



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Projet de loi 6514

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

Date de dépôt : 12-12-2012

Date de l'avis du Conseil d'État : 08-04-2014

Liste des documents

Date	Description	Nom du document	Page
18-07-2014	Résumé du dossier	Résumé	<u>3</u>
12-12-2012	Déposé	6514/00	<u>5</u>
13-03-2013	Avis de la Chambre de Commerce (27.2.2013)	6514/01	<u>48</u>
17-04-2013	Avis du Conseil d'Etat (16.4.2013)	6514/02	<u>53</u>
10-06-2013	Amendements adoptés par la/les commission(s) : Commission juridique	6514/03	<u>64</u>
14-11-2013	Avis complémentaire du Conseil d'Etat (12.11.2013)	6514/04	<u>83</u>
20-03-2014	Amendements adoptés par la/les commission(s) : Commission juridique	6514/05	<u>88</u>
08-04-2014	Deuxième avis complémentaire du Conseil d'Etat (4.4.2014)	6514/06	<u>99</u>
28-05-2014	Rapport de commission(s) : Commission juridique Rapporteur(s) : Monsieur Guy Arendt	6514/07	<u>102</u>
04-06-2014	Premier vote constitutionnel (Vote Positif) En séance publique n°22 Une demande de dispense du second vote a été introduite	6514	<u>127</u>
26-06-2014	Dispense du second vote constitutionnel par le Conseil d'Etat (26-06-2014) Evacué par dispense du second vote (26-06-2014)	6514/08	<u>130</u>
28-05-2014	Commission juridique Procès verbal (19) de la reunion du 28 mai 2014	19	<u>133</u>
23-04-2014	Commission juridique Procès verbal (15) de la reunion du 23 avril 2014	15	<u>141</u>
19-03-2014	Commission juridique Procès verbal (12) de la reunion du 19 mars 2014	12	<u>147</u>
26-02-2014	Commission juridique Procès verbal (09) de la reunion du 26 février 2014	09	<u>153</u>
05-06-2013	Commission juridique Procès verbal (37) de la reunion du 5 juin 2013	37	<u>161</u>
15-05-2013	Commission juridique Procès verbal (34) de la reunion du 15 mai 2013	34	<u>168</u>
08-05-2013	Commission juridique Procès verbal (33) de la reunion du 8 mai 2013	33	<u>183</u>
24-04-2013	Commission juridique Procès verbal (32) de la reunion du 24 avril 2013	32	<u>198</u>
17-04-2013	Commission juridique Procès verbal (31) de la reunion du 17 avril 2013	31	<u>210</u>
13-08-2014	Publié au Mémorial A n°157 en page 2406	6514	<u>225</u>

Résumé

N° 6514

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,**
 - 1) **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,**
 - 1) **modification du Code pénal,**
 - 1) **modification du Code d'instruction criminelle**
 - 1) **modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques**
-

Résumé

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 pré mentionnés 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.

6514/00

N° 6514**CHAMBRE DES DEPUTES**

Session ordinaire 2012-2013

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

* * *

*(Dépôt: le 12.12.2012)***SOMMAIRE:**

	<i>page</i>
1) Arrêté Grand-Ducal de dépôt (5.12.2012)	2
2) Texte du projet de loi	2
3) Exposé des motifs	8
4) Commentaire des articles	10
5) Texte de la Convention	15
6) Texte du Protocole	36

*

ARRETE GRAND-DUCAL DE DEPOT

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

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

Arrêtons:

Article unique.– Notre Ministre de la Justice est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi portant:

- 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.

Palais de Luxembourg, le 5 décembre 2012

Le Ministre de la Justice,

François BILTGEN

HENRI

*

TEXTE DU PROJET DE LOI

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) L'article 231 du Code pénal est modifié comme suit:

„Quiconque aura publiquement pris un nom, ou une identification de quelque nature qu'elle soit, qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à un an, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement.“

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

„**Art. 231bis.**– 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 une identification de quelque nature qu'elle soit, 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.“

- 3) 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 251 euros à 5.000 euros“.
- 4) 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.“.

5) 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 et 135-9 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 et 382-2 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 à l'article 143 de la loi du 29 août portant sur la libre circulation des personnes et l'immigration;
 - 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;“

6) 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 ou tenté d'intercepter des données informatiques lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données.“

7) A l'article 509-4 du Code pénal l'alinéa 2 est supprimé.

8) 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 251 euros à 5.000 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
- un mot de passe, 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.“

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.** Toute 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 135-13¹, 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, pourra être poursuivie et jugée au Grand-Duché, lorsqu'une demande d'extradition est introduite et que l'intéressé n'est pas extradé.“

2) Le point (1) de l'article 24-1 du Code d'instruction criminelle est complété 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 ne soit ouverte.

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

Pour les infractions visées à l'alinéa qui précède ou si les faits 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:

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, conformément à l'article 67-1 et sans qu'une instruction préparatoire ne soit ouverte.“

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 informatique 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 informatique ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, données

¹ Projet de loi n° 6388

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 informatique 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 informatique 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 laissé 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 point (1) de l'article 48-17 du Code d'instruction criminelle est modifié et complété comme suit:

„12. enlèvement de mineurs au sens des articles 368 à 371-1 du Code pénal;

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 informatique, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, l'officier de police judiciaire, de l'accord du Procureur d'Etat ou du juge d'instruction saisi, peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, des données stockées, traitées ou transmises dans un système informatique.“.

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 informatique 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 informatique 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 informatique 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 informatique 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 laissé 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:

„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, 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, si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.

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) (L. 12 août 2003) 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 ou 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. 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 135-4 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, ou à l'article 24-1 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 ou de l'enquête préliminaire et détruites dans la mesure où elles concernent des personnes non visées par l'instruction ou l'enquête préliminaire.“

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 au titre des articles 48-25 et 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales;“.

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 au titre des articles 48-25 et 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a), ou
- demandés par les organes compétents dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation“.

3) 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 au titre des articles 48-25 et 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a).“.

*

EXPOSE DES MOTIFS

Considérations générales

Le présent projet de loi a pour objet l'approbation de certaines dispositions du Code pénal visant plus particulièrement la lutte contre la cybercriminalité.

1. Introduction

La non-ratification par le Luxembourg de la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 dite „Convention de Budapest“ (ci-après „la Convention“) et de son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques du 28 janvier 2003 (ci-après „le Protocole“) est devenue l'objet de pressions de la part de différentes organisations internationales (CdE, UE, ONU, ...) et ce d'autant plus que le Luxembourg est l'un des derniers pays signataires à ne pas encore avoir ratifié ces instruments.

Les pays voisins du Luxembourg et la Suisse ont tous ratifié les instruments susmentionnés. Au vu des lois intervenues en Belgique, en France et en Suisse, on constate que les changements effectués sont minimaux, que ce soit en matière de droit pénal matériel ou en matière de coopération internationale.

A remarquer également qu'une proposition de directive visant à remplacer la décision-cadre 2005/222/JAI relative aux attaques visant les systèmes d'information a été formellement adoptée par le Conseil de l'Union européenne; le texte définitif négocié avec le parlement européen n'attend plus que le feu vert de ce dernier pour entrer en vigueur. L'objectif de cette directive étant d'aligner les dispositions européennes sur la Convention, elle sera en pratique transposée avant la lettre dans le cadre du présent projet de loi.

La Convention comporte quatre chapitres, à savoir le chapitre I „Terminologie“, le chapitre II „Mesures à prendre au niveau national“, le chapitre III „Coopération internationale“ et le chapitre IV „Clauses finales“. La législation luxembourgeoise actuelle couvre la majeure partie des articles de la Convention de sorte que ni les dispositions de droit pénal matériel, ni celles concernant la coopération internationale ne nécessiteront des changements ou ajouts majeurs. C'est pourquoi les auteurs du présent projet de loi ont opté pour une insertion des nouvelles infractions dans le Code pénal respectivement le Code d'instruction criminelle et non pas pour une loi sur la cybercriminalité à part.

2. La Convention du Conseil de l'Europe sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité (ci-après „la Convention“) a été élaborée par le comité d'experts sur la criminalité dans le cyber-espace (PC-CY), créé au sein du Comité européen pour les problèmes criminels du Conseil de l'Europe (CD-PC), et qui a commencé ces travaux en avril 1997.

La nécessité d'élaborer une telle convention dès la fin des années 90 s'explique selon le rapport explicatif du Conseil de l'Europe par „la révolution des technologies de l'information qui a changé radicalement la société et continuera vraisemblablement de le faire dans un avenir prévisible“. Car dans le sillage de cette évolution technologique sont apparus outre de nombreux bienfaits également „de nouveaux types de délinquance“ et des délits classiques commis à l'aide des nouvelles technologies. La caractéristique la plus marquante et la plus grave de cette nouvelle délinquance est le fait „qu'elle ne se cantonne plus à un espace géographique donné et ne se soucie guère des frontières nationales“. C'est pourquoi il faut mettre en place „des mesures de protection des systèmes informatiques en même temps que des mesures juridiques de prévention et de dissuasion de la délinquance“. Le fait que la cybercriminalité ne connaît pas de frontière au sens classique du terme implique que „les solutions aux problèmes relèvent nécessairement du droit international ce qui nécessite l'adoption d'instruments internationaux adéquats“.

