

N° 6514⁷**CHAMBRE DES DEPUTES**

Session extraordinaire 2013-2014

PROJET DE LOI

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**

* * *

RAPPORT DE LA COMMISSION JURIDIQUE

(28.5.2014)

La Commission se compose de: Mme Viviane LOSCHETTER, Présidente; M. Guy ARENDT, Rapporteur; M. Marc ANGEL, Mme Simone BEISSEL, MM. Alex BODRY, Franz FAYOT, Léon GLODEN, Mme Josée LORSCHHE, M. Paul-Henri MEYERS, Mme Octavie MODERT, M. Laurent MOSAR, Mme Lydie POLFER, MM. Roy REDING et Gilles ROTH, Membres.

*

I. ANTECEDENTS

Le projet de loi sous rubrique a été déposé à la Chambre des Députés le 12 décembre 2012 par le Ministre de la Justice.

Le texte du projet était accompagné d'un exposé des motifs et d'un commentaire des articles. Etaient annexés le texte de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, ainsi que le texte 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.

La Chambre de Commerce a rendu son avis le 27 février 2013.

Le Conseil d'Etat a avisé le projet de loi en date du 16 avril 2013.

Lors de sa réunion du 17 avril 2013, la Commission juridique a désigné Monsieur Gilles Roth comme rapporteur du projet de loi. La commission était alors composée de: M. Gilles ROTH, Président; MM. Marc ANGEL, Xavier BETTEL, Alex BODRY, Félix BRAZ, Mme Christine DOERNER, MM. Léon GLODEN, Jacques-Yves HENCKES, Jean-Pierre KLEIN, Paul-Henri MEYERS, Mme Lydie POLFER et M. Lucien WEILER, Membres.

La Commission juridique a examiné le projet de loi ainsi que l'avis du Conseil d'Etat au cours de trois réunions, à savoir le 17 avril 2013 et les 8 et 15 mai 2013.

Le 5 juin 2013, elle a examiné et adopté une série d'amendements parlementaires.

L'avis complémentaire du Conseil d'Etat est parvenu à la Chambre des Députés en date du 12 novembre 2013.

Dans le cadre de la séance constitutive de la Chambre des Députés issue des élections législatives anticipées du 20 octobre 2013, la Commission juridique fut instituée lors de la séance publique du 5 décembre 2013 avec la composition suivante: Mme Viviane LOSCHETTER, Présidente; MM. Marc ANGEL, Guy ARENDT, Mme Simone BEISSEL, MM. Alex BODRY, Franz FAYOT, Léon GLODEN, Paul-Henri MEYERS, Mme Octavie MODERT, M. Laurent MOSAR, Mme Lydie POLFER, MM. Roy REDING et Gilles ROTH, Membres. Mme Josée LORSCHÉ est admise comme nouveau membre de la commission en date du 11 mars 2014.

La Commission juridique a, lors de sa réunion du 22 janvier 2014, désigné Monsieur Guy ARENDT comme nouveau rapporteur du projet de loi.

En date du 26 février 2014, la Commission juridique a examiné l'avis complémentaire du Conseil d'Etat du 12 novembre 2013.

Une série d'amendements parlementaires a été examinée et adoptée le 19 mars 2014.

Le deuxième avis complémentaire du Conseil d'Etat, rendu le 4 avril 2014, a été examiné par la Commission juridique lors de sa réunion du 23 avril 2014.

Le présent rapport a été adopté par les membres de la Commission juridique le 28 mai 2014.

*

II. CONSIDERATIONS GENERALES

Le projet de loi sous rubrique a comme objet d'approuver la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001 ainsi que le Protocole additionnel à cette Convention, 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. Par conséquent, une série de dispositions légales, notamment de droit pénal et de procédure pénale, doivent être adaptées. Dans ce sens, le présent projet de loi vise à renforcer la lutte contre la cybercriminalité de manière générale et également en ce qui concerne les actes de racisme et de xénophobie commis par le biais de systèmes informatiques.

Ainsi, la Convention du Conseil de l'Europe sur la cybercriminalité est un instrument juridique exhaustif qui couvre tous les aspects importants de la lutte contre la cybercriminalité en établissant une terminologie, en harmonisant les éléments d'infractions prévus par le droit pénal matériel, en fournissant au droit procédural les moyens nécessaires à la poursuite des infractions et en mettant en place un régime rapide de coopération internationale.

Suite à de profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques, la raison d'être du Protocole additionnel s'explique par la nécessité de combattre sur un plan international les actes de racisme et de xénophobie commis par le biais de systèmes informatiques. Les réseaux informatiques et l'information électronique sont de plus en plus utilisés pour commettre des infractions pénales.

L'approbation des deux instruments internationaux prémentionnés facilite la détection, l'investigation et la poursuite d'infractions tant au plan national qu'au niveau international et prévoit des dispositions matérielles en vue d'une coopération internationale rapide et fiable.

*

III. AVIS DU CONSEIL D'ETAT

1. Avis du 16 avril 2013

Dans son avis du 16 avril 2013, le Conseil d'Etat émet une série de remarques.

D'abord, il prend position par rapport à certaines observations des auteurs du projet de loi. Alors que ces derniers indiquent que dans un avenir très proche, une directive de l'Union européenne en la matière sera adoptée et que cette directive sera „*transposée avant la lettre dans le cadre du présent*

projet de loi“, le Conseil d’Etat rappelle qu’il a déjà souligné les difficultés inhérentes à des initiatives concurrentes et à l’adoption de textes qui ne sont pas toujours cohérents au niveau du Conseil de l’Europe et de l’Union européenne. Il continue à noter que cette situation oblige le législateur national à des adaptations successives de son dispositif légal. Même si les auteurs estiment que l’adoption du présent projet de loi anticipe les modifications impliquées par la future directive de l’Union européenne, le Conseil d’Etat se demande si une loi globale et unique couvrant les trois instruments européens, la Convention, le Protocole et la future Directive, n’aurait pas été plus appropriée.

Ensuite, le Conseil d’Etat relève que le projet de loi comporte plusieurs dispositions qui sont sans lien direct avec le contenu de la Convention et du Protocole précités, et qui risquent d’être mal comprises comme n’étant pas imposées par les instruments internationaux en question. D’un point de vue légistique, le Conseil d’Etat aurait préféré que le projet de loi aurait été scindé en deux projets de loi distincts, dont l’un se rapporte à l’approbation de la Convention et du Protocole, reprenant les articles 1er et 2 du projet de loi sous avis, et l’autre regroupant les dispositions des articles 3 à 5 du projet de loi sous référence.

En ce qui concerne l’examen des articles, le Conseil d’Etat émet certaines remarques reprises ci-après sous le point „*V. Commentaire des articles*“.

2. 1er avis complémentaire du 13 novembre 2013 et 2. avis complémentaire du 4 avril 2014

Dans ses avis complémentaires du 12 novembre 2013 et du 4 avril 2014, le Conseil d’Etat prend position par rapport aux amendements parlementaires adoptés par la Commission juridique le 5 juin 2013 et le 19 mars 2014 respectivement. Ces remarques sont également énoncées ci-après sous le point „*V. Commentaire des articles*“.

*

IV. AVIS DE LA CHAMBRE DE COMMERCE

Dans son avis du 27 février 2013, la Chambre de Commerce approuve le projet de loi sous avis qui contribue sensiblement au renforcement de la lutte contre la cybercriminalité au Luxembourg, mais également à l’échelle internationale. Elle soutient l’idée que le caractère transfrontalier de la cybercriminalité nécessite la mise en place, à travers des instruments internationaux, de mesures de protection des systèmes informatiques mais également de mesures juridiques de prévention et de dissuasion, afin de sécuriser le recours aux technologies de l’information au premier rang desquelles figure l’Internet. Elle voit ces efforts en ligne avec l’ouverture, en date du 11 janvier 2013, du Centre européen de lutte contre la cybercriminalité.

Elle note par ailleurs que le projet de loi sous avis tend à renforcer le cadre législatif luxembourgeois de l’économie numérique et partant la crédibilité du Luxembourg dans ce secteur en pleine expansion.

Elle salue le projet de loi particulièrement pour les raisons suivantes:

- La préservation de la cohérence du droit pénal national par le choix pour une loi spécifique sur la cybercriminalité et par l’harmonisation du seuil minimal de la peine d’emprisonnement éventuellement encourue en cas d’infractions informatiques sur une durée de quatre mois;
- Le renforcement de la sécurité juridique par
 - (i) l’élargissement de l’infraction d’*usurpation d’identité* au cas d’usurpation faite dans un cadre non public de nom (nom de société) ou d’une identification de quelque nature qu’elle soit;
 - (ii) par l’appréhension par le droit pénal de la technique de l’*hameçonnage* (ou *phishing*), utilisée par des fraudeurs pour obtenir des renseignements personnels (tels que mot de passe, numéro de compte ou de carte bancaire) par le biais de courriers électroniques, de sites web falsifiés ou tous autres moyens électroniques, et
 - (iii) par l’insertion dans le Code pénal de l’*interception ou tentative d’interception de données informatiques* ainsi que de l’*abus de dispositif*;
- Le renforcement de la lutte contre le blanchiment et le financement du terrorisme grâce au fait que les infractions informatiques sont érigées en infractions primaires. A cet égard, la Chambre de

Commerce se félicite que le projet de loi s'inscrit en conformité avec les nouvelles recommandations du GAFI et de la proposition de 4ème directive de lutte contre le blanchiment et le financement du terrorisme; et

- La dotation du droit procédural par de véritables moyens de lutte contre les infractions informatiques par des pouvoirs additionnels du juge d'instruction et des officiers de police judiciaire.

En ce qui concerne le commentaire des articles, la Chambre de Commerce émet une série de remarques, reprise ci-après sous le point „*V. Commentaire des articles*“.

*

V. COMMENTAIRE DES ARTICLES

Article 1er du projet de loi

Cet article porte approbation de la Convention du Conseil de l'Europe sur la cybercriminalité.

Cet article n'appelle pas d'observations de la part du Conseil d'Etat dans son avis du 16 avril 2013.

Article 2 du projet de loi

Cet article porte 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.

Cet article n'appelle pas d'observations de la part du Conseil d'Etat dans son avis du 16 avril 2013.

Article 3 du projet de loi – Modifications du Code pénal

Point 1) initial

Le Conseil d'Etat, dans son avis du 16 avril 2013, a soulevé à propos du point 1) de l'article 3 du projet de loi que la prise d'un faux nom ou d'un faux identifiant dans des rapports particuliers ne serait pas visée, la publicité faisant défaut.

L'idée derrière la modification telle que proposée par les auteurs du texte était d'étendre le faux nom (uniquement le nom patronymique étant visé par le texte actuel) à tout faux identifiant utilisé dans les rapports entre particuliers en public, la notion de „*public*“ étant interprétée de manière très large par la jurisprudence.

