobre 2015 a par contre une autre percée, à savoir le rétablissement de la compétence exclusive, en tant qu'autorité nationale indépendante, des autorités nationales respectives de protection des données à caractère personnel pour le volet du transfert des données visées.

L'orateur précise que cet arrêt n'a pas pour conséquence de devoir procéder à des adaptations du cadre légal national dans l'attente de la finalisation du paquet européen relatif à la protection des données à caractère personnel.

- ❖ Le représentant de la sensibilité politique déi Lénk, en sa qualité d'observateur, estime que l'absence d'un quelconque moyen de recours a également été sanctionnée par la Cour de Justice de l'Union européenne dans son arrêt précité du 6 octobre 2015.

Au sujet du projet de loi 6763, il informe favoriser l'établissement d'une liste d'infractions en lieu et place de la fixation d'un seuil de peine. Il critique le fait que les documents classifiés soient exclus du champ d'application matériel de la loi modifiée du 30 mai 2005 précitée.

L'orateur renvoie à l'avis intitulé «*Data Retention after the Judgement of the Court of Justice of the European Union*» du 30 juin 2014 rédigé par Monsieur le professeur Dr. Mark D. Cole de l'Université de Luxembourg et Madame le professeur Dr. Franziska Boehm de l'Université de Münster.

Il demande à ce qu'un échange de vues soit organisé avec les auteurs dudit avis.

Monsieur le Ministre de la Justice précise les documents classifiés sont régis par un cadre légal spécifique et qu'il convient d'en discuter au sein de la commission parlementaire compétente.

Mme la Présidente informe les membres de la commission que ledit avis a été communiqué aux membres des deux commissions parlementaires. L'oratrice souligne que les conclusions écrites dudit expert ne sont pas univoques.

*

La continuation de l'examen du projet de loi figurera à l'ordre du jour de l'une des prochaines réunions de la commission une fois que le Ministère de la Justice aurait finalisé ses vérifications.

2. Uniquement pour les membres de la Commission juridique:

6759 Projet de loi portant approbation du " Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information ", signé à Luxembourg le 20 juin 2012

Le représentant de la sensibilité politique déi Lénk (observateur) estime qu'il convient de retirer le projet de loi de l'ordre du jour de la commission comme il n'est pas assuré que le niveau de protection des données à caractère personnel échangées dans le cadre de la coopération renforcée, qui vise l'échange d'informations concernant des personnes faisant l'objet d'enquêtes pénales en matière de terrorisme au Luxembourg ou aux Etats-Unis, soit conforme au niveau européen. Ceci s'impose d'autant plus depuis l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximillian Schrems / Data Protection Commissionner*» (affaire C-362/14).

Une traduction française de l'accord intitulé «*Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information*» est distribuée séance tenante aux membres de la commission.

Désignation d'un rapporteur

La commission unanime désigne Mme la Présidente comme rapporteur du projet de loi.

Examen de l'avis du Conseil d'Etat

Il convient de préciser que le Conseil d'Etat a avisé le texte de loi proposé tel qu'amendé par le Gouvernement.

Observation méthodologique: le terme «*Accord*» vise le «*Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information*» qui est approuvé par le projet de loi sous examen.

Article 1^{er}

Le Conseil d'Etat fait observer, en renvoyant à l'article VIII de l'Accord, que tout amendement de l'Accord doit obligatoirement être soumis, conformément aux dispositions de l'article 37 de la Constitution, pour approbation à la Chambre des Députés et ce avant le délai d'entrée en vigueur de la disposition amendée. Il s'agit d'éviter que celle-ci puisse produire des effets au niveau international à l'égard du Luxembourg avant toute approbation parlementaire.

Article 2

La disposition sous référence ne donne pas lieu à observation.

Article 3

Paragraphe 1^{er}

Le contrôle et l'approbation judiciaire de la transmission d'informations concernant une personne faisant l'objet d'une enquête pénale en matière de terrorisme au Luxembourg ou aux Etats-Unis sont centralisés et relèvent de la compétence exclusive du procureur général d'Etat.

L'accord préalable du procureur général d'Etat est requis pour toute transmission d'informations, sauf les deux exceptions prévues à l'endroit du paragraphe 2 de l'article 3 sous examen.

Il convient de préciser, comme le rappelle à juste titre le Conseil d'Etat, qu'il existe trois cas de figure où le procureur général d'Etat peut refuser l'autorisation de transmission, à savoir:

1. si la transmission est de nature à porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à des intérêts essentiels similaires du Grand-Duché de Luxembourg,
2. si la transmission est relative à une infraction aux lois militaires qui ne constitue pas une infraction de droit commun, et
3. si la transmission est relative à une infraction politique.

Par ailleurs, le procureur général d'Etat est obligé de refuser une autorisation de transmission à chaque fois qu'elle se rapporte à un fait pour lequel celle-ci n'est pas prévue par l'Accord ou que son objet dépasse le domaine d'application dudit Accord.

Il importe de noter que cela va de soi comme l'Accord a un objet précis, à savoir l'échange d'informations portant sur des faits de terrorisme à l'exclusion de documents ou de pièces à conviction. Ainsi, il s'agit d'éviter que les transmissions d'informations opérées dans ce cadre empiètent sur le domaine de l'entraide judiciaire.

Paragraphe 2

Le paragraphe 2 énonce les deux cas de figure où la transmission d'informations n'est pas soumise au contrôle et à l'approbation judiciaire.

Le Conseil d'Etat fait observer que «[...] le projet de loi souligne certes que, dans tous les cas, une telle transmission ne peut être que complémentaire à une transmission déjà autorisée par le procureur général d'Etat. Cependant, les données couvertes par le prédit article 34-1 sont très extensives et sont tirées de bases de données très variées. Le Conseil d'Etat s'interroge dès lors sur l'opportunité d'autoriser le point de contact à transmettre ces données sans autorisation ou contrôle préalable de la part du procureur général d'Etat ce, au vu notamment de l'absence de dispositions dans le MoU garantissant un niveau élevé de protection des données personnelles.