Le mandat donné au nouveau comité consistait à examiner les problèmes de procédure pénale liés à la technologie de l'information et notamment les infractions commises dans le cyber-espace, les questions de droit pénal matériel nécessitant une approche commune en vue d'une coopération internationale, le recours à des pouvoirs coercitifs et la viabilité d'un tel recours dans un environnement

technique, la question de la compétence vis-à-vis des infractions informatiques et les questions de coopération internationale.

La Convention a été ouverte à la signature à Budapest le 23 novembre 2001 et est entrée en vigueur le 1er juillet 2004. En novembre 2012, 47 pays avaient signé la Convention et 37 de ces derniers l'avaient également ratifiée (dont les Etats-Unis).

Il s'agit d'un instrument juridique exhaustif composé de quatre chapitres différents couvrant tous les aspects importants relatifs à la lutte contre la cybercriminalité, à savoir:

- la terminologie (système informatique, données informatiques, fournisseur de service);
- le droit pénal matériel;
- les questions de droit procédural;
- les dispositions relatives à l'entraide et l'extradition.

3. 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

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 (ci-après „le Protocole“) a été élaboré par le comité d'experts sur l'incrimination des actes de nature raciste et xénophobe par le biais de systèmes informatiques (PC-RX), créé au sein du Comité européen pour les problèmes criminels du Conseil de l'Europe (CD-PC), et qui a commencé ses travaux en septembre 2001.

La raison de l'élaboration du Protocole s'explique selon le rapport explicatif du Conseil de l'Europe par „l'apparition de réseaux de communication globale comme Internet qui offrent à certaines personnes des moyens modernes et puissants pour soutenir le racisme et la xénophobie“ et leur permet de „diffuser facilement et largement des contenus exprimant de telles idées“. Afin de pouvoir combattre efficacement de tels agissements la coopération internationale s'avère essentielle et c'est pourquoi le Protocole veut d'un côté „harmoniser le droit pénal matériel dans la lutte contre le racisme et la xénophobie sur l'Internet et également améliorer la coopération internationale dans ce domaine“.

Le mandat donné au comité d'experts consistait à traiter de la définition et de l'étendue d'éléments en vue de l'incrimination des actes de nature raciste et xénophobe commis à travers les réseaux informatiques et la mesure dans laquelle les dispositions de droit matériel, procédural et de coopération internationale contenues dans la Convention s'appliquent aux enquêtes et aux poursuites relatives aux infractions à établir dans le Protocole.

Le Protocole a été ouvert à la signature à Strasbourg le 28 janvier 2003 et est entré en vigueur le 1er mars 2006. En novembre 2012, 35 pays avaient signé le Protocole et 20 de ces derniers l'avaient également ratifié.

Il emporte un élargissement de la portée de la Convention de manière à couvrir également les infractions concernant la propagande raciste et xénophobe par le biais d'une harmonisation des éléments de droit pénal matériel et de l'amélioration des moyens de coopération internationale dans ce domaine.

Les dispositions contenues dans le Protocole sont couvertes par les dispositions législatives actuellement en vigueur au Luxembourg de sorte qu'il n'y a pas de modifications législatives à prévoir.

*

COMMENTAIRE DES ARTICLES

Article 1er du projet de loi

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

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.

Article 3 du projet de loi

Ad articles 231 et 231bis du Code pénal

La modification de l'article 231 du Code pénal cumulée avec le nouvel article 231bis a pour but de réprimer l'usurpation d'identité de manière générale, peu importe qu'elle ait lieu dans le monde „réel“ de tous les jours, ou qu'elle ait lieu sur des réseaux de communication en ligne, du moment qu'elle se commet soit en public, soit dans l'intention de nuire d'une manière ou d'une autre à une tierce personne.

Le texte proposé s'inspire de l'article 226-4-1 du Code pénal français, sans pour autant le reprendre, ce texte étant en conflit avec d'autres textes du Code pénal luxembourgeois.

Ainsi l'actuel article 231 est complété par la rajoute du port public de toute sorte de fausse identification. En effet, la cour d'appel dans son arrêt du 27 février 2007, n° 125/07 V. retient que le „nom“ ne se rapporte qu'au seul nom patronymique, excluant ainsi la possibilité d'appliquer l'article 231 dans sa version actuelle entre autres aux certificats Luxtrust (signatures électroniques), qui donnent une identification certaine d'une personne physique ou morale à une administration étatique, comme par exemple l'Administration de l'Enregistrement et des Domaines, sans pour autant livrer directement un nom. Il en est de même de la matricule de la sécurité sociale qui constitue une identification certaine d'une personne sans pour autant donner nécessairement un nom patronymique. Ainsi est réprimé d'un côté le port public de toute identification quelconque, y compris les identifications électroniques, qui n'appartient pas à la personne qui en fait usage. La sécurité juridique, notamment en matière de signature électronique, rend nécessaire ce complément.

Ensuite, pour tenir compte notamment des comportements dans les réseaux sociaux, il est introduit un nouvel article 231bis du Code pénal. 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.

Dans l'article 231 modifié c'est la publicité de l'usurpation qui est punie comme pour l'article 231 dans sa version originale et donc peu importe le mobile. L'article 231bis quant à lui n'exige aucune publicité, mais uniquement l'intention de nuire à un tiers pour rendre répréhensible l'usurpation d'identité.

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 des deux articles sont également inspirées par celles des articles 442-2 et 444 du code pénal.

Ad article 488 du Code pénal

Le seuil de peine de l'article 488 du Code pénal doit être adapté au seuil de peine prévu au nouvel article 509-5 du Code pénal tel que proposé dans le présent projet de loi 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.

Ad article 496 alinéa 1er du Code pénal

L'article 496 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 afin de commettre l'escroquerie.

Il résulte en effet d'un arrêt n° 261/10 X 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 qui consiste selon le Petit Larousse en une „*technique de fraude par courriel, basée sur l'usurpation d'identité, afin d'obtenir de particuliers des renseignements confidentiels (mots de passe, numéros de cartes de crédit)*“. La Cour de dire: „Certes, et les premiers juges l'ont correctement relevé, le prévenu a fait usage d'un faux nom et de manoeuvres frauduleuses à l'encontre de la victime pour obtenir le mot de passe en question en lui envoyant, sous un faux nom, un message par internet dans lequel il l'invitait à communiquer, pour des raisons techniques, son mot de passe à son fournisseur Hotmail. Mais contrairement au raisonnement des premiers juges, la Cour est d'avis que le mot de passe ne constitue pas un meuble au sens de l'article 496 du code pénal. En effet contrairement aux données ou programmes informatiques susceptibles d'être enregistrés, transmis ou reproduits sous la forme d'impulsions dans des circuits électroniques ou sur des bandes ou disques magnétiques et dont la délivrance peut dès lors être constatée matériellement, le mot de passe composé d'une suite de caractères servant de moyen d'authentification à son utilisateur ne constitue qu'une simple clé électronique n'ayant aucune présence matérielle et ne pouvant partant pas être remise ou délivrée à l'auteur de l'infraction.“

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) 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.

Ad article 506-1, point 1) du Code pénal

Les auteurs ont fait le choix, pour préserver la cohérence interne du Code pénal, 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.

Ad article 509-3 du Code pénal

Le nouvel alinéa 2 de l'article 509-3 du Code pénal introduit l'interception illégale dans le Code pénal luxembourgeois.

L'interception illégale constitue en quelque sorte un des corollaires de l'infraction d'accès illégale, telle que prévue à l'article 509-3 du Code pénal.

Cette infraction figure à l'article 3 de la Convention de Budapest et à l'article 6 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 les points 53 et 54 du rapport explicatif de la Convention exposent que „*l'interception effectuée par des „moyens techniques“ concerne l'écoute, le contrôle ou la surveillance du contenu des communications, et l'obtention du contenu soit directement, au moyen de l'accès au système informatique et de son utilisation, soit indirectement, au moyen de l'emploi de dispositifs d'écoute. L'interception peut aussi consister en un enregistrement des données. Par moyens techniques, il faut entendre des dispositifs techniques connectés aux lignes de transmission ainsi que des dispositifs de collecte et d'enregistrement de communications sans fil. Ils peuvent consister en logiciels, mots d'accès et codes. L'exigence de l'utilisation de moyens techniques est une condition restrictive visant à éviter l'écueil de la surpénalisation.*

L'infraction s'applique aux transmissions „non publiques“ de données informatiques. Le terme „non publiques“ qualifie la nature du moyen de transmission (communication), non la nature des données transmises. Il peut arriver que les données transmises soient disponibles pour tout le monde, mais que les participants souhaitent communiquer de façon confidentielle. Les données peuvent aussi être tenues secrètes à des fins commerciales jusqu'à ce que le service ait été rémunéré, comme pour la télévision payante. Il s'ensuit que le terme „non publiques“ n'exclut pas en soi les communications

par le biais des réseaux publics. Les communications de salariés, à des fins professionnelles ou non, qui constituent des „transmissions non publiques de données informatiques“ sont aussi protégées contre l’interception sans droit en vertu de l’article 3 (voir, par exemple, l’arrêt rendu par la CEDH dans l’affaire Halford c. Royaume-Uni, 25 juin 1997, 20605/92).“