Les réserves émises à l'égard du point 1) initial par le Conseil d'Etat, dans son avis du 16 avril 2013, étant partagées par les membres de la Commission juridique qui considèrent que cette modification n'est pas impérative dans le cadre de la ratification de la Convention et de son Protocole, il est proposé de supprimer, par voie d'amendement parlementaire, le point 1) de l'article 3 du projet de loi.

La suppression du point 1) implique la renumérotation du point 2) initial en point 1) nouveau.

Cet amendement n'appelle pas d'observations du Conseil d'Etat, dans son avis complémentaire du 12 novembre 2013.

Point 1) nouveau (Point 2) initial) – Article 231bis du Code pénal

Afin de tenir compte notamment des comportements dans les réseaux sociaux, il est introduit un nouvel article 231bis du Code pénal pour réprimer l'usurpation d'identité commise dans le but de causer un dommage. L'article 231bis du Code pénal n'exige aucune publicité, mais uniquement l'intention de nuire à un tiers pour rendre répréhensible l'usurpation d'identité.

Dès que l'intention de l'usurpateur est celle de porter atteinte aux droits d'autrui, il n'y a plus lieu d'exiger une quelconque publicité. En effet, si une personne cause des torts à autrui, même dans un cercle restreint de personnes (et donc en dehors du public), il n'y a aucune raison de ne pas réprimer ce comportement hautement dommageable à la victime.

Puisque l'article 231bis va de pair avec les articles 442-2 et 443 du Code pénal, il y a lieu de prévoir, comme pour ces articles, la nécessité d'une plainte de la victime. Les peines sont également inspirées par celles des articles 442-2 et 444 du Code pénal.

Dans son avis du 16 avril 2013, le Conseil d'Etat rappelle que le nouvel article 231bis du Code pénal vise à incriminer l'usurpation d'un nom ou d'un identifiant en vue de nuire à autrui. Il note que

c'est cette disposition, et non pas celle de l'article 231 du Code pénal, qui reprend en substance l'article 226-4-1 du Code pénal français. L'usurpation prohibée du nom peut se faire en public ou dans le cadre de rapports particuliers. Le Conseil d'Etat comprend la pertinence de la nouvelle incrimination tout en formulant deux observations. „*Il se demande pourquoi les auteurs n'ont pas repris tels quels les termes du Code pénal français qui présentent l'avantage de consacrer l'idée de l'usurpation et englobent l'atteinte portée à la personne dont l'identité est usurpée et à des tiers qui peuvent être affectés. Le texte français a été inséré, à bon escient, dans une section consacrée à l'atteinte à la vie privée.*

Aussi le Conseil d'Etat considère-t-il qu'il eût été plus approprié d'insérer l'article en cause dans le Chapitre V du Titre VIII du Livre II du Code pénal, qui porte sur les atteintes à l'honneur et à la considération des personnes.“

En réponse à ces observations, la Commission juridique indique que l'application du texte français soulève de multiples problèmes. La notion d'„*usurpation d'identité*“ n'y est pas clairement définie. De plus le texte français mélange les notions d'„*usurpation d'identité*“, d'„*affectation de la tranquillité des personnes*“ et d'„*atteinte à l'honneur*“, qui sont trois concepts différents. Le 2e alinéa de la disposition française prévoit que l'infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. Une interprétation *a contrario* de cet alinéa pourrait donc conduire à se demander dans quel(s) cas l'infraction n'est pas punie. Au vu de ces problèmes, il a été jugé préférable d'adapter le texte luxembourgeois, plutôt que de reprendre textuellement la disposition française.

Point 2) nouveau – Article 461, alinéa 1er du Code pénal

Le Conseil d'Etat, dans son avis du 16 avril 2013, relève, à l'endroit du point 4) initial (article 496, alinéa 1er du Code pénal), une divergence qui existerait désormais entre l'infraction d'escroquerie (article 496 du Code pénal) où l'on a rajouté la notion de „*clef électronique*“ dans la définition des objets visés et celle de vol (article 461 du Code pénal) où l'objet de l'infraction resterait d'ordre matériel. Afin de préserver la cohérence des textes, il est proposé de retenir l'orthographe „*clef*“.

Il propose d'ajouter la notion de „*clef électronique*“ dans la définition des objets visés à l'article 461, alinéa 1er du Code pénal.

Dans un souci d'harmonisation des textes il est proposé de suivre la solution proposée par le Conseil d'Etat.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Le Conseil d'Etat, dans son 1er avis complémentaire du 12 novembre 2013, marque son accord avec cet amendement.

Point 3) nouveau – Article 470, alinéas 1er et 2 du Code pénal

Le Conseil d'Etat, dans son avis du 16 avril 2013, relève, à l'endroit du point 4) initial (article 496, alinéa 1er du Code pénal), une divergence qui existerait désormais entre l'infraction d'escroquerie (article 496 du Code pénal) où l'on a rajouté la notion de „*clef électronique*“ dans la définition des objets visés et celle d'„*extorsion*“ (article 470 du Code pénal) où l'objet de l'infraction resterait d'ordre matériel.

Il propose d'ajouter la notion de „*clef électronique*“ dans la définition des objets visés à l'article 470, alinéas 1er et 2 du Code pénal.

Dans un souci d'harmonisation des textes, la Commission juridique décide de suivre la solution proposée par le Conseil d'Etat.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Le Conseil d'Etat approuve cet amendement.

Point 4) nouveau (Point 3) initial) – Article 488 du Code pénal

Il est proposé d'adapter le seuil de peine de l'article 488 du Code pénal à celui prévu au nouvel article 509-5 du Code pénal afin d'obtenir une certaine cohérence au niveau des peines relatives à des infractions informatiques. En effet, les articles 488 et 509-5 du Code pénal prévoient des infractions similaires, à savoir d'un côté la contrefaçon ou l'altération de clefs et, de l'autre côté, la production, la vente, l'obtention, la détention, l'importation, la diffusion ou la mise à disposition dans une intention

frauduleuse d'un mot de passe, d'un code d'accès ou toute autre clef électronique permettant d'accéder au mépris des droits d'autrui à tout ou à partie d'un système de traitement ou de transmission automatisé de données.

Ce point n'appelle pas d'observations de la part du Conseil d'Etat dans son avis du 16 avril 2013.

Or, le seuil de peine du nouvel article 509-5 du Code pénal est relevé par le biais d'un amendement parlementaire adopté le 5 juin 2013 et ce pour tenir compte d'une réflexion de la Chambre de Commerce dans son avis du 27 février 2013 qui regrette à juste titre l'abaissement de l'amende, actuellement de 1.250 euros à 30.000 euros, telle que prévue à l'article 509-4 du Code pénal sur lequel s'aligne le nouvel article 509-5 du Code pénal, et de son remplacement par une amende de 251 euros à 5.000 euros seulement.

Partant, dans un souci de cohérence, la Commission juridique souhaite adapter le seuil de peine de l'article 488 du Code pénal à celui de l'article 509-5 du Code pénal tel que prévu dans un amendement adopté le 5 juin 2013.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Cet amendement n'appelle pas d'observations du Conseil d'Etat dans son avis complémentaire du 12 novembre 2013.

Point 5) nouveau – Article 491, alinéa 1er du Code pénal

Le Conseil d'Etat, dans son avis du 16 avril 2013, relève, à l'endroit du point 4) initial (article 496, alinéa 1er du Code pénal), une divergence qui existerait désormais entre l'infraction d'escroquerie (article 496 du Code pénal) où l'on a rajouté la notion de „clef électronique“ dans la définition des objets visés et celle d'„abus de confiance“ (article 491 du Code pénal) où l'objet de l'infraction resterait d'ordre matériel.

Il propose d'ajouter la notion de „clef électronique“ dans la définition des objets visés à l'article 491 du Code pénal.

Dans un souci d'harmonisation des textes, les membres de la Commission juridique décident de suivre la solution proposée par le Conseil d'Etat en ajoutant, par voie d'amendement parlementaire, un point 5) nouveau.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

En conséquence de cet amendement, les points subséquents sont renumérotés.

Le Conseil d'Etat marque son accord avec cet amendement dans son avis complémentaire du 12 novembre 2013.

Point 6) nouveau (Point 4) initial) – Article 496, alinéa 1er du Code pénal

L'article 496, alinéa 1er du Code pénal est modifié de façon à inclure les clefs électroniques parmi les objets que l'auteur de l'infraction se sera fait remettre ou délivrer ou aura tenté de se faire remettre ou délivrer dans le cadre de l'escroquerie. Il résulte en effet d'un arrêt n° 261/10 du 14 juin 2010 de la Cour d'appel que l'article 496 du Code pénal, dans sa rédaction actuelle, ne permet pas de retenir l'escroquerie pour l'hameçonnage (en anglais „phishing“) d'un mot de passe, opération cependant courante en matière de cybercriminalité.

L'hameçonnage n'étant cependant rien d'autre qu'une escroquerie en vue de se faire délivrer des informations (notamment et surtout des mots de passe, c'est-à-dire des clefs électroniques) en vue de commettre d'autres infractions, il paraît plus logique et plus facile de rajouter simplement les clefs électroniques au texte de l'article 496 du Code pénal que de créer un article séparé.

En outre le seuil de l'emprisonnement minimal d'un mois est augmenté à 4 mois afin d'obtenir une certaine cohérence au niveau des peines relatives à des infractions informatiques.

Le Conseil d'Etat comprend le souci des auteurs du projet de loi de trouver une réponse à un problème actuel récurrent. „[...] Il constate néanmoins que le texte de l'article 496 du Code pénal luxembourgeois sera différent tant de l'article 496 du Code pénal belge que de l'article 313-1 du Code pénal français. Il se demande si la reprise des termes du Code pénal français qui vise la remise „des fonds, des valeurs ou (d') un bien quelconque“ n'aurait pas été plus appropriée étant entendu que le bien peut être corporel ou incorporel. Une telle formule dispenserait le juge pénal du recours assez artificiel au critère de l'impulsion électronique pour distinguer l'objet corporel, objet d'un vol ou d'une escroquerie, de l'objet incorporel non visé par ces dispositions, même après la modification proposée. Si le législateur décide de

suivre les auteurs du projet, il doit encore être conscient de la divergence qui existera désormais entre l'infraction d'escroquerie et celles de vol, d'extorsion ou encore d'abus de confiance où l'objet de l'infraction restera d'ordre matériel. Une solution pourrait consister à ajouter la notion de clef électronique dans la définition des objets visés aux articles 461, 470 ou 491 du Code pénal.

Le Conseil d'Etat attire encore l'attention des auteurs sur le projet de loi n° 6485 portant modification de l'article 567 du Code de commerce sur lequel le Conseil d'Etat a rendu son avis le 12 mars 2012. Ce texte propose de remplacer le concept de marchandises par celui de „bien corporel fongible“ et d'ajouter une référence au „bien incorporel fongible“. Il serait logique que la consécration du concept de bien incorporel dans le Code de commerce soit suivie de sa prise en considération dans le droit pénal. La question se pose avec acuité particulière pour l'article 490 du Code pénal relatif à la banqueroute qui vise la soustraction, la dissimulation ou le recel des „biens meubles et immeubles“ du failli.