Dans son avis, le Parquet général avait pour sa part proposé de soumettre toute transmission de données nominatives de personnes suspectées d'actes de terrorisme à une autorisation préalable. Aux yeux du Conseil d'Etat tel devrait au moins être le cas lorsque le Luxembourg révèle l'identité d'une personne suspectée de tels actes qui n'est pas encore

connue par les autorités des États-Unis. Le Conseil d'État souligne que toute transmission sur base de l'article 3, paragraphe 2, du projet sous avis ne peut dès lors avoir lieu qu'à titre complémentaire, c'est-à-dire lorsque l'identité de la personne concernée a déjà fait l'objet d'une transmission autorisée par le procureur général d'État ou est déjà connue.».

Monsieur le Ministre de la Justice propose d'envoyer un courrier circonstancié au Conseil d'État et d'en tenir au courant les membres de la Commission juridique. [Ministère de la Justice]

Paragraphe 3

Le libellé proposé tient compte tant de toute transmission de demande envoyée d'un point de contact vers son homologue que d'une transmission spontanée à l'initiative d'un point de contact.

Le texte proposé ne donne pas lieu à observation de la part du Conseil d'État.

Paragraphe 4

L'usage restreint de l'information dont la transmission a été autorisée par le procureur général d'État peut être élargi sous la condition d'une autorisation spécifique émanant de ce dernier.

Cette disposition n'appelle pas d'observation de la part du Conseil d'État.

Article 4

Paragraphe 1^{er}

Le libellé, tel qu'amendé par le Gouvernement, désigne les autorités luxembourgeoises habilitées à présenter des demandes de transmission de données selon le cadre posé par l'Accord.

Paragraphe 2

Le paragraphe 2 précise que les informations transmises au point de contact luxembourgeois peuvent être utilisées par les autorités répressives luxembourgeoises de la même manière que celles obtenues par voie d'entraide judiciaire en matière pénale sous réserve des modalités indiquées par l'Accord.

Le Conseil d'État tient à préciser que «[...] l'accès à ces informations doit être limité sur une base „need-to-know“ et au seul personnel des agences et organes gouvernementaux pertinents. Cet article prohibe en son point a) l'utilisation de ces informations dans des procédures judiciaires, quasi-judiciaires, juridiques ou encore administratives. Elles ne peuvent pas non plus être divulguées à des gouvernements de pays tiers, à des organisations internationales ou à des personnes privées. Toute utilisation aux fins prévues par l'article 4 sous avis est prohibée à moins que les États-Unis d'Amérique ne donnent leur autorisation écrite à une telle utilisation. Il s'ensuit que l'article 4 ne peut s'appliquer qu'au seul cas où les autorités répressives luxembourgeoises ont obtenu la permission, par écrit, d'utiliser ces informations à ces fins. C'est dans ce cas unique que les informations peuvent

être utilisées de la même manière que celles obtenues par voie d'entraide judiciaire ainsi que le prévoit le paragraphe 2 de l'article 4 du projet de loi sous avis.».

Echange de vues

- ❖ Un membre du groupe politique DP estime opportun d'adopter, du moins dans un premier temps, une approche restrictive.

Le représentant du Ministère de la Justice explique qu'à raison de l'objet bien déterminé de l'Accord, la transmission d'informations ne peut qu'intervenir endéans un cadre bien délimité soumise à un contrôle judiciaire préalable et centralisé en les mains du procureur générale d'Etat.

- ❖ Un membre du groupe politique CSV donne à considérer qu'il faut veiller au niveau de la mise en œuvre de l'Accord que toute transmission d'informations soit conforme au principe de la spécialité.

Il convient d'éviter que des informations transmises en toute régularité puissent être détournées pour être utilisées à des fins tout autres et étrangères au cadre autorisé de l'Accord.

- ❖ Le représentant de la sensibilité politique déi Lénk (observateur) s'interroge sur d'éventuelles implications de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximillian Schrems / Data Protection Commissioner*» (affaire C-362/14) en ce qu'il a annulé l'accord dit «Safe Harbour» sur la mise en œuvre de l'échange de transmission tel que visé par le présent Accord.

Monsieur le Ministre de la Justice rappelle que l'accord «*Safe Harbour*» ne vise que les données commerciales, alors que le présent Accord ne vise que des données spécifiques à caractère pénal.

3. 6762 Projet de loi portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012

Le représentant de la sensibilité politique déi Lénk (observateur) estime qu'il convient de retirer le projet de loi de l'ordre du jour de la commission comme il n'est pas assuré que le niveau de protection des données à caractère personnel échangées dans le cadre de la coopération renforcée, qui vise l'échange d'informations pénales entre les autorités de poursuites pénales luxembourgeoises et américaines, soit conforme au niveau européen. Ceci s'impose d'autant plus depuis l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire «*Maximillian Schrems / Data Protection Commissioner*» (affaire C-362/14).

Désignation d'un rapporteur

La proposition de désigner Mme la Présidente comme rapporteur recueille l'accord unanime des membres de la commission.

Examen de l'avis du Conseil d'Etat

Il convient de préciser que le Conseil d'Etat a avisé le texte de loi proposé tel qu'amendé par le Gouvernement.

Observation méthodologique: le terme «*Accord*» vise l'«*Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave*» qui est approuvé par le projet de loi sous examen.

Intitulé

L'intitulé doit être modifié en ce que l'Accord a été signé le 3 février 2012 et non le 3 février 2011.

Article 1^{er}

Le Conseil d'Etat rappelle, en renvoyant à l'article 23 de l'Accord, que tout amendement audit Accord doit être soumis pour approbation à la Chambre des Députés. Il importe, eu égard aux dispositions de l'article 37 de la Constitution, que cette approbation parlementaire intervienne avant l'entrée en vigueur de l'amendement afférent et ce afin d'éviter qu'il produise des effets au niveau international à l'égard du Luxembourg.

Article 2

Le libellé proposé ne donne pas lieu à observation de la part du Conseil d'Etat.

Article 3

Paragraphe 1^{er}

Le libellé proposé (suite à l'amendement gouvernementale du 10 avril 2015) n'appelle pas d'observation de la part du Conseil d'Etat.

Paragraphe 2

Le Conseil d'Etat fait observer qu'aucune autorisation préalable de la part du procureur général d'Etat n'est requise pour les données dactyloscopiques et de profils ADN comme elles sont soumises à une consultation automatisée.