La notion „sans droit“ est définie d’un côté à l’article 1er de la directive: *„un accès, une atteinte à l’intégrité, une interception, ou tout autre comportement visé dans la présente directive non autorisé par le propriétaire ou autre détenteur de droits au système ou à une partie du système, ou non prévu par la législation nationale“* et de l’autre côté au point 58 du rapport explicatif de la Convention en vertu duquel *„Pour que la responsabilité pénale soit engagée, l’interception illégale doit être „intentionnelle“ et „sans droit“. L’acte est justifié, par exemple, si la personne qui effectue l’interception est en droit de le faire, si elle agit sur ordre ou avec l’autorisation des participants à la transmission (y compris dans le cadre d’activités autorisées de contrôle ou de protection approuvées par les participants) ou si la surveillance est légalement autorisée par les autorités chargées d’une enquête dans l’intérêt de la sécurité nationale ou de la détection d’infractions. Il est également entendu que les pratiques commerciales ordinaires, telles que l’utilisation de „cookies“, ne doivent pas être pénalisées en tant que telles, car il ne s’agit pas d’interception „sans droit“. S’agissant des communications non publiques de salariés protégées en vertu de l’article 3 (voir le paragraphe 54 ci-dessus), le droit interne peut prévoir un motif d’interception légitime de telles communications. Dans le cadre de l’article 3, une interception effectuée dans de telles conditions serait assimilée à une interception effectuée „avec droit“.“*

Ad article 509-4 alinéa 2 du Code pénal

La suppression de l’alinéa 2 de l’article 509-4 est une mesure technique due à l’introduction d’un nouvel article 509-5 tel que proposé dans le présent projet de loi.

Ad article 509-5 du Code pénal

L’introduction d’un nouvel article 509-5 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.

Les auteurs du projet de loi se distinguent du libellé du paragraphe 1. a) 1) de l’article 6 de la Convention en remplaçant la référence au *„dispositif principalement conçu ou adapté pour commettre l’une des infractions“* par la référence à un *„dispositif destiné à commettre l’une des infractions“*, cette notion étant plus souple.

L’exigence de l’intention frauduleuse se déduit de l’exigence de l’article 6 de la Convention qui dispose que les infractions doivent avoir été *„commises intentionnellement et sans droit“*. Le paragraphe 76 du rapport explicatif de la Convention en fournit d’ailleurs l’explication en précisant que *„l’infraction doit être commise intentionnellement et sans droit. Avant d’éviter le risque de la surpénalisation lorsque des dispositifs sont fabriqués et commercialisés à des fins légitimes, par exemple pour contrer des atteintes aux systèmes informatiques, des critères supplémentaires sont ajoutés pour restreindre l’infraction. En sus de l’exigence générale de l’intention, il doit exister l’intention spécifique (c’est-à-dire directe) d’utiliser le dispositif pour commettre l’une ou l’autre des infractions visées aux articles 2 à 5 de la Convention“*.

Article 4 du projet de loi

Ad 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.

Ad 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 ainsi engendrée on risquerait de perdre toutes les données. Or, pour le moment le repérage ne peut qu'être autorisé 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.

Ad article 31, point (3) du Code d'instruction criminelle

Cette modification de l'article 31 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.

Ad article 33 du Code d'instruction criminelle

Cette modification de l'article 33 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. L'introduction d'un nouveau point (5) a été décidé pour 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.

Ad article 48-17 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.

Ad Livre Premier, Titre II 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.

Le problème pour satisfaire à l'exigence de conservation rapide est le suivant dans l'état actuel de notre droit: En effet 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 délit ou 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, 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 le cadre de commissions rogatoires internationales. 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.

Ad article 66 du Code d'instruction criminelle

Cette 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 point (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 configure les logiciels et sont souvent détentrices de mots de passe ou de codes sans lesquels un accès est impossible.

Ad 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.

Article 5 du projet de loi

Ad article 4 paragraphe 3 (b) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Cet article étant relatif à la confidentialité des communications et des données relatives au trafic, il excepte cependant de la confidentialité les autorités judiciaires agissant en vertu des articles du Code d'instruction criminelle. Il convient donc d'y rajouter une référence au nouvel article 48-25 du Code d'instruction criminelle introduit par ce projet de loi.

Ad article 5 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Cet article étant relatif aux fournisseurs de services, de leur obligation de conservation des données relatives au trafic et de leur collaboration le cas échéant avec les autorités judiciaires, il convient d'y rajouter une référence au nouvel article 48-25 du Code d'instruction criminelle introduit par ce projet de loi.

Ad article 9 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Cet article étant relatif aux fournisseurs de services ou opérateurs, de leur obligation de conservation des données de localisation autres que les données relatives au trafic et de leur collaboration le cas échéant avec les autorités judiciaires, il convient d'y rajouter une référence au nouvel article 48-25 du Code d'instruction criminelle introduit par ce projet de loi.

*

TEXTE DE LA CONVENTION

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberspace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999);

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberspace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

SONT CONVENUS de ce qui suit:

Chapitre I – Terminologie

Article 1

Définitions

Aux fins de la présente Convention,

- a l'expression „système informatique“ désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
- b l'expression „données informatiques“ désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
- c l'expression „fournisseur de services“ désigne:
 - i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
 - ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
- d „données relatives au trafic“ désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1

Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2

Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3

Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4

Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5

Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6

Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

- a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:
 - i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
 - ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,
 dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et
- b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 Infractions informatiques

Article 7

Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8

Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

- a par toute introduction, altération, effacement ou suppression de données informatiques;
 - b par toute forme d'atteinte au fonctionnement d'un système informatique,
- dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3

Infractions se rapportant au contenu

*Article 9****Infractions se rapportant à la pornographie infantine***

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

- a la production de pornographie infantine en vue de sa diffusion par le biais d'un système informatique;
- b l'offre ou la mise à disposition de pornographie infantine par le biais d'un système informatique;
- c la diffusion ou la transmission de pornographie infantine par le biais d'un système informatique;
- d le fait de se procurer ou de procurer à autrui de la pornographie infantine par le biais d'un système informatique;
- e la possession de pornographie infantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme „pornographie infantine“ comprend toute matière pornographique représentant de manière visuelle:

- a un mineur se livrant à un comportement sexuellement explicite;
- b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
- c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme „mineur“ désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e. et 2, alinéas b. et c.

Titre 4

Infractions liées aux atteintes à la propriété intellectuelle
et aux droits connexes*Article 10****Infractions liées aux atteintes à la propriété intellectuelle
et aux droits connexes***

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la

législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5

Autres formes de responsabilité et de sanctions

Article 11

Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12

Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

- a sur un pouvoir de représentation de la personne morale;
- b sur une autorité pour prendre des décisions au nom de la personne morale;
- c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présente Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

*Article 13****Sanctions et mesures***

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1

Dispositions communes

*Article 14****Portée d'application des mesures du droit de procédure***

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:

- a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;
- b à toutes les autres infractions pénales commises au moyen d'un système informatique; et
- c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:

- i qui est mis en oeuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
- ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

*Article 15****Conditions et sauvegardes***

1 Chaque Partie veille à ce que l'instauration, la mise en oeuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de

la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2

Conservation rapide de données informatiques stockées

Article 16

Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en oeuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17

Conservation et divulgation rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

- a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et
- b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3
Injonction de produire

Article 18

Injonction de produire

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:
 - a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et
 - b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
- 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
- 3 Aux fins du présent article, l'expression „données relatives aux abonnés“ désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:
 - a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
 - b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
 - c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4
Perquisition et saisie de données informatiques stockées

Article 19

Perquisition et saisie de données informatiques stockées

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:
 - a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et
 - b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.
- 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour

lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

- a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;
- b réaliser et conserver une copie de ces données informatiques;
- c préserver l'intégrité des données informatiques stockées pertinentes;
- d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5

Collecte en temps réel de données informatiques

Article 20

Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

- a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et
- b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:
 - i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21

Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne:

- a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

- b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:
 - i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22

Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:

- a sur son territoire; ou
- b à bord d'un navire battant pavillon de cette Partie; ou
- c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou
- d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1

Principes généraux relatifs à la coopération internationale

Article 23

Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2

Principes relatifs à l'extradition

Article 24

Extradition

- 1
 - a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.
 - b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.
- 2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.
- 3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.
- 4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.
- 5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.
- 6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront

l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

- 7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.
- b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3

Principes généraux relatifs à l'entraide

Article 25

Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26

Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire

ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4

Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27

Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

- 2
 - a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;
 - b Les autorités centrales communiquent directement les unes avec les autres;
 - c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;
 - d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:

- a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
- b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

- 9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.
- b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).
- c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.
- d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.
- e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28

Confidentialité et restriction d'utilisation

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:

- a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou
- b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1

Entraide en matière de mesures provisoires

Article 29

Conservation rapide de données informatiques stockées

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

- 2 Une demande de conservation faite en application du paragraphe 1 doit préciser:
- a l'autorité qui demande la conservation;
 - b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;
 - c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;
 - d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;
 - e la nécessité de la mesure de conservation; et
 - f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.
- 3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.
- 4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.
- 5 En outre, une demande de conservation peut être refusée uniquement:
- a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
 - b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.
- 6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.
- 7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30

Divulgation rapide de données conservées

- 1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.
- 2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:
- a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
 - b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2

Entraide concernant les pouvoirs d'investigation

*Article 31****Entraide concernant l'accès aux données stockées***

- 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.
- 2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.
- 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:
 - a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou
 - b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

*Article 32****Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public***

Une Partie peut, sans l'autorisation d'une autre Partie:

- a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
- b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

*Article 33****Entraide dans la collecte en temps réel de données relatives au trafic***

- 1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.
- 2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

*Article 34****Entraide en matière d'interception de données relatives au contenu***

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3
Réseau 24/7

Article 35

Réseau 24/7

- 1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:
 - a apport de conseils techniques;
 - b conservation des données, conformément aux articles 29 et 30;
 - c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.
- 2
 - a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.
 - b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.
- 3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – *Clauses finales*

Article 36

Signature et entrée en vigueur

- 1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.
- 2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.
- 3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.
- 4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37

Adhésion à la Convention

- 1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38

Application territoriale

1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39

Effets de la Convention

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:

- de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24);
- de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30);
- du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40

Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

*Article 41***Clause fédérale**

1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constitutants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constitutants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constitutants, en les encourageant à adopter les mesures appropriées pour les mettre en oeuvre.