Le Conseil d'Etat relève encore une certaine incohérence dans l'approche des auteurs du projet de loi qui, dans le point sous examen, retiennent le seul concept de clef électronique et, à l'endroit du nouvel article 509-5 du Code pénal (article 3, point 10), visent le „mot de passe“, le „code d'accès“ ou „toute autre clef électronique“. Ainsi, „[D]e deux choses l'une: ou bien le concept de clef électronique est le terme générique à consacrer, auquel cas il faudra adapter le texte du nouvel article 509-5 du Code pénal à celui de l'article 496 du Code pénal; ou bien le concept de clef électronique est trop restreint, auquel cas il faudra reprendre, à l'article 496 du Code pénal, tous les concepts de l'article 509-5 du Code pénal. Le Conseil d'Etat renvoie encore, dans ce contexte, à l'article 488 du Code pénal qui consacre déjà le concept de clef électronique.

Au vu de l'ensemble de ces considérations, et à l'image de l'article 313-1 du Code pénal français, le Conseil d'Etat propose de remplacer les termes de „clefs électroniques“, proposés par les auteurs, par l'expression „ou un bien quelconque (corporel ou incorporel)“.

La Commission juridique décide de suivre le Conseil d'Etat en retenant la terminologie de „clef électronique“ et en ajoutant cette notion dans la définition des objets visés aux articles 461, 470 et 491 du Code pénal.

Quant à la terminologie du nouvel article 509-5 du Code pénal, les termes „mot de passe“ et „code d'accès“ étaient cités à titre d'exemples. Les membres de la Commission juridique conviennent de supprimer ces exemples du libellé et de retenir le seul terme de „clef électronique“, étant précisé que la notion de „clef électronique“ englobe les notions de mot de passe et de code d'accès.

Point 7) nouveau (Point 5) initial) – Article 506-1, point 1) du Code pénal

Dans un souci de préserver la cohérence interne du Code pénal, il est proposé d'inclure les nouvelles infractions en matière informatique ainsi que celles qui existent déjà dans la liste des infractions primaires en matière de blanchiment ainsi que certaines infractions connexes commises par le biais de systèmes informatiques et figurant dans la Convention et qui jusqu'ici n'y figuraient pas. Il s'agit d'un choix délibéré pour combler cette lacune existante même s'il ne s'agit pas d'une exigence explicite de la Convention.

Le Conseil d'Etat, dans son avis du 16 avril 2013, relève que le texte proposé relatif à l'article 506-1 point 1) du Code pénal ne tient pas compte des modifications que la loi du 21 juillet 2012 portant approbation du Protocole contre le trafic illicite de migrants par terre, air et mer, signé à Palerme le 12 décembre 2000, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée du 15 novembre 2000 (...) a apportées à l'article 506-1 précité.

Le Conseil d'Etat signale à juste titre que le troisième tiret du texte proposé (modification du point 1) de l'article 506-1 du Code pénal tel que proposé) omet de renvoyer aux articles 382-4 et 382-5 du Code pénal, et que le dix-septième tiret du même texte proposé fait référence à l'article 143 de la loi du 19 août 2008 portant sur la libre circulation des personnes et l'immigration, référence qui a été remplacée par celle à l'article 382-4 du Code pénal.

Il remarque enfin que l'article 143 du Code pénal a été abrogé par la loi précitée du 21 juillet 2012 et propose que la référence prévue au prédit treizième tiret dans sa formulation actuellement en vigueur soit supprimée, alors qu'elle fait double emploi avec le troisième tiret, également introduit par la loi de 2012.

Les membres de la Commission juridique proposent partant, par voie d'amendement parlementaire, de modifier le texte conformément aux propositions du Conseil d'Etat.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Le Conseil d'Etat marque son accord avec cet amendement dans son avis complémentaire du 12 novembre 2013.

Point 8) nouveau (Point 6) initial) – Article 509-3, alinéa 2 (nouveau) du Code pénal

Le point 6) initial (point 8) nouveau) a pour objet de compléter l'article 509-3 du Code pénal par un nouvel alinéa 2 incriminant l'interception de données informatiques. Il s'agit de la première disposition du projet de loi imposée par la Convention à approuver. Le texte retenu est inspiré par l'article 3 de la Convention.

Le Conseil d'Etat, dans son avis du 16 avril 2013, propose d'omettre la tentative dans cet article.

L'article 509-6 du Code pénal prévoit effectivement de manière générale pour toute la section VII du Chapitre II du Titre IX du Livre II du Code pénal, dont relève l'article 509-3 du Code pénal, la tentative, dont l'incrimination est expressément prévue à l'article 11 de la Convention, de sorte qu'elle n'a pas besoin d'être spécialement prévue ici.

Partant, la Commission juridique propose, par voie d'amendement parlementaire, d'enlever la tentative du nouvel alinéa 2 de l'article 509-3 en supprimant les termes „ou tenté d'intercepter“.

Par ailleurs, la commission propose de ne pas utiliser le terme „système informatique“ tel que suggéré par le Conseil d'Etat dans son avis du 16 avril 2013, puisqu'il n'est pas utilisé dans les autres articles de la même section.

De même, le législateur a, à dessein, utilisé dans tous les articles de la section VII du Chapitre II du Titre IX du Livre II du Code pénal, dont relève l'article 509-3 du Code pénal, les termes plus complexes et précis de „système de traitement ou de transmission automatisé de données“ au lieu de „système informatique“.

C'est pourquoi il est proposé de les maintenir également pour le nouvel alinéa 2 de l'article 509-3 du Code pénal.

Pour des raisons de cohérence entre l'alinéa 1er et le nouvel alinéa 2 de l'article 509-3 du Code pénal, il est proposé de supprimer le terme „informatique“ à l'alinéa 2 et de ne parler que de „données“.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Cet amendement n'appelle pas d'observations du Conseil d'Etat dans son avis complémentaire du 12 novembre 2013.

Point 9) nouveau (Point 7) initial) – Article 509-4, alinéa 2 (suppression) du Code pénal

La suppression de l'alinéa 2 de l'article 509-4 du Code pénal est une mesure technique due à l'introduction d'un nouvel article 509-5 du Code pénal tel que proposée dans le présent projet de loi (cf. point 10) ci-après).

Point 10) nouveau (Point 8) initial) – Nouvel article 509-5 du Code pénal

L'introduction d'un nouvel article 509-5 du Code pénal tel que proposé dans le présent projet de loi a pour objectif de créer dans notre législation l'infraction d'abus de dispositif telle que prévue à l'article 6 de la Convention de Budapest et à l'article 7 relatif aux outils utilisés pour commettre les infractions de la future directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Il convient de noter que l'incrimination de l'abus de dispositif constitue une suite logique des articles 487 et 488 du Code pénal.

Dans son avis du 16 avril 2013, le Conseil d'Etat fait quelques observations d'ordre rédactionnel. „Il note que le critère du „mépris des droits d'autrui“ est uniquement consacré au second tiret, alors que, dans la logique de la Convention et des autres dispositions, on aurait parfaitement pu l'ajouter au critère de l'intention frauduleuse figurant au début du nouvel article. Le Conseil d'Etat renvoie encore à sa suggestion de viser, comme la Convention, le système informatique et d'omettre la dualité des concepts „système de traitement“ et „système de transmission automatisé“ de données.“

Afin de tenir compte des observations du Conseil d'Etat et de la Chambre de Commerce, les membres de la Commission juridique proposent, par voie d'amendement parlementaire, de modifier le nouveau point 10).

Il est proposé de ne pas utiliser le terme „*système informatique*“ tel que suggéré par le Conseil d'Etat puisqu'il n'est pas utilisé dans les autres articles de la même section. De même le législateur a, à dessein, utilisé dans tous les articles les termes plus complexes et précis de „*système de traitement ou de transmission automatisé de données*“ au lieu de „*système informatique*“.

C'est pourquoi il est proposé de les maintenir également pour le nouvel article 509-5 du Code pénal.

Conformément aux souhaits du Conseil d'Etat exprimés dans son avis du 16 avril 2013, il est proposé, pour des raisons de cohérence du texte, de supprimer les termes „*mot de passe*“ et „*code d'accès*“ qui étaient uniquement cités comme exemples par les auteurs du texte et de ne retenir que le seul terme générique de „*toute clef électronique*“ qui les englobe de toute façon.

Le terme générique retenu est celui de „*clef électronique*“ et non pas l'expression proposée par le Conseil d'Etat de „*bien quelconque (corporel ou incorporel)*“ la discussion sur une éventuelle incorporation de ces termes venant du Code de commerce dans le Code pénal devant être menée dans le cadre plus général de la réforme du Code pénal.

Dans son avis du 27 février 2013, la Chambre de Commerce relève l'abaissement de l'amende, actuellement de 1.250 euros à 30.000 euros, telle que prévue à l'article 509-4 du Code pénal sur lequel s'aligne le nouvel article 509-5 du Code pénal, et de son remplacement par une amende de 251 euros à 5.000 euros seulement.

Les auteurs du projet de loi souhaitaient initialement aligner les amendes sur celles de l'article 488 du Code pénal. Toutefois il n'était pas dans leur intention de baisser le niveau actuel de l'amende car il est important de prévoir des amendes élevées afin de décourager les auteurs d'infractions.

Partant, il est proposé de relever le seuil de l'amende prévue à l'article 509-5 de „*251 euros à 5.000 euros*“ à „*1.250 euros à 30.000 euros*“, ce qui correspond à l'amende actuelle figurant à l'article 509-4 du Code pénal sur lequel s'aligne l'article 509-5 du Code pénal et dont il remplace l'alinéa 2.

En ce qui concerne les termes „*au mépris des droits d'autrui*“ qui figurent uniquement au second tiret du nouvel article et non pas au début de ce dernier tel que le relève le Conseil d'Etat dans son avis du 16 avril 2013, la doublure du critère intentionnel pour le deuxième tiret est prévue dans la Convention et voulue par l'industrie informatique et les groupements chargés de prévenir les attaques cyber pour éviter une pénalisation de leurs actions de prévention.

En effet, ils utilisent souvent des clefs informatiques d'origine délictuelle pour accéder (ou tenter d'accéder) à des systèmes informatiques dans un but de pure prévention et donc pas au mépris des droits d'autrui, mais dans un but de prévention d'infraction (amélioration des fire-walls et système antivirus). La doublure de l'intention frauduleuse au seul second tiret a donc été maintenue.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Cet amendement n'appelle pas d'observations de la part du Conseil d'Etat dans son avis complémentaire du 12 novembre 2013.