Il continue en soulignant que, pour les données issues des bases de données visées par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, aucune autorisation préalable de la part du procureur général d'Etat n'est requise et ce contrairement à ce qui est prévu à l'article 3, paragraphe 2 du projet de loi 6759 (cf. point 2. ci-avant). Il fait observer «*[...] que ce dernier prévoit que ces données ne peuvent être transmises que de manière complémentaire à une transmission autorisée préalablement par le procureur général d'Etat, une telle restriction n'est pas prévue par l'article 3 du projet de loi sous avis. Le Conseil d'Etat s'interroge sur les raisons de cette distinction, d'autant plus que*

la différenciation, opérée dans le commentaire des articles entre, d'une part, les données moins sensibles et, d'autre part, celles visées par ailleurs par l'Accord et qui renseignent sur la participation d'une personne à une infraction pénale, ne ressort pas du texte du projet de loi sous avis. Ce dernier ne précise pas que les données à transmettre sans autorisation sont des données moins sensibles et pas en relation avec une telle infraction grave. Il n'est donc pas exclu que les données à transmettre sur base de l'article 11 de l'Accord (transmission de données à caractère personnel et autres informations aux fins de la prévention d'infractions criminelles et terroristes graves) englobent toutes les données tirées des bases de données visées par l'article 34-1 susmentionné. A l'instar de ce que propose le Parquet général, le Conseil d'État estime cependant que les données à caractère personnel transmises sur base du prédit article 11 devraient être soumises à une autorisation préalable. Il pourrait s'accommoder d'une solution telle que prévue par le projet de loi portant approbation du MoU à savoir qu'une transmission complémentaire de données à caractère personnel peut se faire sans autorisation préalable pour les cas où une première transmission de données identifiant une personne a fait l'objet d'une telle autorisation.».

Paragraphe 3

Le libellé tel que proposé ne donne pas lieu à observation.

Paragraphe 4

Le Conseil d'Etat émet des observations quant à «[...] l'utilisation que les États-Unis d'Amérique peuvent faire des données qui leur ont été transmises. Ainsi, il prévoit que les données leur transmises par le Grand-Duché de Luxembourg sur base de l'article 11 de l'Accord, ne peuvent être utilisées sans le consentement préalable du procureur général d'État aux fins d'une enquête en matière pénale autre que celle dans le cadre de laquelle elles ont été transmises, pour la prévention d'une menace grave à la sécurité publique autre que celle dans le cadre de laquelle elles ont été transmises ou aux fins visées par l'article 13, paragraphes 1, sous c) et d), et 2.

Se posent ici cependant deux questions.

En premier lieu, outre les restrictions prévues par le paragraphe 4 et dont la conformité avec l'Accord sera analysée ci-dessous, le Luxembourg peut imposer, sur base de l'article 11, paragraphe 3, de l'Accord, d'autres conditions quant à l'utilisation qui pourra être faite de ces données. Or, le texte du projet de loi reste muet quant à la question qui déterminera, du côté luxembourgeois, de telles conditions. Est-ce que ce sera également le procureur général d'État? Le point de contact? Le projet de loi sous avis devra spécifier qui sera autorisé à imposer des conditions sur base de l'article 11 de l'Accord. L'article 11, paragraphe 3, prévoit encore que ces conditions sont imposées „dans le respect du droit national“. Le Conseil d'État s'interroge sur le contenu de ce renvoi et se demande s'il n'y a pas lieu de spécifier la matière visée.

En second lieu, le Conseil d'État s'interroge sur la conformité du paragraphe 4 de l'article 3 du projet de loi avec l'Accord soumis pour approbation, et notamment avec ses articles 11, paragraphe 3, et 13, paragraphes 1er et 2. Il semble en effet que les auteurs du projet de loi en question estiment qu'une lecture combinée de ces articles de l'Accord permet de soumettre à autorisation préalable du procureur général d'État l'utilisation des données dans les situations y reprises à savoir, globalement, à des fins ou dans des procédures autres que celles pour lesquelles elles ont été transmises. Or, une autre lecture de ces textes est possible et, aux yeux du Conseil d'État, plus appropriée.

En effet, l'article 11, paragraphe 3, de l'Accord prévoit certes que „[l]a Partie qui transmet les données peut, dans le respect de son droit national, imposer des conditions quant à l'utilisation qui en sera faite par la Partie destinataire. Si cette dernière accepte les données, elle sera liée par ces conditions“. Cependant, l'article 13, paragraphe 1er, de l'Accord prévoit que „chaque Partie peut traiter les données obtenues en vertu du présent Accord:

- a. aux fins de ses enquêtes en matière pénale;
- b. pour la prévention d'une menace grave à la sécurité publique;
- c. dans le cadre de ses procédures administratives ou judiciaires non pénales mais liées directement aux enquêtes visées à l'alinéa (a); ou
- d. pour toute autre finalité, mais uniquement avec le consentement préalable de la Partie ayant transmis les données.“

En outre, le paragraphe 2 du même article impose que „[l]es Parties ne procéderont à aucun transfert de données prévu aux termes de cet Accord à un quelconque État tiers, organisme international ou entité privée sans le consentement de la Partie ayant transmis les données et sans l'adoption de mesures de protection appropriées“.

Il ressort des dispositions précitées que l'utilisation des données transmises peut être soumise à consentement préalable uniquement dans les cas où la Partie qui les a reçues souhaite les utiliser „pour toute autre finalité“ ou les transférer à des entités tierces ou privées. Contrairement à ce que prévoient les auteurs au paragraphe 4, de l'article 3, du projet de loi soumis pour avis, l'utilisation des données en question aux fins d'enquêtes en matière pénale autres que celle dans le cadre de laquelle elles ont été transmises ou l'utilisation de ces données pour la prévention d'une menace grave à la sécurité autre que celle pour la prévention de laquelle elles ont été transmises, ne pourrait alors pas être soumise à un tel accord préalable, global et anticipé. L'article 13, paragraphes 1er et 2, de l'Accord limiterait ce consentement préalable aux deux cas bien précis précités. Certes, la première phrase de l'article 13, paragraphe 1er fait référence à l'article 11, paragraphe 3, de l'Accord, qui prévoit que la Partie qui transmet les données peut imposer des conditions. Or, ces conditions ne peuvent, à la lumière de ce qui précède, consister dans un accord préalable, imposé de manière tellement extensive que prévue par les auteurs du projet de loi.