*Article 42***Réserves**

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

*Article 43***Statut et retrait des réserves**

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

*Article 44***Amendements**

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45

Règlement des différends

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46

Concertation des Parties

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter:

- a l'usage et la mise en oeuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;
- b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;
- c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47

Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48

Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer:

- a toute signature;
- b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;
- c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37;
- d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42;
- e tout autre acte, notification ou communication ayant trait à la présente Convention.

EN FOI DE QUOI, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

FAIT à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

*

TEXTE DU PROTOCOLE

Les Etats membres du Conseil de l'Europe et les autres Etats parties à la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, signataires du présent Protocole;

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Rappelant que tous les êtres humains sont nés libres et égaux en dignité et en droits;

Soulignant la nécessité de garantir une mise en oeuvre exhaustive et efficace de tous les droits de l'homme sans distinction ni discrimination, tels qu'énoncés dans les instruments européens et autres instruments internationaux;

Convaincus que des actes de nature raciste et xénophobe constituent une violation des droits de l'homme, ainsi qu'une menace pour l'Etat de droit et la stabilité démocratique;

Considérant que le droit national et le droit international nécessitent de prévoir une réponse juridique adéquate à la propagande de nature raciste et xénophobe diffusée par le biais des systèmes informatiques;

Conscients que la propagande de tels actes est souvent criminalisée par les législations nationales;

Ayant égard à la Convention sur la cybercriminalité qui prévoit des moyens flexibles et modernes de coopération internationale, et convaincus de la nécessité d'harmoniser la lutte contre la propagande raciste et xénophobe;

Conscients de ce que les systèmes informatiques offrent un moyen sans précédent de faciliter la liberté d'expression et de communication dans le monde entier;

Reconnaissant que la liberté d'expression constitue l'un des principaux fondements d'une société démocratique, et qu'elle est l'une des conditions essentielles de son progrès et de l'épanouissement de chaque être humain;

Préoccupés toutefois par le risque que ces systèmes informatiques soient utilisés à mauvais escient ou de manière abusive pour diffuser une propagande raciste et xénophobe;

Convaincus de la nécessité d'assurer un bon équilibre entre la liberté d'expression et une lutte efficace contre les actes de nature raciste et xénophobe;

Reconnaissant que ce Protocole ne porte pas atteinte aux principes établis dans le droit interne concernant la liberté d'expression;

Tenant compte des instruments juridiques internationaux pertinents dans ce domaine, et en particulier de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales et de son Protocole n° 12 relatif à l'interdiction générale de la discrimination, des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, en particulier de la Convention sur la cybercriminalité et de la Convention internationale des Nations Unies du 21 décembre 1965 sur l'élimination de toutes les formes de discrimination raciale, l'Action commune du 15 juillet 1996 de l'Union européenne adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne concernant l'action contre le racisme et la xénophobie;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la cybercriminalité, ainsi que celle contre le racisme et la xénophobie;

Prenant également en compte le Plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet, tenu à Strasbourg les 10 et 11 octobre 1997, afin de chercher des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

SONT CONVENUS de ce qui suit:

Chapitre I – Dispositions communes

Article 1

But

Le but du présent Protocole est de compléter, pour les Parties au Protocole, les dispositions de la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001 (appelé ci-après „la Convention“) eu égard à l'incrimination des actes de nature raciste et xénophobe diffusés par le biais de systèmes informatiques.

Article 2

Définition

- 1 Aux fins du présent Protocole, l'expression:
„*matériel raciste et xénophobe*“ désigne tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes.
- 2 Les expressions et termes employés dans ce Protocole sont interprétés de la même manière qu'ils le sont dans la Convention.

Chapitre II – Mesures à prendre au niveau national

Article 3

Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants:

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe.

2 Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.

3 Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.

Article 4

Menace avec une motivation raciste et xénophobe

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant:

la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 5

Insulte avec une motivation raciste et xénophobe

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant:

l'insulte en public, par le biais d'un système informatique, (i) d'une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.

2 Une Partie peut:

- a soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule;
- b soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

*Article 6****Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité***

1 Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants:

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.

2 Une Partie peut:

- a soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments;
- b soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

*Article 7****Aide et complicité***

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, en vertu de son droit interne, lorsqu'il est commis intentionnellement et sans droit, le fait d'aider à perpétrer une infraction telle que définie dans ce Protocole, ou d'en être complice, avec l'intention qu'une telle infraction soit commise.

Chapitre III – Relations entre la Convention et ce Protocole*Article 8****Relations entre la Convention et ce Protocole***

1 Les articles 1, 12, 13, 22, 41, 44, 45 et 46 de la Convention s'appliquent, *mutatis mutandis*, à ce Protocole.

2 Les Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole.

Chapitre IV – Dispositions finales*Article 9****Expression du consentement à être lié***

1 Le présent Protocole est ouvert à la signature des Etats signataires de la Convention, qui peuvent exprimer leur consentement à être liés par:

- a la signature sans réserve de ratification, d'acceptation ou d'approbation; ou
- b la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.

2 Un Etat ne peut signer le présent Protocole sans réserve de ratification, d'acceptation ou d'approbation ni déposer un instrument de ratification, d'acceptation ou d'approbation s'il n'a pas déjà déposé ou ne dépose pas simultanément un instrument de ratification, d'acceptation ou d'approbation de la Convention.

3 Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

Article 10

Entrée en vigueur

1 Le présent Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats auront exprimé leur consentement à être liés par le Protocole conformément aux dispositions de l'article 9.

2 Pour tout Etat qui exprimera ultérieurement son consentement à être lié par le Protocole, celui-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de sa signature sans réserve de ratification, d'acceptation ou d'approbation ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation.

Article 11

Adhésion

1 Après l'entrée en vigueur du présent Protocole, tout Etat qui a adhéré à la Convention pourra adhérer également au Protocole.

2 L'adhésion s'effectuera par le dépôt, près le Secrétaire Général du Conseil de l'Europe, d'un instrument d'adhésion qui prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de son dépôt.

Article 12

Réserves et déclarations

1 Les réserves et les déclarations formulées par une Partie concernant une disposition de la Convention s'appliqueront également à ce Protocole, à moins que cette Partie n'exprime l'intention contraire au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion.

2 Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou des réserves prévues aux articles 3, 5 et 6 du présent Protocole. Une Partie peut aussi formuler, par rapport aux dispositions de ce Protocole, les réserves prévues à l'article 22, paragraphe 2, et à l'article 41, paragraphe 1, de la Convention, sans préjudice de la mise en oeuvre faite par cette Partie par rapport à la Convention. Aucune autre réserve ne peut être formulée.

3 Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la possibilité de prévoir des éléments additionnels, tels que prévus à l'article 5, paragraphe 2.a, et à l'article 6, paragraphe 2.a, de ce Protocole.

Article 13

Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 12 ci-dessus retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception

d'une notification de retrait par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves en application de l'article 12 des informations sur les perspectives de leur retrait.

Article 14

Application territoriale

1 Toute Partie peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera le présent Protocole.

2 Toute Partie peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de ce Protocole à tout autre territoire désigné dans la déclaration. Le Protocole entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 15

Dénonciation

1 Toute Partie peut, à tout moment, dénoncer le présent Protocole par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 16

Notification

Le Secrétaire Général du Conseil de l'Europe notifiera aux Etats membres du Conseil de l'Europe, aux Etats non-membres ayant participé à l'élaboration du présent Protocole, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer:

- a toute signature;
- b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;
- c toute date d'entrée en vigueur du présent Protocole conformément à ses articles 9, 10 et 11;
- d tout autre acte, notification ou communication ayant trait au présent Protocole.

EN FOI DE QUOI, les soussignés, dûment autorisés à cet effet, ont signé le présent Protocole.

FAIT à Strasbourg, le 28 janvier 2003, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non-membres ayant participé à l'élaboration du présent Protocole et à tout Etat invité à y adhérer.