Article 4 du projet de loi – Modifications du Code d'instruction criminelle

Point 1) – Article 7-4 du Code d'instruction criminelle

L'article 24 de la Convention sur l'extradition prévoit dans son paragraphe (6) l'introduction du principe „*aut dedere aut judicare*“ pour les infractions en matière informatique. C'est pourquoi les articles 509-1 à 509-7 du Code pénal sont ajoutés à la liste de l'article 7-4 du Code d'instruction criminelle. En outre ce texte est corrigé en vue de lui rendre son sens voulu par le législateur.

Dans son avis du 16 avril 2013, le Conseil d'Etat note qu'il y a lieu de libeller le texte sous examen comme suit:

„Art. 7-4. *Lorsqu'une personne qui se sera rendue coupable à l'étranger d'une des infractions prévues par les articles 112-1, 135-1 à 135-6, 135-9, 135-11 à 135-13, 136bis à 136quinquies, 260-1 à 260-4, 379, 382-1, 382-2, 384, 385-2 et 509-1 à 509-7 du Code pénal, n'est pas extradée, l'affaire sera soumise aux autorités compétentes aux fins de poursuites en application des règles prévues.“*

La Commission juridique décide de suivre le Conseil d'Etat.

Un amendement parlementaire en ce sens est adopté le 5 juin 2013.

Point 2) – Article 24-1, point 1) du Code d’instruction criminelle

Pour pouvoir satisfaire aux exigences des articles 16, 17 et 19 de la Convention sur la conservation rapide des données informatiques stockées, la conservation et la divulgation rapide de données relatives au trafic et la perquisition et saisie des données informatiques stockées, il est nécessaire de prévoir la possibilité de pouvoir procéder au repérage des données d’appel de moyens de télécommunications et de pouvoir localiser l’origine ou la destination de la télécommunication sans qu’une instruction préparatoire ne soit ouverte.

En effet, avec la perte de temps engendrée par l’ouverture d’une instruction on risquerait de perdre toutes les données. Or, pour le moment le repérage ne peut être autorisé que dans le cadre d’une instruction préparatoire conformément à l’article 67-1 du Code d’instruction criminelle. L’article 67-1 du Code d’instruction criminelle sera donc modifié en conséquence dans le cadre du présent projet de loi.

Le Conseil d’Etat peut suivre les auteurs du projet de loi dans leur raisonnement. Il propose néanmoins un texte simplifié qui aurait la teneur suivante:

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

Il précise pour le surplus que ce texte tend à compléter le paragraphe 1er de l’article 24-1 du Code d’instruction criminelle et non le point 1) de cet article, ainsi que l’indiquent les auteurs.

Les membres de la Commission juridique indiquent que, pour pouvoir satisfaire aux exigences des articles 16, 17 et 19 de la Convention sur la conservation rapide des données informatiques stockées, la conservation et la divulgation rapide de données relatives au trafic et la perquisition et saisie des données informatiques stockées, il est nécessaire de prévoir la possibilité de pouvoir procéder au repérage des données d’appel de moyens de télécommunications et de pouvoir localiser l’origine ou la destination de la télécommunication sans qu’une instruction préparatoire ne soit ouverte. Or, actuellement le repérage ne peut être autorisé que dans le cadre d’une instruction préparatoire conformément à l’article 67-1 du Code d’instruction criminelle.

En ce qui concerne la proposition de texte précitée du Conseil d’Etat, la Commission juridique décide de la reprendre.

Par le biais d’un amendement parlementaire adopté le 19 mars 2014, la Commission juridique propose

- (i) d’ajouter, à l’endroit de l’article 24 du Code d’instruction criminelle, deux nouveaux paragraphes, et
- (ii) de prévoir un renvoi de l’article 24-1 du Code d’Instruction criminelle à l’article 67-1 du même Code.

Cependant, le renvoi, tel que proposé à l’endroit de l’article 24 du Code d’instruction criminelle, est uniquement fait aux paragraphes (1) et (2) de l’article 67-1 du Code d’instruction criminelle et le paragraphe (3) de ce même article est repris en substance à l’endroit de l’article 24-1 du Code d’instruction criminelle, tel que proposé par le Conseil d’Etat dans son avis complémentaire du 12 novembre 2013.

Un tel renvoi limité est nécessaire pour deux raisons, à savoir:

- 1) Il ne faut pas faire double emploi, c’est-à-dire renvoyer à l’article 67-1 du Code d’instruction criminelle en entier et recopier en substance une partie de ce même article dans l’article 24-1 du Code d’instruction criminelle, et
- 2) Il faut éviter de renvoyer de l’article 24-1 du Code d’instruction criminelle à „l’instruction“, aucune instruction n’étant ouverte dans le cas de l’article 24-1 du Code d’instruction criminelle.

Dans son deuxième avis complémentaire du 4 avril 2014, le Conseil d’Etat marque son accord avec l’amendement qui répond aux suggestions qu’il avait émises dans son avis complémentaire du 12 novembre 2013.

En ce qui concerne le remplacement des termes „ou si les faits“ par les mots „et pour les délits“, le Conseil d’Etat prend acte des explications fournies par les auteurs de l’amendement, même s’il ne peut pas suivre les craintes émises quant à une démarche du juge d’instruction qui déduirait de l’emploi du mot „fait“ qu’il est saisi „in rem“.

A ce sujet, il est renvoyé aux commentaires faits ci-dessous par rapport à la modification de l'article 67-1 du Code d'instruction criminelle.

Point 3) – Article 31, point 3) du Code d'instruction criminelle

Cette modification de l'article 31 du Code d'instruction criminelle est nécessaire pour inclure les données stockées, traitées ou transmises dans un système informatique dans les dispositions du Code d'instruction criminelle sur les perquisitions et saisies et le rendre ainsi conforme aux exigences de l'article 19 de la Convention.

Le Conseil d'Etat approuve cette extension, tout en formulant une observation de fond et une observation de forme.

Il note qu'„[a]u terme des modifications apportées au Code d'instruction criminelle, la donnée informatique pourra désormais constituer l'objet d'une perquisition ou d'une saisie. Par contre, la donnée informatique ne sera pas toujours l'objet d'un vol, d'une extorsion, d'une escroquerie ou d'un abus de confiance. Les modifications apportées à l'article 496 du Code pénal ou encore à l'endroit du nouvel article 509-5 du Code pénal, qui ont recours aux concepts de clef électronique, de mot de passe ou de code d'accès, en sont l'illustration. Le Conseil d'Etat relève l'incohérence de cette approche qu'il a déjà soulignée dans ses observations à propos des modifications apportées au Code pénal.“

Le très récent arrêt de la Cour de cassation (n° 17/2014 du 3.4.2014) donne une réponse à ce reproche, en ce qu'il décide „... que les données électroniques enregistrées sur le serveur de la banque et qui sont juridiquement sa propriété exclusive constituent des biens incorporels qui peuvent faire l'objet d'une appréhension par voie de téléchargement;“ et donc d'un vol, d'une extorsion, d'une escroquerie ou d'un abus de confiance. Il n'y a donc plus d'incohérence au moment de la rédaction du présent rapport, puisque les données informatiques peuvent faire l'objet d'une saisie, mais aussi, suivant la jurisprudence récente de la Cour de cassation, d'une soustraction frauduleuse.

En ce qui concerne la terminologie, les auteurs proposent la formule assez complexe de „données stockées, traitées ou transmises dans un système informatique“. „Le Conseil d'Etat rappelle que le terme générique de la législation sur la protection des données est celui de „traitement“ et que le stockage et la transmission ne constituent que des formes de traitement. Il note encore que la Convention qui adopte une approche légèrement différente, vise, aux Titres 2 et 4 de la section 2 du Chapitre II, les données stockées. Il se demande si le concept plus simple de données informatiques ne pourrait pas être considéré comme suffisant, tant pour rester cohérent avec la législation sur la protection des données que pour respecter la Convention.“

Par le biais d'un amendement parlementaire adopté le 5 juin 2013, les membres de la Commission juridique proposent de remplacer les termes „système informatique“ par ceux de „système de traitement ou de transmission automatisé de données“, étant donné que cette terminologie correspond à celle déjà utilisée dans les articles 509-1 à 509-7 du Code pénal.

En ce qui concerne la formule de „données stockées, traitées ou transmises“, qualifiée de complexe par le Conseil d'Etat dans son avis du 16 avril 2013 et qui voudrait la remplacer par le terme „données informatiques“, il est précisé que c'est la terminologie utilisée par la Convention.

La Convention différencie en effet les „données stockées, traitées ou transmises“, qui englobent toutes les données y compris leur contenu, des „données relatives au trafic“, qui représentent seulement une partie des données informatiques (celles concernant l'origine et la destination de la communication).

Il est proposé de conserver la terminologie retenue par le texte du projet de loi.

Point 4) – Article 33 du Code d'instruction criminelle

La modification de l'article 33 du Code d'instruction criminelle est nécessaire pour inclure les données stockées, traitées ou transmises dans un système informatique dans les dispositions du Code d'instruction criminelle sur les perquisitions et saisies et le rendre ainsi conforme aux exigences de l'article 19 de la Convention.

Etant donné que le point 4) est le corollaire du point 3), le Conseil d'Etat, dans son avis du 16 avril 2013, renvoie à ses observations antérieures.

Il note que le qualificatif „informatique“ est à adjoindre au concept de données qui est ajouté dans différents points du paragraphe 1er de l'article 33 du Code d'instruction criminelle.

Le nouveau paragraphe (5) vise à permettre la saisie par voie d'établissement d'une copie.

Selon le Conseil d'Etat „*Les auteurs du projet de loi ne donnent pas d'explication sur l'introduction d'un système d'effacement visé à la seconde phrase du nouveau paragraphe sauf à invoquer des „raisons pratiques“ non autrement précisées. La saisie semble se doubler d'une décision de justice ou d'une mesure de sûreté fondée sur le caractère illégal ou dangereux pour la sécurité des biens et des personnes de la détention ou de l'usage des biens. Le Conseil d'Etat s'interroge sur cette logique et sur la cohérence juridique. La saisie est une mesure d'enquête et d'instruction. Elle porte sur la conservation d'objets utiles à la manifestation de la vérité. La saisie est susceptible d'être levée. Quelle sera la nature juridique de la décision d'effacement? Est-elle couverte par le concept traditionnel de saisie? Les données ne sont a priori pas saisies parce qu'elles sont illégales ou dangereuses, sauf l'hypothèse où l'infraction consiste dans le traitement de données illégales ou dangereuses. S'il s'agit de geler les données et d'interdire leur usage, le nouvel article 48-25 pourrait, si nécessaire, être utilisé. Par ailleurs, qu'en est-il en cas de décision de non-lieu ou d'acquiescement? Est-il possible de rétablir les données effacées? Et quel est alors l'intérêt de la mesure d'effacement des données? La décision d'effacement ne s'apparente-elle pas à une sanction de confiscation anticipée?*“

Selon les membres de la Commission juridique, il convient d'appliquer la même logique que pour l'article 31 du Code d'instruction criminelle et pour les articles 509-1 à 509-7 du Code pénal. En ce qui concerne les termes „*système informatique*“ et ceux de „*données stockées, traitées ou transmises*“, il est renvoyé au commentaire sous le point 3) ci-avant.