Il résulterait dès lors de cette lecture que l'article 3, paragraphe 4, du projet de loi ne soit pas conforme aux articles 11, paragraphe 3, et 13, paragraphes 1er et 2, de l'Accord.

Cette interprétation recueillant la préférence du Conseil d'État, il sera nécessaire que les auteurs fournissent, à la lumière de ce qui précède, des explications additionnelles quant à leur interprétation de ces dispositions, avant que le Conseil d'État ne puisse se prononcer en définitive sur la dispense du second vote constitutionnel.»

Monsieur le Ministre de la Justice propose d'envoyer un courrier circonstancié au Conseil d'Etat et d'en tenir au courant les membres de la Commission juridique. [Ministère de la Justice]

Article 4

Paragraphe 1^{er}

Le libellé, tel qu'amendé par le Gouvernement, désigne les autorités luxembourgeoises habilitées à présenter des demandes de transmission de données selon le cadre posé par l'Accord.

Paragraphe 2

Le paragraphe 2 précise que les informations transmises au point de contact luxembourgeois peuvent être utilisées par les autorités répressives luxembourgeoises de la même manière que celles obtenues par voie d'entraide judiciaire en matière pénale sous réserve des modalités indiquées par l'Accord.

Echange de vues

- ❖ Un membre du groupe politique LSAP est d'avis que les deux interrogations soulevées par le Conseil d'Etat à l'endroit du paragraphe 3 de l'article 3 méritent d'être examinées plus amplement par la commission.

Monsieur le Ministre de la Justice propose d'y revenir une fois que le Conseil d'Etat s'est prononcé sur le courrier circonstancié lequel le ministère de la Justice propose de lui envoyer.

- ❖ Un membre du groupe politique CSV donne à considérer qu'il faut veiller, eu égard à la propension américaine de conférer une compétence universelle, au niveau de la mise en œuvre de l'Accord que toute transmission d'informations soit conforme au principe de la spécialité.

Il convient d'éviter que des informations transmises en toute régularité puissent être détournées pour être utilisées à des fins tout autres et étrangères au cadre autorisé de l'Accord.

- ❖ Un membre du groupe politique DP souligne qu'il importe d'adopter une approche restrictive.

Le représentant du Ministère de la Justice explique que l'architecture du système proposé repose sur deux phases distinctes.

Dans un premier temps, il y a un échange d'information par le biais de la recherche et de la comparaison automatisée d'empreintes digitales et de profils d'ADN dans les bases de données luxembourgeoise et américaine.

Dans le cas de figure d'une concordance, des informations à caractère personnel et non-personnel à des fins de prévention du terrorisme sont, dans une deuxième phase, transmises par le biais du point de contact respectif désigné. Cet échange d'informations se fait de manière non automatisée.

- ❖ Un membre du groupe politique CSV se demande si la Commission européenne, dans le cadre des négociations menées dans le cadre du TTIP (*Transatlantic Trade and Investment Partnership*) et du TISA (*Trade in Services Agreement*), même si les deux arrêts de la Cour de justice de l'Union européenne pré-mentionnés ne devraient pas être sans conséquence, parvient à imposer le maintien de certains niveaux standards propres à l'Union européenne.

Monsieur le Ministre de la Justice donne à considérer que la Commission européenne est bien consciente de l'impact de la jurisprudence récente de la juridiction européenne. Il estime partant qu'elle ne peut pas ne pas en tenir compte comme l'accord futur devra rencontrer l'approbation du Parlement européen qui affiche un regard très critique quant au TTISP et TISA.

4. Divers

1) Demande de convocation d'une réunion du groupe politique CSV du 21 août 2015 portant sur les solutions proposées en vue de rencontrer les problèmes liées à la mendicité

Un membre du groupe politique CSV déplore qu'à ce jour, deux mois après la notification de ladite demande de convocation, aucune réunion à ce sujet n'ait été convoquée.

L'orateur renvoie aux réunions du 16 septembre 2015 (cf. P.V. J 30) et à celle du 7 octobre 2015 (cf. P.V. J 32) où ce point a été abordé à chaque fois sur sa demande.

Il rappelle que cette demande de convocation a été faite suite aux déclarations faites tant par Monsieur le Premier Ministre, Ministre d'Etat, que par Monsieur le Ministre de la Sécurité intérieure.

L'orateur informe les membres de la commission que son groupe politique est d'accord, compte tenu des nombreux engagements de Monsieur le Ministre de la Sécurité, pris à raison de ses multiples responsabilités ministérielles, d'inviter Monsieur le Ministre de la Justice ainsi que des représentants du parquet général et de la Police Grand-ducale.

Les membres de la commission décident, compte tenu des disponibilités de Monsieur le Ministre de la Justice, de fixer cette réunion au mercredi 18 novembre 2015 de 13h00 à 14h00.

Cette réunion a été reportée, postérieurement à la tenue de la présente réunion, au **jeudi 19 novembre 2015 de 12h30 à 13h50**.

2) Réforme de la Cour de Justice de l'Union européenne – augmentation des postes de magistrats – accord de principe intervenu

Monsieur le Ministre de la Justice informe les membres de la commission qu'un accord de principe a pu être trouvé au niveau du Conseil JAI, du Parlement européen et de la Commission européenne. Il reste encore l'étape de validation au sein du COREP.

Ledit accord comporte l'obligation, par voie de déclaration politique, d'assurer la parité des sexes lors de la nomination future des magistrats par les Etats membres. Cette condition ne saura être consacrée sur le plan légal formel afin d'éviter à introduire un critère de nomination supplémentaire contraire aux dispositions des traités régissant l'Union européenne.

La Cour de Justice de l'Union européenne se voit renforcée au niveau des magistrats qui passeront de 28 magistrats à 56, y compris les 8 magistrats affectés au Tribunal de la fonction publique qui sera fusionné avec le Tribunal de 1^{ère} instance.

Ce renforcement se fera en trois étapes. Les Etats membres sont désignés par lots (trois lots successifs) pour procéder à la nomination d'un magistrat supplémentaire. En effet, chaque Etat membre a désormais droit à deux magistrats.