CTIE – Division Imprimés et Fournitures de bureau

6514/01

N° 6514¹

CHAMBRE DES DEPUTES

Session ordinaire 2012-2013

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**

* * *

AVIS DE LA CHAMBRE DE COMMERCE

(27.2.2013)

L'objet du projet de loi sous avis est de **renforcer la lutte contre la cybercriminalité**, c'est-à-dire les actes de délinquance commis à l'aide des nouvelles technologies, (i) en ratifiant la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 ainsi que son Protocole additionnel du 28 janvier 2003 relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques et (ii) en apportant les changements nécessaires à la législation luxembourgeoise pour la mettre en conformité avec la Convention et son Protocole additionnel.

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. Quant au Protocole additionnel, sa raison d'être 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.

*

CONSIDERATIONS GENERALES

La Chambre de Commerce salue 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, avec l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ainsi que son Protocole additionnel. Elle soutient en effet 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 internet.

La Chambre de Commerce rappelle à cette occasion la récente ouverture, le 11 janvier 2013, du Centre européen de lutte contre la cybercriminalité¹ – dont l’objectif est de renforcer la protection des entreprises dans l’Union européenne – qui atteste de la prise de conscience par les Etats de l’importance du phénomène que constitue la cybercriminalité et de la nécessité de le combattre à l’échelle internationale.

Plus généralement, la Chambre de Commerce relève que le projet de loi sous avis tend, à l’instar des projets de loi portant sur la possibilité de revendiquer des données informatiques en cas de faillite² et l’archivage électronique³, à renforcer le cadre législatif luxembourgeois de l’économie numérique et partant la crédibilité du Luxembourg dans ce secteur en pleine expansion.

Pour toutes ces raisons, et en dépit de la ratification tardive de la Convention et de son Protocole additionnel par le Luxembourg, la Chambre de Commerce ne peut que soutenir le présent projet de loi et saluer le travail des auteurs pour la pertinence des dispositions introduites dans la législation luxembourgeoise, en particulier sur les points suivants:

La cohérence du droit pénal est préservée grâce au choix des auteurs:

- de n’avoir pas opté pour une loi spécifique sur la cybercriminalité – au motif que la législation luxembourgeoise actuelle couvre la majeure partie des articles de la Convention – mais plutôt d’avoir procédé, dans le Code pénal et le Code d’instruction criminelle, à l’insertion des nouvelles infractions incriminées par la Convention⁴;
- d’avoir harmonisé le seuil minimal de la peine d’emprisonnement éventuellement encourue en cas d’infractions informatiques, en le relevant d’un à quatre mois.

La sécurité juridique est renforcée puisque:

- l’infraction d’*usurpation d’identité*, actuellement limitée au port public de faux nom patronymique, sera élargie 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 (certificat Luxtrust, matricule de sécurité sociale ...), ce qui devient indispensable notamment en matière de signature électronique;
- 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, sera à l’avenir appréhendée par le droit pénal. Cette nouvelle incrimination répond à un arrêt de la Cour d’appel du 14 juin 2010 qui avait considéré que dans sa rédaction actuelle, l’article 496 du Code pénal ne permettait pas de retenir l’escroquerie en cas d’hameçonnage d’un mot de passe;
- outre les nouvelles infractions précitées, seront insérées dans le Code pénal l’*interception ou tentative d’interception de données informatiques* (lors de transmissions non publiques à destination, en provenance ou à l’intérieur d’un système de traitement ou de transmission automatisé de données) ainsi que l’*abus de dispositif* (qui a pour but de prohiber la fabrication, la possession et la diffusion de programmes informatiques permettant de commettre des infractions pénales, ainsi que le trafic des mots de passe ou des codes d’accès).

La lutte contre le blanchiment et le financement du terrorisme est renforcée grâce au fait que les infractions informatiques sont érigées en infractions primaires:

- Alors qu’actuellement, certaines infractions informatiques génératrices de revenus importants échappent soit à toute poursuite – à défaut d’être incriminées – soit ne sont pas qualifiées d’infractions primaires et ne peuvent dès lors pas donner lieu à des poursuites au titre du blanchiment, il sera possible à l’avenir de poursuivre l’infraction de blanchiment en cas d’utilisation des revenus tirés des infractions informatiques.

¹ Site officiel: „www.europol.europa.eu/ec3“

² Projet de loi n° 6485 portant modification de l’article 567 du Code de commerce.

³ Projet de loi n° 6543 relatif à l’archivage électronique et modifiant la loi modifiée du 5 avril 1993 relative au secteur financier.

⁴ Concernant les dispositions contenues dans le Protocole additionnel, elles sont couvertes par les dispositions législatives actuellement en vigueur.

- Le projet de loi s’inscrit à cet égard 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, ce dont la Chambre de Commerce se félicite.

Le droit procédural se dote de véritables moyens de lutte contre les infractions informatiques puisque:

- le juge d’instruction pourra (i) procéder au repérage des données d’appel de moyens de télécommunication et de pouvoir localiser l’origine ou la destination de télécommunications sans qu’une instruction préparatoire ne soit ouverte; et (ii) enjoindre une personne ayant des connaissances particulières du système informatique ou du mécanisme de protection ou de cryptage, hormis celle visée par l’instruction, à lui donner accès aux données saisies (injonction de produire),
- les officiers de police judiciaire pourront (i) procéder à des perquisitions et saisies des données informatiques stockées en la possession des personnes incriminées; et (ii) faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, des données stockées, traitées ou transmises dans un système informatique lorsqu’il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

*

COMMENTAIRES DES ARTICLES

Concernant l’article 3

Sous le **point 5)** de l’article 3 du projet de loi qui modifie le point 1) de l’article 506-1 du Code pénal – relatif à l’infraction de blanchiment –, la Chambre de Commerce s’étonne qu’au dix-septième tiret, la référence à *l’article 143 de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et l’immigration* ait été ajoutée dans la mesure où cet article 143 a été abrogé par la loi du 21 juillet 2012 portant: 1) 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 le 15 novembre 2000, 2) modification du Code pénal, 3) modification du Code d’instruction criminelle, 4) modification de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et l’immigration.

Parallèlement, la Chambre de Commerce ne comprend pas pourquoi dans le nouvel article 506-1 du Code pénal proposé par le présent projet de loi, la référence aux *articles 382-4 et 382-5 du Code pénal* a été supprimée alors que ces deux articles ont été insérés par la loi du 21 juillet 2012 précitée, suite à l’abrogation de l’article 143 de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et l’immigration, pour former le „Chapitre VI-II. – Du trafic illicite des migrants“. Il convient partant de remédier à ces erreurs de renvoi.

Le **point 8)** de l’article 3 du projet de loi introduit un article 509-5 dans le Code pénal réprimant spécifiquement *la production, la vente, l’obtention, la détention, l’importation, la diffusion ou la mise à disposition de dispositif informatique permettant de commettre des infractions informatiques ou d’obtenir un mot de passe ou code d’accès*.

A la lecture du commentaire des articles, la Chambre de Commerce comprend que cette nouvelle disposition remplacera l’alinéa 2 à l’article 509-3 du Code pénal – corrélativement supprimé par le point 7) de l’article 3 du projet de loi – qui réprime *la fabrication, la réception, l’obtention, la détention, la vente ou la cession à des tiers des logiciels permettant de commettre des infractions informatiques*. Dans ce contexte, la Chambre de Commerce s’étonne, à défaut pour les auteurs d’en justifier les raisons, de l’abaissement de l’amende prévue à l’alinéa 2 à l’article 509-3 du Code pénal, actuellement de 1.250 euros à 30.000 euros, et de son remplacement par une amende de 251 euros à 5.000 euros seulement.

*

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

CTIE – Division Imprimés et Fournitures de bureau

6514/02

N° 6514²**CHAMBRE DES DEPUTES**

Session ordinaire 2012-2013

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**

* * *

AVIS DU CONSEIL D'ETAT

(16.4.2013)

Par dépêche du 12 décembre 2012, le Premier Ministre, Ministre d'Etat, a soumis à l'avis du Conseil d'Etat le projet de loi sous rubrique, élaboré par le ministre de la Justice. Le texte du projet était accompagné d'un exposé des motifs, d'un commentaire des articles, de même que d'une fiche d'évaluation d'impact. Etaient annexés le texte de la Convention du Conseil de l'Europe sur la cybercriminalité 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.

Par dépêche du 11 mars 2013, le Conseil d'Etat s'est vu communiquer l'avis de la Chambre de commerce.

*

CONSIDERATIONS GENERALES

Le projet de loi sous avis vise à approuver la Convention du Conseil de l'Europe sur la cybercriminalité et le Protocole additionnel, précités. En conséquence de l'approbation de ces instruments internationaux, une série de dispositions légales, notamment de droit pénal et de procédure pénale, doivent être adaptées. Les auteurs du projet de loi indiquent que dans un avenir très proche sera adoptée une directive de l'Union européenne en la matière et expliquent que cette directive sera „transposée avant la lettre dans le cadre du présent projet de loi“. Le Conseil d'Etat a déjà eu l'occasion de souligner 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, ce qui 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 directive, n'aurait pas été plus appropriée.

Le Conseil d'Etat relève par ailleurs 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 fût 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 regroupe les dispositions des articles 3 à 5 du projet.