Il est rappelé que l'introduction d'un nouveau point 5) a été décidée pour des raisons pratiques. En effet, il est souvent impossible de saisir le support physique sur lequel sont stockées les données informatiques, car il s'agit la plupart du temps de serveurs qui remplissent des pièces entières. Cette problématique se pose surtout dans les cas des grands centres de traitement de données dans lesquels il n'est pas possible physiquement de saisir des disques durs. Il est par conséquent plus simple de saisir les données en les copiant. La copie pourra ensuite être facilement transportée et analysée dans les locaux des autorités compétentes.

Il faut par ailleurs créer la possibilité d'effacer définitivement des données sur les disques durs. Ceci est particulièrement important dans certains cas, comme par exemple ceux concernant la pédopornographie ou de la malware (c'est-à-dire de programmes causant un dommage à d'autres ordinateurs). Partant, la décision d'effacement ne peut pas être assimilée à une sanction de confiscation anticipée. Il s'agit soit d'une protection des personnes et des biens contre de nouvelles infractions (en cas de malware notamment), soit d'une mesure tendant à éviter la propagation de matériel illégal (telle que la pédopornographie).

En cas d'acquiescement ou de décision de ne pas procéder à des poursuites, les données saisies (leur copie) pourront être restituées. En cas de poursuites, en revanche, les données seront confisquées.

Il est précisé par ailleurs que, conformément au paragraphe (5), seules sont concernées „*des données stockées, traitées ou transmises dans un système informatique dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens*“. Cette disposition vise notamment la pédopornographie, la malware ou encore l'incitation à la haine, voire le terrorisme.

Par le biais d'un amendement parlementaire adopté le 5 juin 2013, les membres de la Commission juridique proposent de remplacer les termes „*système informatique*“ par ceux de „*système de traitement ou de transmission automatisé de données*“, étant donné que cette terminologie correspond à celle déjà utilisée dans les articles 509-1 à 509-7 du Code pénal.

En ce qui concerne la formule de „*données stockées, traitées ou transmises*“, qualifiée de complexe par le Conseil d'Etat dans son avis du 16 avril 2013 et qui voudrait la remplacer par le terme „*données informatiques*“, il est précisé que c'est la terminologie utilisée par la Convention.

La Convention différencie en effet les „*données stockées, traitées ou transmises*“, qui englobent toutes les données y compris leur contenu, des „*données relatives au trafic*“ qui représentent seulement une partie des données informatiques (celles concernant l'origine et la destination de la communication).

Il est proposé de conserver la terminologie retenue par le texte du projet de loi.

Dans son avis complémentaire du 12 novembre 2013, le Conseil d'Etat renvoie à ses considérations à l'endroit du point 3 ci-dessus.

Point 5) – Article 48-17, paragraphe (1) du Code d’instruction criminelle

Il est proposé d’inclure les infractions en matière informatique dans les cas de figure où il peut être recouru à l’infiltration, car plus encore que pour d’autres infractions les raisons d’être de celle-ci, à savoir que „l’enquête ou l’instruction préparatoire l’exigent et que les moyens ordinaires d’investigation s’avèrent inopérants en raison de la nature des faits et des circonstances spéciales de l’espèce“, sont remplis dans le cadre de la cybercriminalité.

Le Conseil d’Etat, dans son avis du 16 avril 2013, n’a pas d’observations à formuler, sauf à préciser que c’est le paragraphe 1er de l’article 48-17 du Code d’instruction criminelle qui est ainsi modifié et non le point 1) tel que l’indiquent les auteurs du projet de loi, et à rendre attentif au fait que l’enlèvement des mineurs figurant au point 12 de la liste des infractions visées se trouve déjà dans la version actuelle de l’article 48-17 du Code d’instruction criminelle.

La commission fait sienne la remarque du Conseil d’Etat de préciser que c’est le paragraphe 1er de l’article 48-17 du Code d’instruction criminelle qui est ainsi modifié et non le point 1) tel que l’indiquent les auteurs du projet de loi. Elle décide en outre de supprimer le point 12).

Point 6) – nouveau Chapitre X à insérer au Livre Premier, Titre II „Des enquêtes“ du Code d’instruction criminelle

Pour satisfaire aux exigences de l’article 16 de la Convention sur la conservation rapide des données informatiques stockées, il est proposé d’introduire un nouvel article dans le Code d’instruction criminelle. Comme il s’agit d’un concept nouveau il est également proposé de faire figurer cet article dans un nouveau Chapitre X du Livre Premier, Titre II „Des enquêtes“ du Code d’instruction criminelle, le Chapitre IX étant consacré à l’accès à certains traitements de données. Le texte est en partie la reprise pure et simple des dispositions de l’article 16, paragraphe (1) de la Convention.

Dans l’état actuel de notre droit, le problème pour satisfaire à l’exigence de la conservation rapide est le suivant: En combinant les articles 67-1 du Code d’instruction criminelle et 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, une saisie de données relatives au trafic dans le cadre du flagrant crime ou délit n’est pas possible. Avec le nouvel article, la conservation rapide pourra être demandée dans le cadre du flagrant crime ou délit ou à tout moment de l’enquête préliminaire par le procureur d’Etat et dans le cadre de l’instruction par le juge d’instruction. S’il s’agit de données de télécommunications visées par l’article 67-1 du Code d’instruction criminelle, la saisie ne pourra être faite que suivant cet article. Si par contre il s’agit de données informatiques autres, le droit commun des saisies s’applique. Les articles 5 et 9 de la loi du 30 mai 2005 devront être adaptés en conséquence dans le cadre de ce projet de loi.

Cette nouvelle procédure pourra être utilisée aussi bien au niveau national qu’au niveau international. Dans ce dernier cas, elle sera appliquée avant même toute commission rogatoire internationale sur simple demande d’une autorité étatique de poursuite. Cependant la procédure devra être régularisée par l’envoi et la réception d’une commission rogatoire internationale en bonne et due forme avant l’expiration du délai de 90 jours. Il convient de remarquer qu’un règlement grand-ducal sera pris pour satisfaire aux articles 16 et 17 de la Convention, notamment en ce qui concerne la divulgation rapide de données relatives au trafic.

Dans son avis du 16 avril 2013, le Conseil d’Etat note que le nouveau texte est encore destiné à répondre aux obligations découlant pour le Luxembourg de l’article 29 de la Convention sur l’entraide judiciaire. Le Conseil d’Etat indique qu’il „[...] ne peut pas apprécier, sur un plan technique, si les dispositions existantes sur la saisie et la perquisition, étendues aux données informatiques, ne permettent pas d’ores et déjà d’opérer le gel ou la saisie conservatoire de données informatiques entre les mains d’un opérateur tiers, ce qui rendrait superflue l’adoption du texte sous examen.“

Dans la grande majorité des cas nationaux, les dispositions de la saisie devraient effectivement suffire. En revanche, dans la majeure partie des cas internationaux, une conservation rapide s’impose en attendant la commission rogatoire internationale. Il a été décidé de ne pas distinguer entre cas nationaux et internationaux afin de ne pas priver les affaires nationales d’une procédure très utile et rapide.

Par le biais d’un amendement parlementaire adopté le 5 juin 2013, la Commission juridique propose de remplacer les termes „système informatique“ par ceux de „système de traitement ou de transmission automatisé de données“, étant donné que cette terminologie correspond à celle déjà utilisée dans les articles 509-1 à 509-7 du Code pénal.

Le Conseil d'Etat, dans son avis du 16 avril 2013, marque encore ses réserves par rapport à l'octroi d'une compétence propre à un officier de police judiciaire agissant „*de l'accord du procureur d'Etat ou du juge d'instruction*“ et fait une proposition de texte pour l'éviter.

Il propose en outre une simplification de texte à la fin du nouvel article pour éviter la formule complexe qui figure au début de l'article et la remplacer par „*ces données*“.

La Commission juridique suit ces propositions du Conseil d'Etat.

Pour des raisons de cohérence avec les autres textes du Code pénal sur les infractions en matière informatique le nouvel article parle de „*données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données*“ et non pas de „*données informatiques*“.

Dans son avis complémentaire du 12 novembre 2013, le Conseil d'Etat indique qu'il suit les auteurs des amendements dans leur volonté d'assurer une cohérence d'ordre terminologique entre les différentes dispositions.

Point 7) – Article 66 du Code d'instruction criminelle

La modification de l'article 66 du Code d'instruction criminelle est nécessaire pour inclure les données stockées, traitées ou transmises dans un système informatique dans les dispositions du Code d'instruction criminelle sur les perquisitions et saisies et le rendre ainsi conforme aux exigences des articles 18 et 19 de la Convention. L'introduction d'un nouveau paragraphe (3) est due à des raisons pratiques. En effet, il est souvent impossible ou extrêmement fastidieux de saisir le support physique sur lequel sont stockées les données informatiques, car il s'agit la plupart du temps de serveurs qui remplissent des pièces entières. Il est par conséquent plus simple d'en faire une copie qui pourra être facilement transportée et analysée dans les locaux des autorités compétentes.

L'introduction du nouveau point 4) met la loi luxembourgeoise en conformité avec l'article 18 de la Convention qui prévoit une injonction de produire. Ceci est en effet extrêmement important en matière d'infractions informatiques, car souvent l'accès aux réseaux et donc aux données ne peut se faire que par des personnes hautement spécialisées qui ont elles-mêmes programmé et configuré les logiciels et sont souvent détentrices de mots de passe ou de codes sans lesquels un accès est impossible.

Dans son avis du 16 avril 2013, le Conseil d'Etat note que les modifications proposées sont le corollaire de celles apportées à l'article 33 du Code d'instruction criminelle (cf. article 4, point 4) ci-avant) et il renvoie à ses observations afférentes, y compris pour ce qui est du nouveau paragraphe (3) inséré à l'endroit de l'article 66 du Code d'instruction criminelle.

„Le Conseil d'Etat note encore que l'article 18 de la Convention prévoit le mécanisme de l'injonction de produire des données informatiques, injonction ordonnée par les autorités compétentes. La Convention conçoit ce régime comme un mécanisme particulier, à côté de la perquisition et de la saisie prévue à l'article 19. Le Conseil d'Etat note que les auteurs du projet n'expliquent pas les raisons qui les ont amenés à se limiter aux procédures de perquisition et de saisie.“

La Commission juridique indique que la perquisition englobe l'injonction de produire. En cas de refus, face à une injonction de produire, il n'existe pas réellement de possibilité de contraindre la personne visée par l'instruction, non coopérant, de donner accès aux données, contrairement à la perquisition. Partant il a été jugé préférable de se limiter aux procédures de perquisition et de saisie. En pratique, en cas de perquisition non hostile (c'est-à-dire effectuée chez des tiers et non pas chez un suspect) les perquisitions sont exécutées comme les injonctions de produire.