Le Luxembourg faisant partie des pays du premier lot, procédera prochainement à la nomination du magistrat supplémentaire. Cette décision dûment motivée sera prise en Conseil de Gouvernement (avant la fin de cette année) qui ne compte pas lancer une procédure d'appel à candidature, comme c'était le cas lors de la dernière nomination d'un

magistrat à la Cour de Justice de l'Union européenne. Cette façon de procéder avait essuyé à l'époque de nombreuses critiques.

Une fois ce renforcement complétée, toute nouvelle nomination par les Etats membres portera sur deux magistrats avec respect de la parité homme/femme.

En ce qui concerne la capacité d'accueil de la Cour de Justice de l'Union européenne, il convient de renvoyer au projet de loi 6825 relatif à la construction de la 5^e extension de la Cour de Justice de l'Union européenne dont le rapport a été adopté par la Commission du Développement durable en date du 15 octobre 2015. Cette 5^e extension comporte notamment la construction d'une 3^e tour adjacente aux deux tours préexistantes.

Le secrétaire-administrateur,
Laurent Besch

La Présidente de la Commission juridique,
Viviane Loschetter

La Présidente de la Commission de
l'Enseignement supérieur, de la Recherche,
des Médias, des Communications et de
l'Espace,
Simone Beissel



Commission juridique

Procès-verbal de la réunion du 11 février 2015

Ordre du jour :

1. Echange de vues sur la lutte contre le terrorisme (*demande du groupe politique CSV*)
2. Approbation des projets de procès-verbal de la réunion jointe du 28 janvier 2015 et de la réunion du 4 février 2015
3. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques
- Présentation du projet de loi

(Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne)

4. Divers

*

Présents : Mme Cécile Hemmen remplaçant M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Alex Bodry, M. Franz Fayot, M. Léon Gloden, Mme Josée Lorsché, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth

M. Serge Urbany, M. Justin Turpel, députés (*observateurs*)

M. Félix Braz, Ministre de la Justice

M. Luc Reding, du Ministère de la Justice

M. Patrick Heck, Directeur du Service de Renseignement de l'Etat

M. Robert Biever, Procureur général d'Etat

M. Georges Oswald, Procureur d'Etat adjoint

M. Laurent Besch, de l'Administration parlementaire

Excusé : M. Marc Angel

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission

*

1. Echange de vues sur la lutte contre le terrorisme (*demande du groupe politique CSV*)

Introduction

Un représentant du groupe politique CSV énonce les deux raisons ayant amené son groupe politique à formuler la demande de mise à l'ordre du jour d'un échange de vues sur la lutte contre le terrorisme, à savoir

1. l'arrestation en date du mercredi 4 février 2015 par les agents de l'unité spéciale de la Police grand-ducale à Pétange d'une personne suspectée d'entretenir des relations avec le milieu islamiste radicalisé, et
2. les déclarations du vice-président de la Shoura parues dans un quotidien luxembourgeois en date du 2 février 2015 selon lesquelles les six personnes identifiées à ce jour comme étant parties en Syrie rejoindre en tant que combattants terroristes étrangers les rangs de l'entité de l'Etat Islamique (connue sous le sigle IS ou encore appelé Daesch) seraient tous membres de l'Association multiculturelle de l'Ouest (AMCO).

L'orateur estime que ces éléments, de même que le fait que la personne arrêtée à Pétange a été remise en liberté le jour même, et déclarations sont de nature à soulever un certain nombre d'interrogations.

Explications

Monsieur le Ministre de la Justice souligne que cette demande, en ce qu'elle impliquerait nécessairement la révélation d'informations couvertes par le secret de l'instruction, pose problème.

Au sujet du premier point de la demande précitée, il souligne que conformément au principe du secret de l'instruction, il ne dispose pas, même en sa qualité de ministre de la Justice, de plus amples informations que celles divulguées par les médias.

En ce qui concerne le deuxième point de ladite demande, l'orateur informe les membres de la commission que cela relève de la compétence du Service de Renseignement de l'Etat dont le ministère d'Etat est l'autorité de tutelle.

Ainsi, les autorités afférentes sont tenues de par la loi de respecter le principe du secret de l'instruction et sont donc liées par le secret professionnel.

M. le Procureur d'Etat adjoint évoque également le principe du secret de l'instruction qui lui interdit, sous peine de s'exposer à des poursuites pénales, de révéler des informations relatives au dossier ayant conduit à l'arrestation et à la libération ultérieure d'une personne à Pétange.

M. le Directeur du Service de Renseignement de l'Etat précise que ce dossier relève de la compétence des autorités judiciaires.

Au sujet des déclarations concernant l'AMCO, il donne à considérer qu'il est tenu, conformément aux dispositions de l'article 16 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat, de respecter l'obligation au secret.

Il rappelle que la Commission de Contrôle parlementaire du Service de Renseignement de l'Etat est régulièrement informée sur l'état de la menace.

Le volet relatif au salafisme constitue une des priorités du Service de Renseignement de l'Etat depuis trois ans et a connu une certaine actualité dès la généralisation du phénomène des départs de personnes vers des terres de jihad / lieux de combat en vue d'y rejoindre des groupes terroristes armés.

Echange de vues

❖ Un membre du groupe politique CSV explique que les détails tels que révélés par la presse à propos de l'arrestation d'une personne à Pétange sont de nature à susciter des interrogations dans l'opinion public.

L'orateur estime qu'il est de son devoir légitime, en tant qu'élu du Parlement, de demander de plus amples informations à ce sujet.

❖ Un autre membre du groupe politique CSV conclut que les autorités confirment tenir à une application conforme du principe du secret de l'instruction et ce pour tous les dossiers en cours. L'orateur ne peut qu'approuver cette volonté et souligne qu'il convient d'assurer une mise en œuvre égalitaire et univoque et ce quelque soit les tenants et les circonstances propres à un dossier pénal.

❖ M. le Procureur général d'Etat est d'avis qu'indépendamment du fait que certaines informations, qu'elles soient vraies ou fausses, soient rendues publics, il n'appartient certainement pas aux autorités judiciaires d'y réagir et de porter atteinte, voire de saper le principe du secret de l'instruction. Il s'agit d'un élément fondamental d'un Etat de droit.