*

EXAMEN DES ARTICLES

Articles 1er et 2

Ces articles portent approbation de la convention et du protocole additionnel précités. Ils n'appellent pas d'observation.

Article 3

L'article 3 porte modification de toute une série de dispositions du Code pénal. Le Conseil d'Etat relève d'emblée que la plupart de ces modifications ont une portée autonome et ne sont pas liées à l'approbation de la convention précitée. Il renvoie à l'observation qu'il a faite dans les considérations générales.

Point 1

Sous le point 1, il est proposé de compléter l'article 231 actuel du Code pénal sur l'usurpation de nom par une référence à une „identification de quelque nature qu'elle soit“. Les auteurs exposent qu'il résulte de la jurisprudence que l'article 231, dans sa teneur actuelle, ne permet pas de sanctionner l'usage de certificats type Luxtrust qui confèrent une identification d'une personne à une administration¹. Les auteurs exposent encore s'être inspirés de l'article 226-4-1 du Code pénal français figurant dans une section relative à „l'atteinte à la vie privée“.²

Le Conseil d'Etat note, d'abord, que le texte tel que proposé ne permet pas de rencontrer tous les problèmes visés dans le commentaire. En effet, l'utilisation d'une signature électronique, d'un certificat type Luxtrust ou d'un identifiant numérique dans des relations commerciales ou bancaires s'inscrit dans des rapports particuliers avec l'entité qui a décerné ou accepté l'identifiant; il ne s'agit toutefois pas de la prise publique illicite d'une identification dès lors que l'usage frauduleux s'inscrit dans des rapports particuliers. Le Conseil d'Etat note encore que ce type de comportement est souvent sanctionné par le biais de l'infraction de faux. Le seul cas de figure couvert, mais qui n'est pas visé dans le commentaire, est l'utilisation d'un matricule national d'autrui. Se pose, par ailleurs, la question de savoir si un identifiant, plus ou moins abstrait, qu'une personne s'est donné à elle-même, en particulier dans le secteur de l'Internet et qui ne revêt pas une fonction d'identification par un opérateur qui décerne ou accepte l'identifiant, est à protéger.

Le Conseil d'Etat relève de même le caractère vague des termes „identification de quelque nature que ce soit“. L'incrimination d'actes par le biais de formules aussi peu précises n'est à tout le moins pas heureuse. Si le texte, malgré les interrogations formulées ci-dessus, devait être maintenu, il y aurait lieu d'écrire „identifiant“ ou de reprendre la formulation du Code pénal français „données permettant d'identifier une autre personne“. Le Conseil d'Etat comprend que l'article 231**bis** nouveau, qui se réfère sans distinction au „tiers“, vise la protection des personnes physiques et morales. Qu'en est-il de l'usage injustifié ou frauduleux, de la dénomination ou de l'intitulé officiel d'organes publics qui ne constituent pas des personnes juridiques différentes de l'Etat ou d'une commune?

1 L'arrêt n° 125/07 de la Cour d'appel du 27 février 2007, que les auteurs n'ont pas communiqué au Conseil d'Etat, porte sur le problème très particulier d'un faux prénom et ne vise pas le problème des systèmes d'identification électronique.

2 Article 226-4-1 du Code pénal français:

„Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15.000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.“

Point 2

Les auteurs du projet proposent d'insérer dans le Code pénal un nouvel article 231*bis* incriminant l'usurpation d'un nom ou d'un identifiant en vue de nuire à autrui. C'est cette disposition, et non pas celle de l'article 231, 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. Il voudrait formuler deux observations. Pourquoi les auteurs n'ont-ils 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, qui porte sur les atteintes à l'honneur et à la considération des personnes.

Point 3

Le point 3 modifie les peines prévues à l'article 488 du Code pénal. Le Conseil d'Etat n'a pas d'observation particulière.

Point 4

Il est proposé de compléter l'article 496 du Code pénal par l'ajout, à la liste des objets remis ou délivrés, des clés électroniques. Les auteurs font état d'un arrêt de la Cour d'appel n° 261/10 X du 14 juin 2010 dont il résulterait que l'article 496, dans sa teneur actuelle, ne permet pas d'appréhender „l'hameçonnage d'un mot de passe (en anglais „phishing““.

Le Conseil d'Etat comprend le souci des auteurs du projet de trouver une réponse à un problème actuel récurrent. Il voudrait faire les observations suivantes. Il constate 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 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 électronique³ 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 clé électronique dans la définition des objets visés aux articles 461, 470 ou 491 du Code pénal.

Le Conseil d'Etat voudrait encore attirer 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 ceux 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 clé électronique et, au point 8 relatif au nouvel article 509-5, visent le „mot de passe“, le „code d'accès“ ou „toute autre clé électronique“. De deux choses l'une: ou bien le concept de clé électronique est le terme générique à consacrer, auquel cas il faudra adapter le texte du nouvel article 509-5 à celui de l'article 496; ou bien le concept de clé électronique est trop restreint, auquel cas il faudra reprendre, à l'article 496, tous les concepts de

³ Voir: arrêt de la Cour d'appel n° 154/04V du 11 mai 2004 qui exclut du domaine du vol les droits ou biens incorporels et arrêt de la Cour d'appel n° 57/08 V du 29 janvier 2008 qui assimile à la notion de „chose qui a, dans notre monde physique (réel) une présence matérielle, les données électroniques ou informatiques pouvant être enregistrées sous la forme d'impulsions dans des circuits électroniques ou sur des bandes magnétiques“ (Putz, Jurisprudence pénale, Tome 1, *verbo* chose mobilière, n° 9.1.1.1.).

l'article 509-5. Le Conseil d'Etat renvoie encore, dans ce contexte, à l'article 488 du Code pénal qui consacre déjà le concept de clé 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)“.

Point 5

Sous le point 5, il est prévu de compléter l'article 506-1 du Code pénal sur le blanchiment en ajoutant à la liste des infractions primaires une série d'infractions nouvelles en matière informatique. Le Conseil d'Etat relève le caractère extrêmement succinct du commentaire qui ne donne aucune indication des ajouts apportés à l'article 506-1; seule une lecture comparée du texte actuel avec l'article tel que modifié permet de mettre en évidence les compléments apportés au texte actuel de l'article 506-1. Le Conseil d'Etat relève encore que la plupart des ajouts ne concernent en rien les nouvelles infractions en matière informatique et que la volonté des auteurs semble plutôt être d'étendre la liste des infractions primaires en matière de blanchiment. Il renvoie à la proposition qu'il a faite dans les considérations générales du présent avis. Il rend par ailleurs attentif que le texte proposé ne tient pas compte des modifications que la loi du 21 juillet 2012 portant 1) 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. En effet, le troisième tiret du texte proposé omet de renvoyer aux articles 382-4 et 382-5 du Code pénal, et le dix-septième tiret 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. L'article 143 a d'ailleurs été abrogé par la loi précitée du 21 juillet 2012. La référence prévue au précédent treizième tiret dans sa formulation actuellement en vigueur peut d'ailleurs utilement être supprimée, alors qu'elle fait double emploi avec le troisième tiret, également introduit par la loi de 2012.

Point 6

Le point 6 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 note qu'au concept de données est ajouté le qualificatif „informatiques“ qui ne figure pourtant pas dans les autres articles de la section VII relative aux „infractions en matière électronique“. Le Conseil d'Etat s'interroge encore sur la nécessité de la partie finale de la disposition nouvelle „ou (système) de transmission automatisé de données“. Outre le problème que le terme de transmission est utilisé à deux reprises, une fois pour qualifier l'opération et une fois pour décrire le système, ce qui n'est pas très logique, le respect de l'article 3 de la Convention est, de l'avis du Conseil d'Etat, garanti même si ce bout de phrase est omis. Le Conseil d'Etat a constaté que l'article 3 de la Convention vise le système informatique en tant que tel sans distinguer entre l'aspect traitement et transmission, la transmission étant au demeurant également un traitement. Une solution plus simple encore serait de reprendre tel quel le texte de la Convention et de viser le système informatique. Enfin, le Conseil d'Etat relève que la tentative est spécialement prévue, alors que tel n'est pas le cas pour les dispositions actuelles qui ne subiront pas de changement. La Convention n'impose d'ailleurs pas expressément d'incriminer la tentative. Eu égard à ces observations, le Conseil d'Etat propose de reprendre le texte de l'article 3 de la Convention. L'alinéa 2 de l'article 509-3 du Code pénal aurait ainsi la teneur suivante:

„Est puni des mêmes peines l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.“

Point 7

La suppression de l'alinéa 2 de l'article 509-3 faisant l'objet du point 7 s'explique par le point 8.

Point 8

Le nouvel article 509-5 du Code pénal introduit au point 8 est destiné à transposer en droit national l'article 6 de la Convention. Le Conseil d'Etat voudrait faire quelques observations d'ordre rédaction-

nel. 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.

Article 4

L'article 4 porte modification de diverses dispositions du Code d'instruction criminelle.

Point 1

L'article 7-4 du Code d'instruction criminelle qui consacre le principe „*aut dedere aut iudicare*“ est complété par l'ajout des articles 509-1 à 509-7 du Code pénal sur les infractions en matière informatique.