En réponse aux observations du Conseil d'Etat, la Commission juridique renvoie aux commentaires figurant sous le point 4), article 4 du texte de loi (modification de l'article 33 du Code d'instruction criminelle). A l'instar des paragraphes (3) et (4), elle propose de remplacer, par voie d'amendement parlementaire, les termes „*système informatique*“ par ceux de „*système de traitement ou de transmission automatisé de données*“.

En ce qui concerne la formule de „*données stockées, traitées ou transmises*“, qualifiée de complexe par le Conseil d'Etat dans son avis du 16 avril 2013 et qui voudrait la remplacer par le terme „*données informatiques*“, il est précisé que c'est la terminologie utilisée par la Convention.

La Convention différencie en effet les „*données stockées, traitées ou transmises*“, qui englobent toutes les données y compris leur contenu, des „*données relatives au trafic*“ qui représentent seulement une partie des données informatiques (celles concernant l'origine et la destination de la communication).

Il est proposé de conserver la terminologie retenue par le texte du projet de loi.

Dans son avis complémentaire du 12 novembre 2013, le Conseil d'Etat renvoie à ses observations précédentes.

Point 8) – Article 67-1 du Code d'instruction criminelle

Cette modification est le corollaire de l'introduction de la nouvelle procédure de l'article 48-25 du Code d'instruction criminelle et de la modification de l'article 24-1 du Code d'instruction criminelle qui prévoient désormais la possibilité du repérage même en absence d'une instruction préparatoire.

Le point 8) prévoit la suppression, dans la première phrase du paragraphe 1er de l'article 67-1 du Code d'instruction criminelle, des mots „saisi de faits“ visant la situation du juge d'instruction qui ordonne un repérage de données d'appel. Selon les auteurs, cette modification s'imposerait au vu de l'introduction de la nouvelle procédure de l'article 48-25 du Code d'instruction criminelle et de la modification de l'article 24-1 du Code d'instruction criminelle qui prévoient désormais la possibilité du repérage, même en l'absence d'une instruction préparatoire.

Le Conseil d'Etat, dans son avis du 16 avril 2013, „[...] est d'avis que cette modification est parfaitement superflue et est à omettre. La modification de l'article 24-1 du Code d'instruction criminelle portant extension de la procédure particulière de saisine du juge d'instruction en l'absence d'une instruction préparatoire à l'article 67-1 du même code se suffit à elle-même et ne requiert aucune adaptation de l'article 67-1 du Code d'instruction criminelle. Il s'agit d'une procédure spécifique permettant justement l'adoption des mesures prévues à l'article 67-1 du Code d'instruction criminelle en dehors d'une procédure d'instruction. Le Conseil d'Etat note que pour les actes visés au texte actuel de l'article 24-1 du Code d'instruction criminelle, il n'a pas été procédé à une adaptation des dispositions relatives aux actes d'instruction adoptés par le juge d'instruction.

Le Conseil d'Etat propose également d'omettre les adaptations prévues au paragraphe (3) de l'article 67-1 du Code d'instruction criminelle, à propos desquelles le commentaire ne donne d'ailleurs aucune explication. La procédure de la requête en annulation est régie de façon exhaustive à l'article 24-1 du Code d'instruction criminelle sans qu'il ne faille introduire un renvoi à cette disposition à l'endroit de l'article 67-1 du Code d'instruction criminelle. Le Conseil d'Etat reconnaît que se pose la question de l'information de la personne qui fait l'objet de la mesure de repérage ou de la localisation et du retrait des données obtenues. Plutôt que d'ajouter une référence à l'enquête préliminaire dans un article sur la procédure d'instruction, le Conseil d'Etat propose, dans l'intérêt de la cohérence des textes et de l'articulation des compétences, d'insérer le texte suivant à l'article 24-1 du Code d'instruction criminelle [...]“ à la suite des modifications y proposées.

Le texte se lira comme suit:

„Pour tout délit, le procureur d'Etat peut requérir du juge d'instruction d'ordonner une perquisition, une saisie, l'audition d'un témoin ou une expertise sans qu'une instruction préparatoire soit ouverte.

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

Pour les infractions visées à l'alinéa qui précède et pour les délits qui emportent une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, le procureur d'Etat peut requérir du juge d'instruction de faire procéder à une des mesures visées à l'article 67-1.

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

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

D'après le Conseil d'Etat, „il reste une question importante ayant trait à l'autorité compétente pour apprécier si les mesures de repérage des télécommunications sont sans résultat et si les données sont

à retirer du dossier. Logiquement, il devrait s'agir du procureur d'Etat, sauf à prévoir une nouvelle saisine „ad hoc“ du juge d'instruction, alors que c'est ce dernier qui a ordonné la mesure. Se pose encore la question du droit des parties concernées de demander la destruction des données obtenues.“

D'un point de vue formel et à toutes fins utiles, le Conseil d'Etat rend attentif au fait que les auteurs négligent d'indiquer le paragraphe 1er en début du texte de l'article 67-1 nouveau du Code d'instruction criminelle et qu'au paragraphe (3) du même article, avant le commencement du texte, ils prévoient une référence à une loi du 12 août 2003 qui doit être omise.

La Commission juridique fait siennes les remarques du Conseil d'Etat.

A l'endroit du paragraphe (3), la Commission juridique propose, par voie d'amendement parlementaire, d'adapter le texte pour tenir compte des modifications introduites par la loi du 26 décembre 2012 et figurant dans la version actuelle du Code d'instruction criminelle.

Concernant les autres réflexions du Conseil d'Etat et sa proposition de texte pour l'article 24-1 du Code d'instruction criminelle, il est proposé dans une première phase de maintenir le texte du projet de loi.

A défaut de supprimer les termes „saisi de faits“ dans la première phrase du paragraphe 1er de l'article 67-1 du Code d'instruction criminelle, celui-ci pourrait être considéré en contradiction avec l'article 24-1 a du Code d'instruction criminelle lors que ce dernier renvoie à l'article 67-1 du Code d'instruction criminelle.

Dans la mesure où l'article 24-1 du Code d'instruction criminelle renvoie à l'article 67-1 du Code d'instruction criminelle, la solution la plus simple est d'ajouter l'enquête préliminaire au paragraphe (3) de l'article 67-1 du Code d'instruction criminelle. En effet, l'article 67-1 du Code d'instruction criminelle prévoit toute une série de procédures à respecter et non seulement celles que le Conseil d'Etat propose d'ajouter à l'article 24-1 du Code d'instruction criminelle. Il est donc préférable de préciser, à l'article 67-1 lui-même, que, suivant le cas, elles s'appliquent en instruction ou en enquête préliminaire. La procédure des nullités de l'article 126 du Code d'instruction criminelle n'est par ailleurs pas applicable à l'article 24-1 du même code.

Concernant la question importante du Conseil d'Etat ayant trait à l'autorité compétente pour apprécier si les mesures de repérage des télécommunications sont sans résultat et si les données sont à retirer du dossier, la Commission juridique est d'avis que c'est en effet le procureur d'Etat qui est l'autorité compétente, dans le cadre de l'enquête préliminaire (le juge d'instruction n'étant pas saisi du dossier), pour apprécier si les mesures de repérage des télécommunications sont sans résultat et si les données sont à retirer du dossier.

Dans son avis complémentaire du 12 novembre 2013, le Conseil d'Etat rappelle que dans son avis du 16 avril 2013, il avait considéré qu'il n'y avait pas lieu de modifier le texte du paragraphe 1er de l'article 67-1 du Code d'instruction criminelle, alors que la cohérence avec l'article 24-1 du Code d'instruction criminelle n'exigeait aucune modification. Il note que les auteurs de l'amendement expliquent vouloir „suivre les propositions du Conseil d'Etat“. „Or, ils maintiennent les modifications envisagées dans le projet de loi initial, en relation avec cette disposition consistant dans la suppression des restrictions au recours au repérage qui, en vertu des dispositions actuelles, peut seulement se faire pour des faits emportant une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. Cette limite tombe dans le texte du projet de loi, tel que maintenu par les auteurs des amendements. Le Conseil d'Etat se demande si la volonté effective des auteurs des amendements est de permettre au juge d'instruction d'opérer des repérages en toute matière. A noter que, pour l'article 24-1 du Code d'instruction criminelle, relatif à la „mini-instruction“, les limites, en termes de taux de peines, sont conservées, ce qui aboutit à une divergence des mécanismes que les auteurs du projet de loi entendaient justement éviter.

Le Conseil d'Etat ne peut pas davantage suivre les auteurs des amendements quand ils proposent, pour l'information de la personne concernée, d'ajouter une référence à l'enquête préliminaire à l'article 67-1, paragraphe (3) du Code d'instruction criminelle. Cet article ne concerne pas l'enquête préliminaire et la consécration de l'information de la personne concernée est à ajouter à la disposition portant repérage dans le cadre de la „mini-instruction“, à savoir l'article 24-1 du Code d'instruction criminelle.

Le Conseil d'Etat reste encore d'avis, dans un souci de clarté du mécanisme, qu'il convient de faire référence, à l'article 24-1 du Code d'instruction criminelle, au régime de la destruction. On ne peut

pas fonder la compétence importante du procureur d'Etat de retirer les données du dossier ou de les détruire sur la simple mention, dans l'article 67-1 du Code d'instruction criminelle, de l'enquête préliminaire.

Le Conseil d'Etat invite les auteurs à reconsidérer leurs positions et renvoie aux propositions de texte qu'il avait formulées dans son avis du 16 avril 2013.

En réponse à ces observations, il est précisé que l'introduction du mécanisme de la „mini-instruction“ dans le droit luxembourgeois de la procédure criminelle par l'article 24-1 du Code d'instruction criminelle (inséré par la loi du 27 octobre 2010 portant renforcement du cadre légal en matière de lutte contre le blanchiment et contre le financement du terrorisme, Mémorial A n° 193 du 3 novembre 2010) découle d'une obligation internationale (norme juridique supérieure) souscrite par le Luxembourg. De même il est rappelé que ledit mécanisme de la „mini-instruction“ équivaut bel et bien, par son caractère dérogoire au principe de la saisine „*in rem*“ du juge d'instruction, à un changement de paradigme.

Par le biais d'un amendement parlementaire adopté le 19 mars 2014, la Commission juridique propose de modifier l'article 67-1 du Code d'instruction criminelle.

La raison du transfert du bout phrase „*saisi de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement*“ de la première partie de la phrase vers le milieu de celle-ci a une raison pratique: en effet certains juges d'instruction (qui sont indépendants et donc liés que par les textes) ont interprété (et interprètent toujours) les 3 mots „*saisi de faits*“ qui figurent dans la rédaction actuelle de l'article 67-1 du Code d'instruction criminelle comme une obligation d'être „*saisi in rem*“ et donc de tout le dossier pénal avant de pouvoir opérer des repérages ou des localisations de communications.