❖ Monsieur le Ministre de la Justice déclare ne pouvoir qu'approuver le souci premier des autorités judiciaires d'assurer le respect, dans toute son intégralité et étendue, du principe du secret de l'instruction. Une application univoque n'en est que la suite qui s'impose.

Au sujet de l'état de la menace pour le Luxembourg, il renvoie aux déclarations faites par Monsieur le Premier Ministre, Ministre d'Etat, à l'issue de la réunion du Conseil de Gouvernement du 9 janvier 2015 selon lesquelles il n'existe aucune menace spécifique ni concrète pour le Luxembourg.

Les autorités compétentes se trouvent néanmoins placées en mode de vigilance accrue en vue d'assurer la sécurité du territoire et de la population. Ainsi, toutes les pistes et menaces éventuelles font l'objet d'une attention particulière et sont suivies de près, même si par après, elles se révéleraient être dénuées d'intérêt ou de tout fondement. L'échange d'informations entre les différents acteurs impliqués est régulier et intense.

❖ Un membre du groupe politique CSV estime qu'on ne peut pas reprocher à son groupe politique d'avoir agi de manière irresponsable. En effet, son groupe politique n'a ni pris position ni posé une quelconque question parlementaire ayant un lien avec les faits et informations dont est question sous rubrique.

Il a été ainsi jugé utile d'en discuter dans l'enclos de la Commission juridique; c'est la raison de la demande de mise à l'ordre du jour du groupe politique CSV du 6 février 2015.

- ❖ Un autre membre du groupe politique CSV rappelle sa demande posée dans le cadre de la présentation des projets de loi 6759 et 6761 (*cf. procès-verbal n°13 de la réunion du 4 février 2015*) qui consiste notamment à ce que Monsieur le Ministre de la Justice prenne position au sujet de la consécration légale exigée des notions de donnée «judiciaire» et «policière» et ce sous le point de vue du respect des principes généraux de droit applicables en droit luxembourgeois.
- ❖ Mme la Présidente de la commission rappelle qu'on y revient une fois que les informations telles que demandées au cours de la réunion précitée du 4 février 2015 ont été communiquées aux membres de la Commission juridique.

2. Approbation des projets de procès-verbal de la réunion jointe du 28 janvier 2015 et de la réunion du 4 février 2015

Les deux projets de procès-verbal rencontrent l'assentiment unanime des membres de la commission.

3. 6763 Projet de loi portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

I. Présentation du projet de loi

Introduction

Le texte de loi tel que proposé vise à adapter le cadre légal relatif à la rétention des données de télécommunications à des fins de poursuite aux exigences telles que découlant des arrêts C-293/12 et C-594/12 du 8 avril 2014 de la Cour de Justice de l'Union européenne, communément connu sous le sigle «*arrêt Digital Rights*».

Ledit arrêt a invalidé la directive 2006/24/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves. Or, le cadre luxembourgeois ayant transposé ladite directive n'a pas été invalidé.

Ladite directive a été transposée en droit luxembourgeois par des modifications

- du Code d'instruction criminelle, dont essentiellement l'article 67-1 du Code d'instruction criminelle, et
- de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

M. le Ministre de la Justice explique que la lecture de «*l'arrêt Digital Rights*» n'est pas aisée à raison des nombreuses considérations et points développés par la Cour de Justice de l'Union européenne. L'interprétation concernant notamment les considérations tenant au principe de la rétention des données est loin d'être univoque.

Ainsi, certains affirment, à la lecture dudit arrêt, que le principe de la rétention de données de télécommunications aurait été invalidé tandis que d'autres proclament bien le contraire.

Devant ce constat et malgré l'existence d'un certain flou juridique, il a été jugé utile de procéder à une adaptation ponctuelle du dispositif légal national, sans pour autant aménager, pour le moment, le principe de la rétention des données.

A ce sujet, l'orateur souligne qu'il ne convient pas d'ignorer la dimension européenne. En effet, la Cour de Justice de l'Union européenne ayant invalidé une directive, il paraît plus que logique de déterminer et de formaliser une position sur le plan communautaire qui s'imposera à l'ensemble des Etats membres de l'Union européenne.

Il informe les membres de la commission que dans certains Etats membres de l'Union européenne, la législation nationale prise en application de la directive précitée du 15 mars 2006 en ce qu'elle comporte le principe de la rétention des données, a été, dans le cadre d'un procès judiciaire, invalidée par les cours et tribunaux.

L'idée est donc de procéder, sur le plan national, aux adaptations ponctuelles et de soutenir activement, sur le plan européen, la formalisation d'une approche cohérente et univoque quant au principe de la rétention des données. Sur ce point, il convient de noter que la Commission européenne a promis d'initier une proposition de texte.

Il se peut que ce thème figurera à l'agenda de la présidence luxembourgeoise de l'Union européenne au cours du second semestre de cette année.

Article 1^{er} du projet de loi – modifications de l'article 67-1 du Code d'instruction criminelle

Point 1) – paragraphe (1)

Il est proposé de remplacer, à l'endroit de l'article 67-1, paragraphe (1), le seuil de peine des infractions pour lesquelles les autorités judiciaires peuvent avoir recours aux données de télécommunications retenues par les opérateurs par une liste précise d'infractions qu'il est proposé de faire figurer en tant que paragraphe (4) nouveau.

Point 2) – nouveau paragraphe (4)

Le nouveau paragraphe (4) qu'il est proposé d'adjoindre à l'article 67-1 du Code d'instruction criminelle énumère les catégories d'infractions, trente-trois au total, pour lesquelles les autorités judiciaires peuvent avoir accès aux données de télécommunication retenues.

Article 2 du projet de loi – modifications de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Point 1) – modification de l'article 5, paragraphe (1), lettre a)

Il s'agit d'adapter le libellé de la lettre a) du paragraphe (1) de l'article 5 à la modification proposée à l'endroit de l'article 67-1 du Code d'instruction criminelle en ce qui concerne le remplacement du seuil de peine des infractions par celui d'une liste précise d'infractions.