D'un point de vue formel, le Conseil d'Etat relève que la note de bas de page n° 1, qui figure dans le texte qui lui a été transmis et qui renvoie au projet de loi n° 6388, est à omettre compte tenu de la loi du 26 décembre 2012 qui a modifié l'article 7-4⁴ (Mémorial A n° 290 du 31 décembre 2012).

Le Conseil d'Etat rend encore attentif au fait que l'article 7-4 du Code d'instruction criminelle actuellement en vigueur, tel que modifié en dernier lieu par la loi précitée du 26 décembre 2012, n'a pas été correctement repris. Aussi y a-t-il 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.“

Point 2

Les auteurs du projet de loi exposent que pour répondre 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 que le procureur d'Etat puisse demander au juge d'instruction d'ordonner les mesures prévues à l'article 67-1 du Code d'instruction criminelle sans ouvrir une instruction préparatoire.

Le Conseil d'Etat peut suivre les auteurs du projet de loi dans leur raisonnement. Il propose 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.

Point 3

L'article 31 du Code d'instruction criminelle relatif à la saisie en cas de flagrant crime est complété en vue de permettre la saisie de données informatiques. Le Conseil d'Etat approuve cette extension. Il voudrait formuler une observation de fond et une observation de forme.

4 Loi du 26 décembre 2012 portant approbation de la Convention du Conseil de l'Europe sur la prévention du terrorisme, signée à Varsovie, le 16 mai 2005, et modifiant

- le Code pénal;
- le Code d'instruction criminelle;
- la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne;
- la loi modifiée du 11 avril 1985 portant approbation de la Convention sur la protection physique des matières nucléaires, ouverte à la signature à Vienne et à New York en date du 3 mars 1980; et
- la loi modifiée du 14 avril 1992 instituant un code disciplinaire et pénal pour la marine.

Au 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 ou encore le nouvel article 509-5 du Code pénal, qui ont recours aux concepts de clé 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.

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, adoptant 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.

Point 4

Ce point vise à élargir l'objet de la perquisition prévue à l'article 33 du Code d'instruction criminelle aux données informatiques. Ce point est le corollaire du point 3 et le Conseil d'Etat renvoie à ses observations antérieures.

Le qualificatif „informatique“ est à adjoindre au concept de données qui est ajouté dans différents points du paragraphe 1er de l'article 33.

Le nouveau paragraphe 5 vise à permettre la saisie par voie d'établissement d'une copie. 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 a du mal à comprendre cette logique et s'interroge sur sa 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?

Point 5

Le point 5 vise à compléter la liste des infractions pour lesquelles une infiltration peut être décidée en incluant les infractions en matière informatique. Le Conseil d'Etat n'a pas d'observation 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.

Point 6

Les auteurs du projet de loi expliquent que, pour répondre 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 48-25 dans le Code d'instruction criminelle figurant sous un nouveau chapitre X intitulé „De la conservation rapide des données informatiques“.

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 ne peut pas apprécier, sur un plan technique, si les dispositions existantes sur la saisie et la perquisition, étendues aux données informatiques, ne permettraient 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.

Le Conseil d'Etat voudrait formuler les observations suivantes.

En ce qui concerne le fond, le Conseil d'Etat marque 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“. S'agissant d'une mesure grave dans le cadre d'une procédure d'enquête, d'instruction ou d'entraide judiciaire en matière pénale, la mesure doit être décidée ou ordonnée par un magistrat et ne saurait être avalisée après coup. Au regard de la disponibilité 24 heures sur 24 de magistrats du parquet et du cabinet d'instruction, on ne saurait avancer des considérations tenant à la perte de temps due à l'intervention des autorités judiciaires. Il y a donc lieu d'écrire „le procureur d'Etat ou le juge d'instruction ... peut faire procéder ...“.

En ce qui concerne la formulation du texte, le Conseil d'Etat renvoie à la suggestion déjà formulée de viser les données informatiques. Il propose, à la fin du texte, d'écrire „ces données“ plutôt que de reprendre la formule complexe qui figure déjà au début du libellé.

Point 7

L'article 66 du Code d'instruction criminelle est modifié pour étendre la saisie ordonnée par le juge d'instruction aux données informatiques. Les modifications proposées sont le corollaire de celles apportées à l'article 33. Le Conseil d'Etat renvoie à ses observations à l'endroit du point 4 y compris pour ce qui est du nouveau point 3 inséré dans l'article 66.

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. Les auteurs du projet n'expliquent pas les raisons qui les ont amenés à se limiter aux procédures de perquisition et de saisie.

Point 8

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 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 Code se suffit à elle-même et ne requiert aucune adaptation de l'article 67-1. Il s'agit d'une procédure spécifique permettant justement l'adoption des mesures prévues à l'article 67-1 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, 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, 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 sans qu'il ne faille introduire un renvoi à cette disposition à l'article 67-1. Le Conseil d'Etat reconnaît que se pose la question de l'information de la personne 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 à la suite des modifications proposées au point 2.

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.“

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 que les auteurs négligent d'indiquer le paragraphe 1er en début du texte de l'article 67-1 nouveau 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.

Article 5

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 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'observation.

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'observation.

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'observation.

Le Conseil d'Etat voudrait néanmoins faire 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 ...“.

La référence expresse aux articles 88-1 et 88-4 peut être maintenue, parce qu’il ne s’agit pas de dispositions relatives à l’enquête préliminaire ou à la procédure d’instruction.

Ainsi délibéré en séance plénière, le 16 avril 2013.

Le Secrétaire général,
Marc BESCH

Le Président,
Victor GILLEN

CTIE – Division Imprimés et Fournitures de bureau

6514/03

N° 6514³

CHAMBRE DES DEPUTES

Session ordinaire 2012-2013

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

* * *

SOMMAIRE:

<i>Amendements adoptés par la Commission juridique</i>	<i>page</i>
1) Dépêche du Président de la Chambre des Députés au Président du Conseil d'Etat (7.6.2013).....	1
2) Texte coordonné.....	12

*

**DEPECHE DU PRESIDENT DE LA CHAMBRE DES DEPUTES
AU PRESIDENT DU CONSEIL D'ETAT**

(7.6.2013)

Monsieur le Président,

J'ai l'honneur de vous faire parvenir une série d'amendements au projet de loi mentionné sous rubrique, adoptés par la Commission juridique en date du 5 juin 2013.

Je joins en annexe, à toutes fins utiles, un texte coordonné du projet de loi sous rubrique reprenant les amendements proposés (figurant en caractères gras soulignés) et les propositions de texte du Conseil d'Etat que la commission a reprises (figurant en caractères soulignés).

Amendement 1

Il est proposé de supprimer le point 1) à l'article 3 du projet de loi.

Commentaire:

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'aligner ce dernier à la jurisprudence des juridictions luxembourgeoises qui interprètent la notion de „public“ de manière très large.

Les réserves du Conseil d'Etat étant partagées par les membres de la Commission juridique et cette modification n'étant pas impérative dans le cadre de la ratification de la Convention et de son Protocole, il est proposé de supprimer 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.

Amendement 2

Il est proposé d'ajouter à l'article 3 un point 2) nouveau, libellé comme suit:

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.“

Commentaire:

Le Conseil d'Etat dans son avis du 16 avril 2013 relève 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 clé électronique dans la définition des objets visés à l'article 461 du Code pénal.

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

Amendement 3

Il est proposé d'ajouter à l'article 3 un point 3) nouveau libellé comme suit:

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 électroniques, 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.“

Commentaire:

Le Conseil d'Etat dans son avis du 16 avril 2013 relève une divergence qui existerait désormais entre l'infraction d'escroquerie (article 496 du Code pénal) où l'on a rajouté la notion de clé 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 clé électronique dans la définition des objets visés à l'article 470 du Code pénal.

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

Amendement 4

Il est proposé de renuméroter le point 3) initial de l'article 3 en point 4) et de le modifier comme suit:

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 251 euros à 1.250 euros à 5.000 30.000 euros“.

Commentaire:

Le seuil de peine de l'article 488 du Code pénal doit être adapté au seuil de peine prévu au nouvel article 509-5 du Code pénal tel que proposé dans le présent projet de loi 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 de 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.

Or, le seuil de peine du nouvel article 509-5 est relevé à l'amendement 11 du présent document 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, et de son remplacement par une amende de 251 euros à 5.000 euros seulement.

En ce qui concerne la renumérotation de l'article, il s'agit d'une simple adaptation de forme pour préserver la cohérence de la numérotation des différents articles du projet de loi.

Amendement 5

Il est proposé d'ajouter à l'article 3 un point 5) nouveau libellé comme suit:

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.“

Commentaire:

Le Conseil d'Etat, dans son avis du 16 avril 2013, relève une divergence qui existerait désormais entre l'infraction d'escroquerie (article 496 du Code pénal) où l'on a rajouté la notion de clé 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 clé électronique dans la définition des objets visés à l'article 491 du Code pénal.