Or, une saisine „*in rem*“ est exclue dans le cadre de l'article 24-1 du Code d'instruction criminelle et donc si l'article 24-1 du Code d'instruction criminelle renvoie dorénavant à l'article 67-1 du Code d'instruction criminelle (tel que proposé par le Conseil d'Etat et retenu par l'amendement 1er ci-dessus, il faut nécessairement enlever cette éventuelle saisine *in rem* de l'article 67-1 du Code d'instruction criminelle, sinon certains juges risquent de ne pas appliquer l'article 24-1 du Code d'instruction criminelle en combinaison avec l'article 67-1 du Code d'instruction criminelle parce qu'ils les estimeront contradictoires.

Les ajouts au paragraphe (3) „*ou de l'enquête préliminaire*“ et „*ou à l'article 24-1 du Code d'instruction criminel*“ prévus dans le projet de loi initial sont de nouveau à biffer, cet alinéa étant incorporé tel que demandé par le Conseil d'Etat à l'article 24-1 du Code d'instruction criminelle.

Le Conseil d'Etat, dans son deuxième avis complémentaire du 4 avril 2014, rappelle qu'il avait préconisé, dans son avis complémentaire du 12 novembre 2013, de ne pas modifier le texte de l'article 67-1 du Code d'instruction criminelle. Il constate qu'il a été suivi par les auteurs de l'amendement, sauf en ce qui concerne l'élimination des termes „*saisi de faits*“.

Le Conseil d'Etat prend encore acte des explications fournies par les auteurs, mais rappelle qu'il ne saurait pas les partager. L'article 67-1 du Code d'instruction criminelle vise, sans discussion aucune, les compétences propres du juge d'instruction. Pour pouvoir agir, au titre de l'article 67-1 du Code d'instruction criminelle, ce dernier est saisi d'une instruction *in rem*. L'apport du projet de loi sous examen est justement de permettre l'adoption de ces mesures dans le cadre de l'article 24-1 du Code d'instruction criminelle. Ce texte fait référence aux mesures prévues à l'article 67-1 du Code d'instruction criminelle et précise qu'une instruction préparatoire n'est pas ouverte. La modification de l'article 67-1 du Code d'instruction criminelle retenue par l'amendement est encore le résultat d'un mélange non justifié entre les deux dispositions.

Les membres de la Commission juridique soulignent la pertinence du raisonnement du Conseil d'Etat, tout en préconisant la suppression des trois termes „*saisi de faits*“. En effet, ces termes prêtent à confusion dans la mesure où un certain nombre de juges interprétaient – et risquent de continuer à interpréter – les termes „*saisi de faits*“ qui figurent dans la rédaction actuelle de l'article 67-1 du Code d'instruction criminelle comme une obligation spécifique de cet article (en effet les articles relatifs à la perquisition et la saisie ne prévoient pas ces termes tandis qu'ils se trouvent au même endroit du Code d'instruction criminelle que l'article 67-1 du Code d'instruction criminelle d'être „*saisi in rem*“ et donc de tout le dossier pénal avant de pouvoir opérer des repérages ou des localisations de communications.

Etant donné que l'article 24-1 du Code d'instruction criminelle, tel que modifié par le projet de loi, prévoit désormais expressément, à côté des perquisitions, saisies, auditions et expertises, aussi la pos-

sibilité de retraçages et de repérages, sans saisine *in rem*, et qu'il renvoie dorénavant à l'article 67-1 du Code d'instruction criminelle, ils estiment qu'il est préférable de supprimer les termes „saisi de faits“ qui risquent de donner lieu à des difficultés d'interprétation.

L'article 67-1 du Code d'instruction criminelle dans sa nouvelle rédaction gardera cependant le même sens et les mêmes conditions d'applications que dans la version antérieure.

Article 5 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

L'article 5 porte modification de diverses dispositions de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Point 1)

Le point 1) vise à insérer dans l'article 4, paragraphe (3), sous le point b) de la loi précitée du 30 mai 2005 concernant la confidentialité des communications et des données relatives au trafic, une référence au nouvel article 48-25 du Code d'instruction criminelle pour excepter de la confidentialité les autorités judiciaires agissant en vertu de ce nouvel article.

L'ajout de cette référence ne soulève pas d'observations de la part du Conseil d'Etat.

Point 2)

Le point 2) qui vise à insérer dans l'article 5, paragraphe (2), de la loi précitée du 30 mai 2005 concernant les fournisseurs de services, leur obligation de conservation des données relatives au trafic et leur collaboration, le cas échéant, avec les autorités judiciaires, une référence au nouvel article 48-25 du Code d'instruction criminelle, n'appelle pas d'observations de la part du Conseil d'Etat.

Point 3)

Le point 3) vise à insérer dans l'article 9, paragraphe (2), de la loi précitée du 30 mai 2005 concernant les fournisseurs de services ou opérateurs, leur obligation de conservation des données de localisation autres que les données relatives au trafic et leur collaboration, le cas échéant, avec les autorités judiciaires, une référence au nouvel article 48-25 du Code d'instruction criminelle.

Le point 3) ne soulève pas d'observations.

Le Conseil d'Etat, dans son avis du 16 avril 2013, formule néanmoins une observation générale sur ces trois points. Les exceptions à l'obligation de confidentialité que le législateur a instituées en 2005 en faveur des autorités judiciaires sont une évidence. La question se pose si l'ajout d'une référence au nouvel article 48-25 du Code d'instruction criminelle est suffisant pour couvrir tous les cas de figure. Ne faudrait-il pas ajouter également une référence à l'article 24-1 du Code d'instruction criminelle? Qu'en est-il des saisies au titre des articles 31, 33 et 66 du Code d'instruction criminelle qui peuvent également porter sur des données traitées par un opérateur pour compte d'un tiers? La référence à des articles particuliers du Code d'instruction criminelle entraîne encore l'obligation de revoir la loi de 2005 lors de chaque modification du contenu ou de la numérotation du Code d'instruction criminelle. Le Conseil d'Etat préconise une formule plus générale ayant la teneur suivante: „*autorités judiciaires agissant dans le cadre des compétences prévues au Code d'instruction criminelle ...*“ ou bien „*procureur d'Etat et juge d'instruction agissant ...*“.

Le Conseil d'Etat note enfin que la référence expresse aux articles 88-1 et 88-4 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques peut être maintenue, parce qu'il ne s'agit pas de dispositions relatives à l'enquête préliminaire ou à la procédure d'instruction.

Par voie d'un amendement parlementaire adopté le 5 juin 2013, les membres de la Commission juridique décident de suivre les propositions du Conseil d'Etat, en supprimant les références aux articles 48-25 et 67-1 du Code d'instruction criminelle et en retenant la formule „*autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi*“.

Dans son avis complémentaire du 12 novembre 2013, le Conseil d'Etat continue à considérer que la référence aux „*compétences prévues par le Code d'instruction criminelle*“, qu'il avait proposée dans son avis du 16 avril 2013, est plus précise.

En réponse aux observations du Conseil d'Etat, il est rappelé que la raison pour le maintien du texte tel que proposé par les auteurs du projet de loi est dictée par le souci de continuer à viser les compétences déléguées aux autorités judiciaires par des textes de loi particuliers.

*

VI. TEXTE PROPOSE PAR LA COMMISSION

Sous le bénéfice des observations qui précèdent, la Commission juridique recommande à la Chambre des Députés d'adopter le projet de loi n° 6514 dans la teneur qui suit:

*

PROJET DE LOI

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**

Art. 1er.— Est approuvée la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001.

Art. 2.— Est approuvé le 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.

Art. 3.— Le Code pénal est modifié et complété comme suit:

- 1) Il est introduit un article 231*bis* du Code pénal libellé comme suit:

„**Art. 231*bis*.**— Quiconque, dans le but de troubler la tranquillité d'un tiers, ou dans le but de porter atteinte à l'honneur ou à la considération d'un tiers, aura pris un nom ou un identifiant qui ne lui appartient pas sera puni d'un emprisonnement de trois mois à deux ans, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement.

Le délit prévu par le présent article ne pourra être poursuivi que sur la plainte de la victime, de son représentant légal ou de ses ayants droit.“

- 2) L'alinéa 1er de l'article 461 du Code pénal est modifié comme suit:

„Quiconque a soustrait frauduleusement une chose ou une clef électronique qui ne lui appartient pas est coupable de vol.“

- 3) Les alinéas 1 et 2 de l'article 470 du Code pénal sont modifiés comme suit:

„Quiconque aura extorqué, par violences ou menaces, soit la remise de fonds, valeurs, objets mobiliers ou clefs électroniques, soit la signature ou la remise d'un écrit, d'un acte, d'une pièce quelconque contenant ou opérant obligation, disposition ou décharge sera puni des peines portées aux articles 468, 471, 472, 473, 474 et 475, d'après les distinctions qui y sont établies.

Quiconque, à l'aide de la menace écrite ou verbale de révélations ou d'imputations calomnieuses ou diffamatoires, aura extorqué, soit la remise de fonds, valeurs, objets mobiliers ou clefs électro-

- niques, soit la signature ou la remise des écrits énumérés ci-dessus, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 500 euros à 30.000 euros.“
- 4) A l'article 488 du Code pénal, les termes „trois mois à deux ans et à une amende de 251 euros à 2.000 euros“ sont remplacés par ceux de „quatre mois à cinq ans et à une amende de 1.250 euros à 30.000 euros.“
- 5) L'alinéa 1er de l'article 491 du Code pénal est modifié comme suit:
- „Quiconque aura frauduleusement soit détourné, soit dissipé au préjudice d'autrui, des effets, deniers, marchandises, billets, quittances, clefs électroniques, écrits de toute nature contenant ou opérant obligation ou décharge et qui lui avaient été remis à la condition de les rendre ou d'en faire un usage ou un emploi déterminé, sera puni d'un emprisonnement d'un mois à cinq ans et d'une amende de 251 euros à 5.000 euros.“
- 6) L'alinéa 1er de l'article 496 du Code pénal est modifié comme suit:
- „Quiconque, dans le but de s'approprier une chose appartenant à autrui, se sera fait remettre ou délivrer ou aura tenté de se faire remettre ou délivrer des fonds, meubles, obligations, quittances, décharges, clefs électroniques, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses pour persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, pour faire naître l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique, ou pour abuser autrement de la confiance ou de la crédulité, sera puni d'un emprisonnement de quatre mois à cinq ans et d'une amende de 251 euros à 30.000 euros.“
- 7) Le point 1) de l'article 506-1 du Code pénal est modifié comme suit:
- „1) 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, alinéa premier, sous 1), formant l'objet ou le produit, direct ou indirect,
- d'une infraction aux articles 112-1, 135-1 à 135-6, 135-9 et 135-11 à 135-13 du Code pénal;
 - de crimes ou de délits dans le cadre ou en relation avec une association au sens des articles 322 à 324ter du Code pénal;
 - d'une infraction aux articles 368 à 370, 379, 379bis, 382-1, 382-2, 382-4 et 382-5 du Code pénal;
 - d'une infraction aux articles 383, 383bis, 383ter et 384 du Code pénal;
 - d'une infraction aux articles 496-1 à 496-4 du Code pénal;
 - d'une infraction de corruption;
 - d'une infraction à la législation sur les armes et munitions;
 - d'une infraction aux articles 184, 187, 187-1, 191 et 309 du Code pénal;
 - d'une infraction aux articles 463 et 464 du Code pénal;
 - d'une infraction aux articles 489 à 496 du Code pénal;
 - d'une infraction aux articles 509-1 à 509-7 du Code pénal;
 - d'une infraction à l'article 48 de la loi du 14 août 2000 relative au commerce électronique;
 - d'une infraction 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 des données à caractère personnel dans le secteur des communications électroniques;
 - d'une infraction à l'article 10 de la loi du 21 mars 1966 concernant a) les fouilles d'intérêt historique, préhistorique, paléontologique ou autrement scientifique; b) la sauvegarde du patrimoine culturel mobilier;
 - d'une infraction à l'article 5 de la loi du 11 janvier 1989 réglant la commercialisation des substances chimiques à activité thérapeutique;
 - d'une infraction à l'article 18 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine;
 - d'une infraction aux articles 82 à 85 de la loi du 18 avril 2001 sur le droit d'auteur;
 - d'une infraction à l'article 64 de la loi modifiée du 19 janvier 2004 concernant la protection de la nature et des ressources naturelles;