Point 2) – modification de l'article 5, paragraphe (1), lettre b)

Il est proposé de prévoir que les données relatives au trafic devront être effacées au bout de six mois de manière irrémédiable et immédiate, sauf celles qui ont été accessibles et préservées légalement.

Ainsi, à l'issue dudit délai légal, il n'est plus possible de sauvegarder les données afférentes sous une forme anonymisée.

Point 3) – modification de l'article 5, paragraphe (6)

Il est proposé de relever pour des raisons de dissuasion les peines d'emprisonnement.

Point 4) – modification de l'article 5-1

Le libellé actuel de l'article 5-1 est remplacé par un nouveau libellé.

Les opérateurs de télécommunications seront tenus de conserver les données retenues sur le territoire de l'Union européenne. Il s'agit de s'assurer que les règles de protection des personnes à l'égard du traitement de données en vigueur au sein de l'Union européenne s'appliquent (*paragraphe (1)*).

Il est proposé de déterminer les dispositions d'exécution et tenant à des contraintes d'ordre technique dont un règlement grand-ducal. Cela permettra, à raison des évolutions techniques propres en le domaine, de tenir à jour les dispositions prescrites en vue d'assurer la confidentialité et l'intégrité des données à caractère personnel retenues.

Point 5) – modification de l'article 9, paragraphe (1), lettre a)

Il s'agit, à l'instar de la modification proposée à l'endroit du point 1) ci-avant, d'adapter le libellé de la lettre a) du paragraphe (1) de l'article 9.

Il convient de rappeler que l'article 5, paragraphe (1), lettre a) traite des données relatives au trafic de télécommunications, alors que le point a) du paragraphe (1) de l'article 9 vise les données de localisation.

Point 6) – modification de l'article 9, paragraphe (1), point b)

A l'instar de la modification proposée à l'endroit du point 2) ci-avant, il convient d'adapter le libellé de la lettre b) du paragraphe (1) de l'article 9.

Point 7) – modification de l'article 9, paragraphe (6)

Il est proposé, à l'instar de la modification telle que proposée à l'endroit du point 3) ci-avant, d'adapter le texte du paragraphe (6) de l'article 9.

II. Echange de vues

De l'échange de vues qui s'ensuit, il y a lieu de retenir les éléments suivants:

- ❖ Un membre du groupe politique CSV déclare que les propositions telles qu'envisagées correspondent aux préoccupations exprimées par son groupe politique et rencontrent partant son accord.

Il demande de vérifier le caractère pertinent et dissuasif de l'ensemble des dispositions pénales prévoyant des peines d'amendes et d'emprisonnement et figurant dans les dispositions du cadre légal relatif à la protection des données à caractère personnel. Le cas échéant, il convient de les adapter à l'image des modifications telles que proposées dans le cadre du projet de loi 6763 sous examen.

Quant au principe de la rétention des données de télécommunications

- ❖ Un membre de la sensibilité politique déi Lénk (observateur) remémore la position de son groupe telle que consignée dans le procès-verbal relatif à la réunion jointe du 16 juillet 2014 (PV J26 / PV ERMCE 31).

Il rappelle que le principe de la rétention des données de télécommunication est disproportionné eu égard au résultat escompté.

Il fait observer que malgré les adaptations d'ordre technique telles que proposées par le projet de loi sous examen le principe même de la rétention des données est maintenu dans son intégralité. Ainsi, le Gouvernement a pris, certes de manière indirecte, position.

A raison du souci exprimé par les autorités judiciaires en ce que la rétention des données de télécommunication constitue un outil de travail indispensable dans le cadre de l'exécution de leur mission, l'orateur propose d'entendre des experts afférents, dont notamment M. Mark Cole¹ de l'Université du Luxembourg.

Devant le constat de l'argument invoqué en faveur du maintien, du moins en attente d'une initiative européenne, du principe de la rétention des données de télécommunications afin de permettre aux autorités répressives de disposer d'un outil qualifié par eux-mêmes de nécessaire, l'orateur rappelle que la sensibilité politique déi Lénk maintient sa position en faveur de l'abandon de ce principe. En d'autres termes, le maintien de la rétention des données de télécommunication est justifié pour des seules considérations de nécessité, indépendamment de toute considération quant au fond et au principe même.

L'orateur demande au ministère de la Justice de communiquer aux membres de la commission le projet de règlement grand-ducal visé à l'endroit du paragraphe (2) de l'article 5-1 nouvellement libellé qu'il est proposé de remplacer le texte actuel de l'article 5-1 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Monsieur le Ministre de la Justice explique qu'il existe une multitude de solutions envisageables autres que l'alternative consistant en le maintien ou l'abandon de la rétention des données à caractère personnel.

Le représentant de la sensibilité politique déi Lénk estime qu'une solution nationale représente certes un certain intérêt. Ainsi, on pourrait utilement avancer en ce domaine sans que cela soit de nature à porter préjudice à l'adoption d'une position commune sur le plan de l'Union européenne. Il cite la législation autrichienne.

L'obligation de conserver des données retenues sur le territoire de l'Union européenne traduit une bonne volonté, encore faut-il en apprécier la faisabilité sur le plan technique.

¹ M. Mark Cole, Professeur en Droit des Nouvelles Technologies de l'Information, des Médias et des Communications auprès de l'Université du Luxembourg

De manière générale, l'orateur est d'avis qu'il convient de veiller à la protection des données à caractère personnel dans le cadre d'autres initiatives comme celle du Partenariat transatlantique de commerce et d'investissement (TTIP).

Un membre du groupe politique CSV est d'avis que rien ne s'oppose à ce que la loi luxembourgeoise, dans son application souveraine et indépendamment de toute considération au niveau européenne, prescrit un cadre mettant l'accent sur la sauvegarde de la protection des données à caractère personnel. Cela vaut d'ailleurs également pour tout droit fondamental.

Au sujet du cadre légal autrichien, Monsieur le Ministre de la Justice précise que les modifications intervenues font suite à un arrêt afférent de la Cour constitutionnelle autrichienne (Verfassungsgerichtshof).

Projet de règlement grand-ducal (nouveau libellé proposé pour l'article 5-1, paragraphe (2))

- ❖ Un membre du groupe politique CSV renvoie, au sujet dudit règlement grand-ducal, à l'article 11, paragraphe (3) qui dispose que «*L'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi.*». Cette disposition soit être lue ensemble avec l'article 32, paragraphe (3) de la Constitution qui dispose que «*Dans les matières réservées à la loi par la Constitution, le Grand-Duc ne peut prendre des règlements et arrêtés qu'aux fins, dans les conditions et suivant les modalités spécifiées par la loi.*»

Ainsi, il se peut que le recours à un règlement grand-ducal pour déterminer les dispositions d'exécution plus détaillées en vue d'assurer la pleine intégrité et la confidentialité des données de télécommunication ne soit pas conforme à la Constitution.

De plus, l'objet même de ce règlement grand-ducal en limite son champ d'application.

Monsieur le Ministre de la Justice précise que l'objet dudit règlement grand-ducal est de prescrire les mesures de sécurité devant être prises et mises en œuvre par les opérateurs en vue d'assurer le respect de la protection des données à caractère personnel.

Il renvoie à cet égard au règlement grand-ducal relatif à Visupol (projet de vidéosurveillance de la Police grand-ducale), à savoir le règlement grand-ducal du 1^{er} août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance dans des zones de sécurité qui n'a pas essuyé des critiques, voire une opposition formelle de la part du Conseil d'Etat.

Les zones de sécurité ont été définies par voie de règlements ministériels prorogés depuis à plusieurs reprises.

Un membre du groupe politique CSV fait remarquer que l'article 11, paragraphe (3) de la Constitution a été introduite par une loi du 29 mars 2007 portant 1. révision des paragraphes (1), (3), (4), (5) et (6), alinéa 1er de l'article 11 de la Constitution; 2. création d'un article 11bis nouveau de la Constitution.

Il renvoie au projet de règlement grand-ducal concernant la saisie et le traitement des données nominatives des élèves qui a essuyé, dans sa version initiale, une opposition formelle de la part du Conseil d'Etat.

Liste d'infractions (modifications de l'article 67-1 du Code d'instruction criminelle)

- ❖ Un membre du groupe politique LSAP aimerait disposer de plus amples informations quant à l'établissement de la liste des 33 infractions pour lesquelles les autorités judiciaires peuvent avoir recours aux données relatives au trafic retenues par les opérateurs.

Le représentant du ministère de la Justice explique que cette liste s'inspire de celle prévue à l'annexe D de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête en matière pénale. Il s'agit d'une disposition formelle récente et présentant un lien connexe avec le projet de loi 6763 sous examen.

La liste a été adaptée en fonction des dispositions afférentes du Code pénal et de certaines lois spéciales et comparée à d'autres listes préexistantes dans le droit pénal luxembourgeois. Les autorités judiciaires, auxquelles la liste a été communiquée pour avis, l'ont qualifié d'adéquate.

Monsieur le Ministre de la Justice explique que le Gouvernement optera à l'avenir pour la technique d'une liste d'infraction en lieu et place du seuil de peine des infractions.

Dimension européenne – état des discussions quant au principe de la rétention des données de télécommunication

- ❖ Un membre du groupe politique CSV s'interroge sur le maintien des exigences formelles et procédurales en matière de la protection des données à caractère personnel qui ne se limite pas au seul domaine judiciaire et juridique. Il convient d'adopter une attitude désormais transversale qui devra se caractériser par une approche cohérente et conséquente.

Il aimerait connaître l'évolution actuelle du dossier au niveau européen, notamment en ce qui concerne les aboutissements en vue d'arrêter une position commune sur le principe de la rétention des données.

M. le Ministre de la Justice explique que les discussions au niveau européen sont laborieuses.

Le Conseil européen a accentué la pression et a posé comme principe de trouver en premier lieu une position commune quant au cadre des droits et de ne définir que dans un deuxième temps les dérogations régulièrement admises.

Ainsi, le calendrier impose que les considérations générales afférentes soient fixées pour au plus tard fin 2015.

L'orateur informe les membres de la commission que le Luxembourg prône, quant au principe de la rétention des données, une solution au niveau européen.

A cet égard il donne à considérer que le simple abandon dudit principe sur le seul plan national n'aurait guère qu'une portée pratique étant donné l'exiguïté du territoire et des conséquences qui vont de pair sur le plan technique. Ainsi, seule une solution sur le plan européen dans le cadre et dans l'intérêt de l'espace de liberté, de sécurité et de justice s'impose.

Loi du 18 juillet 2014 portant approbation de la Convention de Budapest sur la cybercriminalité et le droit à l'oubli numérique

- ❖ Un membre du groupe politique LSAP s'interroge sur la nécessité d'adapter la loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

L'orateur s'enquière sur l'incidence éventuelle de l'arrêt de la Cour de Justice du 13 mai 2014 (C-131/12 «Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González») ayant consacré le droit à l'oubli numérique sur la législation luxembourgeoise.

Monsieur le Ministre de la Justice explique que la loi précitée ne peut être comparée au projet de loi sous examen. En effet, dans le cadre de l'application de la loi précitée du 18 juillet 2014, les informations retenues obéissent à la logique du «quickfreeze» (approche non rétrospective), tandis que dans le cadre de la rétention de données relatives au trafic, la mesure peut être mise en œuvre par les autorités judiciaires dans les conditions légales sans qu'il existe un élément prédéterminant de suspicion (technique du «backfreeze», approche rétrospective).

Au sujet de l'arrêt de la Cour de Justice ayant consacré le droit à l'oubli numérique, il explique que cela relève de la compétence du ministère d'Etat, Service des Médias et des Communications.

III. Suites à réserver à l'instruction parlementaire du projet de loi 6763

La commission décide d'organiser, une fois l'avis afférent du Conseil d'Etat disponible, une commission jointe de la Commission juridique et de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace.

Le ministère de la Justice communiquera le projet de règlement grand-ducal aux membres de la Commission juridique [ministère de la Justice].

L'étude scientifique élaborée par M. Mark Cole sera communiquée aux membres de la Commission juridique.

4. Divers

Calendrier

La prochaine réunion de la commission aura lieu le mercredi 25 février 2015 à 09h00.

Le secrétaire-administrateur,
Laurent Besch

La Présidente,
Viviane Loschetter