- d’une infraction à l’article 9 de la loi modifiée du 21 juin 1976 relative à la lutte contre la pollution de l’atmosphère;
 - d’une infraction à l’article 25 de la loi modifiée du 10 juin 1999 relative aux établissements classés;
 - d’une infraction à l’article 26 de la loi du 29 juillet 1993 concernant la protection et la gestion de l’eau;
 - d’une infraction à l’article 35 de la loi modifiée du 17 juin 1994 relative à la prévention et à la gestion des déchets;
 - d’une infraction aux articles 220 et 231 de la loi générale sur les douanes et accises;
 - d’une infraction à l’article 32 de la loi du 9 mai 2006 relative aux abus de marché;
 - de toute autre infraction punie d’une peine privative de liberté d’un minimum supérieur à 6 mois;
- ou constituant un avantage patrimonial quelconque tiré de l’une ou de plusieurs de ces infractions;“

8) L’article 509-3 du Code pénal est complété par un alinéa 2 libellé comme suit:

„Sera puni des mêmes peines celui qui aura intentionnellement et au mépris des droits d’autrui, intercepté des données lors de transmissions non publiques à destination, en provenance ou à l’intérieur d’un système de traitement ou de transmission automatisé de données.“

9) A l’article 509-4 du Code pénal l’alinéa 2 est supprimé.

10) Il est introduit un article 509-5 du Code pénal libellé comme suit:

„**Art. 509-5.** Sera puni de 4 mois à cinq ans d’emprisonnement et d’une amende de 1.250 euros à 30.000 euros quiconque aura, dans une intention frauduleuse, produit, vendu, obtenu, détenu, importé, diffusé ou mis à disposition,

- un dispositif informatique destiné à commettre l’une des infractions visées aux articles 509-1 à 509-4; ou
- toute clef électronique permettant d’accéder, au mépris des droits d’autrui, à tout ou à partie d’un système de traitement ou de transmission automatisé de données.“

Art. 4.– Le Code d’instruction criminelle est modifié et complété comme suit:

1) L’article 7-4 du Code d’instruction criminelle est modifié et complété comme suit:

„**Art. 7-4.** Lorsqu’une personne qui se sera rendue coupable à l’étranger d’une des infractions prévues par les articles 112-1, 135-1 à 135-6, 135-9, 135-11 à 135-13, 136*bis* à 136*quinquies*, 260-1 à 260-4, 379, 382-1, 382-2, 384, 385-2 et 509-1 à 509-7 du Code pénal, n’est pas extradée, l’affaire sera soumise aux autorités compétentes aux fins de poursuites en application des règles prévues.“

2) Le paragraphe 1er de l’article 24-1 du Code d’instruction criminelle est complété comme suit:

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

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

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

3) Le point 3) de l’article 31 du Code d’instruction criminelle est modifié comme suit:

„Il saisit les objets, documents, données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données et effets qui ont servi à commettre le crime ou qui étaient destinés à le commettre et ceux qui ont formé l’objet du crime, de même que tout ce qui paraît avoir été le produit du crime, ainsi qu’en général, tout ce qui paraît utile à la manifestation de la vérité ou dont l’utilisation serait de nature à nuire à la bonne marche de l’instruction et tout ce qui est susceptible de confiscation ou de restitution.“

4) L'article 33 du Code d'instruction criminelle est modifié comme suit:

„(1) Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, données ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces dernières pour y procéder à une perquisition dont il dresse procès-verbal et opérer la saisie. Cette perquisition peut avoir lieu à toute heure du jour ou de la nuit.

(2) Il a seul, avec les personnes désignées à l'article 34 et celles auxquelles il a éventuellement recours en application de l'article 36, le droit de prendre connaissance des papiers, données ou documents avant de procéder à leur saisie.

(3) Toutefois, il a l'obligation de provoquer préalablement toutes mesures utiles pour que soit assuré le respect du secret professionnel et des droits de la défense.

(4) Tous objets, données et documents saisis sont immédiatement inventoriés après avoir été présentés, pour reconnaissance, aux personnes qui paraissent avoir participé à l'infraction, si elles sont présentes, ainsi qu'aux personnes visées à l'article suivant. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés jusqu'au moment de leur inventaire en présence des personnes qui ont assisté à la perquisition.

(5) La saisie des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données peut se faire, soit par la saisie du support physique de ces données, soit par une copie de ces données réalisée en présence des personnes visées à l'article suivant. Si une copie est réalisée, il peut être procédé, sur demande du Procureur d'Etat, à l'effacement définitif sur le support physique, lorsque celui-ci se trouve au Grand-Duché de Luxembourg et qu'il n'a pas été placé sous la main de la justice, des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

(6) Le procès-verbal des perquisitions et des saisies est signé par les personnes qui paraissent avoir participé à l'infraction, par les personnes au domicile desquelles elles ont eu lieu et par les personnes qui y ont assisté; en cas de refus de signer, le procès-verbal en fait mention. Il leur est laissée copie du procès-verbal.

(7) Les objets, données et documents saisis sont déposés au greffe du tribunal d'arrondissement ou confiés à un gardien de saisie.

(8) Avec l'accord du procureur d'Etat, l'officier de police judiciaire ne maintient que la saisie des objets, données et documents utiles à la manifestation de la vérité.

(9) Dans l'intérêt de la manifestation de la vérité, le procureur d'Etat peut ordonner la prise d'empreintes digitales et de photographies des personnes qui paraissent avoir participé au crime flagrant. Les empreintes digitales et les photographies recueillies en application du présent article peuvent être traitées ultérieurement par la Police à des fins de prévention, de recherche et de constatation des infractions pénales.“

5) Le paragraphe 1er de l'article 48-17 du Code d'instruction criminelle est modifié et complété comme suit:

„13. infractions en matière informatique au sens des articles 509-1 à 509-7 du Code pénal.“

6) Le Livre Premier, Titre II du Code d'instruction criminelle est complété par un Chapitre X qui est libellé comme suit:

„Chapitre X.– De la conservation rapide des données informatiques

Art. 48-25. Lorsqu'il y a des raisons de penser que des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, le procureur d'Etat ou le juge d'instruction saisi peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, de ces données.“

7) L'article 66 du Code d'instruction criminelle est modifié et complété comme suit:

„(1) Le juge d'instruction opère la saisie de tous les objets, documents, effets, données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données et autres choses visés à l'article 31(3).

(2) Les objets, documents, effets, données et autres choses saisis sont inventoriés dans le procès-verbal. Si leur inventaire sur place présente des difficultés, ils font l'objet de scellés jusqu'au moment de leur inventaire, en présence des personnes qui ont assisté à la perquisition.

(3) La saisie des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données peut se faire, soit par la saisie du support physique de ces données, soit par une copie de ces données réalisée en présence des personnes qui assistent à la perquisition. Si une copie est réalisée, le juge d'instruction peut ordonner l'effacement définitif sur le support physique, lorsque celui-ci se trouve au Grand-Duché de Luxembourg et qu'il n'a pas été placé sous la main de la justice, des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

(4) Le juge d'instruction peut, par ordonnance motivée, enjoindre à une personne, hormis la personne visée par l'instruction, dont il considère qu'elle a une connaissance particulière du système de traitement ou de transmission automatisé de données ou du mécanisme de protection ou de cryptage, qu'elle lui donne accès au système saisi, aux données saisies contenues dans ce système ou aux données saisies accessibles à partir de ce système ainsi qu'à la compréhension de données saisies protégées ou cryptées. Sous réserve des articles 72, 73 et 76 ci-dessous, la personne désignée est tenue de prêter son concours.

(5) Le procès-verbal des perquisitions et des saisies est signé par l'inculpé, par la personne au domicile de laquelle elles ont été opérées et par les personnes qui y ont assisté; en cas de refus de signer, le procès-verbal en fait mention. Il leur est laissée copie du procès-verbal.

(6) Les objets, documents, effets, données et autres choses saisis sont déposés au greffe ou confiés à un gardien de saisie.“

8) L'article 67-1 du Code d'instruction criminelle est modifié comme suit:

„**Art. 67-1.** (1) Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité, et si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de télécommunications:

1. au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés;
2. à la localisation de l'origine ou de la destination de télécommunications.

Dans les cas visés à l'alinéa 1er, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur d'Etat.

Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder un mois à dater de l'ordonnance, sans préjudice de renouvellement.

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

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

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

(3) La personne dont un moyen de télécommunication a fait l'objet de la mesure prévue au paragraphe (1) est informée de la mesure ordonnée au cours même de l'instruction et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance. Toutefois ce délai de 12 mois ne s'applique pas lorsque la mesure a été ordonnée dans une instruction pour des faits qui se situent dans le cadre ou en relation avec une association ou une organisation criminelle au sens des articles 322 à 324ter du Code pénal, ou qui se situent dans le cadre ou en relation avec le terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-13 du Code pénal, ou au sens de l'article 10, alinéa 1er de la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie.

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

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

Art. 5.– 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 4, paragraphe (3), la lettre (b) est remplacée par le texte suivant:

„(b) ne s'applique pas aux autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales;“

2) Le paragraphe (2) de l'article 5 est modifié comme suit:

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

- ordonnés par les autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a), ou
- demandés par les organes compétents dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation.“

3) Le paragraphe (2) de l'article 9 est modifié comme suit:

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

Luxembourg, le 28 mai 2014

Le Rapporteur,
Guy ARENDT

La Présidente,
Viviane LOSCHETTER