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

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

Amendement 6

Il est proposé de renuméroter le point 5) de l'article 3 en point 7) et de le modifier comme suit:

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 **et**, 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 à l’article 143 de la loi du 29 août portant sur la libre circulation des personnes et l’immigration;~~
- 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;“

Commentaire:

Le Conseil d’Etat dans son avis du 16 avril 2013 relève que le texte proposé relatif à l’article 506-1 point 1) ne tient pas compte des modifications que la loi du 21 juillet 2012 portant 1) 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 omet de renvoyer aux articles 382-4 et 382-5 du Code pénal, et que le dix-septième tiret 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 a été abrogé par la loi précitée du 21 juillet 2012 et propose que la référence prévue au précédent 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.

C’est pourquoi il est proposé de modifier le texte conformément aux propositions du Conseil d’Etat.

Amendement 7

Il est proposé de renuméroter le point 6) de l'article 3 en point 8) et de le modifier comme suit:

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 ~~ou tenté d'intercepter~~ des données informatiques lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données.“

Commentaire:

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 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.

Il est proposé d'enlever la tentative du nouvel alinéa 2 de l'article 509-3 conformément à la proposition du Conseil d'Etat.

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 de la section VII du chapitre II du titre IX du livre II du Code pénal, dont relève l'article 509-3, 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.

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“.

Amendement 8

Il est proposé de renuméroter le point 8) de l'article 3 en point 10) et de le modifier comme suit:

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 ~~251 1.250 euros à 5.000 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
- ~~un mot de passe, 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.“

Commentaire:

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.

Conformément aux souhaits du Conseil d'Etat 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 incor-

poration 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, 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.

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 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 anti-virus).

Amendement 9

Il est proposé de modifier le point 3) de l'article 4 comme suit:

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 **informatique 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.“

Commentaire:

Il est proposé 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 la communication).

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

Amendement 10

Il est proposé de modifier le point 4) de l'article 4 comme suit:

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 **informatique 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 der-

nières 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 **informatique 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 **informatique 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 laissé 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."

Commentaire:

Il est proposé 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 la communication).

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

Amendement 11

Il est proposé de modifier le point 6) de l'article 4 comme suit:

- 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 **informatique de traitement ou de transmission automatisé de données**, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, ~~l'officier de police judiciaire, de l'accord du~~ le Procureur d'Etat ou ~~du~~ le juge d'instruction saisi, peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, **des ces données stockées, traitées ou transmises dans un système informatique.**

Commentaire:

Il est proposé 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 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“.

Il est proposé de suivre 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“.

Amendement 12

Il est proposé de modifier le point 7) de l'article 4 comme suit:

- 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 **informatique 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 **informatique 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 **informatique 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 **informatique 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“.

Commentaire:

Il est proposé 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 la communication).

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

Amendement 13

Il est proposé de modifier le point 8) de l'article 4 comme suit:

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

„(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, 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, si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.

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) (~~L. 12 août 2003~~) 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 ou 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. 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 135-13 135-4** 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, ou à l'article 24-1 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 ou de l'enquête préliminaire et détruites dans la mesure où elles concernent des personnes non visées par l'instruction ou l'enquête préliminaire.“

Commentaire:

Dans son avis du 16 avril 2013 le Conseil d'Etat indique que le paragraphe 1er en début de texte de l'article 67-1 nouveau du Code d'instruction criminelle n'est pas indiqué et qu'au paragraphe 3 du même article la référence à une loi du 12 août 2003 est à omettre.

Il est proposé de suivre les propositions du Conseil d'Etat.

Au paragraphe (3) il est proposé 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 de maintenir le texte du projet de loi.

En effet à défaut de supprimer les termes „saisi de faits“ dans la première phrase du paragraphe 1er de l'article 67-1, celui-ci est en contradiction avec l'article 24-1 alors que ce dernier renvoie à l'article 67-1.

Dans la mesure où l'article 24-1 renvoie à l'article 67-1, la solution la plus simple est d'ajouter l'enquête préliminaire au paragraphe 3 de l'article 67-1. En effet, l'article 67-1 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. 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, il est confirmé 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.

Amendement 14

Il est proposé de modifier l'article 5 comme suit:

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 ~~au titre des articles 48-25 et 67-1 du Code d'instruction criminelle 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 ~~au titre des articles 48-25 et 67-1 du Code d'instruction criminelle 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 sauvegar-

der 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 **au titre des articles 48-25 et 67-1 du Code d'instruction criminelle 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).“

Commentaire:

Le Conseil d'Etat dans son avis du 16 avril 2013 remarque que la référence à des articles particuliers du Code d'instruction criminelle entraîne l'obligation de revoir la loi de 2005 lors de chaque modification du contenu ou de la numérotation du Code d'instruction criminelle.

Il préconise une formule plus générale qu'il est proposé de retenir en la modifiant très légèrement en parlant de „autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi“ au lieu de „autorités judiciaires agissant dans le cadre des compétences prévues au Code d'instruction criminelle“.

*

Compte tenu de l'urgence du présent projet de loi, qui doit idéalement être voté avant les vacances d'été, je vous saurais gré, Monsieur le Président, si le Conseil d'Etat pouvait émettre son avis complémentaire dans les meilleurs délais.

J'envoie copie de la présente, pour information, au Premier Ministre, Ministre d'Etat, à la Ministre de la Justice et au Ministre aux Relations avec le Parlement.

Veillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

Le Président de la Chambre des Députés,
Laurent MOSAR

*

TEXTE COORDONNE

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 231bis du Code pénal libellé comme suit:

„**Art. 231bis.**– 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 électroniques, 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 ~~251 euros~~ **1.250 euros à 5.000 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 ~~et~~, 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 à l'article 143 de la loi du 29 août portant sur la libre circulation des personnes et l'immigration;~~
 - 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 **ou tenté d’intercepter** des données **informatiques** 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 **251 1.250 euros à 5.000 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
- ~~un mot de passe, 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.“

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, 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.“

2) Le point (1) 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 à l’article 67-1 et sans qu’une instruction préparatoire ne soit ouverte.“

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 **informatique 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 **informatique 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 désemperer 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 **informatique 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 **informatique 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 laissé 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:

„12. enlèvement de mineurs au sens des articles 368 à 371-1 du Code pénal,

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 **informatique de traitement ou de transmission automatisé de données**, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, ~~l'officier de police judiciaire, de l'accord du~~ le Procureur d'Etat ou ~~du~~ le juge d'instruction saisi, peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, ~~des ces~~ **données stockées, traitées ou transmises dans un système informatique**.“

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 **informatique 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 **informatique 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 **informatique 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 **informatique 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:

„(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, 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, si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.

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) (L. 12 août 2003) 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 ou 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. 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 135-13 135-4** 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, ou à l'article 24-1 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 ou de l'enquête préliminaire et détruites dans la mesure où elles concernent des personnes non visées par l'instruction ou l'enquête préliminaire.“

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 **au titre des articles 48-25 et 67-1 du Code d'instruction criminelle 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 **au titre des articles 48-25 et 67-1 du Code d'instruction criminelle 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 **au titre des articles 48-25 et 67-1 du Code d'instruction criminelle 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).“

CTIE – Division Imprimés et Fournitures de bureau

6514/04

N° 6514⁴**CHAMBRE DES DEPUTES**

Session extraordinaire 2013

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**

* * *

AVIS COMPLEMENTAIRE DU CONSEIL D'ETAT

(12.11.2013)

Par dépêche du 7 juin 2013, le Président de la Chambre des députés a saisi le Conseil d'Etat d'une série d'amendements au projet de loi sous rubrique, adoptés par la Commission juridique.

Au texte des amendements étaient joints un commentaire et un texte coordonné du projet de loi ainsi amendé.

Amendement 1

Sans observation.

Amendement 2

La Commission juridique propose de maintenir l'ajout du concept de clef électronique à l'article 496 du Code pénal sur l'escroquerie et de compléter, dans un souci de cohérence, l'article 461 relatif au vol par un ajout parallèle. Malgré la préférence que le Conseil d'Etat avait exprimée en faveur d'une approche nouvelle consacrant le concept de bien incorporel, il peut marquer son accord avec l'amendement.

Amendement 3

Dans la suite logique de l'amendement précédent, il est proposé de compléter l'article 470 du Code pénal sur l'extorsion par une référence au concept de clef électronique. Le Conseil d'Etat marque son accord avec cet amendement.

Amendement 4

Sans observation.

Amendement 5

Dans la suite logique des amendements 2 et 3, l'amendement sous examen vise à compléter l'article 491 du Code pénal sur l'abus de confiance par une référence au concept de clef électronique. Le Conseil d'Etat marque son accord avec cet amendement.

Amendement 6

Sans observation.

Amendement 7

L'amendement suit, en partie, les suggestions émises par le Conseil d'Etat dans son avis du 16 avril 2013 et n'appelle pas d'observations nouvelles par rapport à celles formulées dans cet avis.

Amendement 8

L'amendement reprend, encore, certaines suggestions émises par le Conseil d'Etat dans son avis du 16 avril 2013 et n'appelle pas d'observations nouvelles par rapport à celles formulées dans cet avis.

Amendement 9

Le Conseil d'Etat a pris acte des considérations des auteurs des amendements qui renvoient la question d'une consécration éventuelle, dans les dispositions du Code pénal relatives aux crimes et délits contre les propriétés, du concept de bien incorporel à une discussion future plus générale sur la réforme du Code pénal. Il se permet toutefois de réitérer ses interrogations quant à la cohérence du système répressif, en rappelant l'observation qu'il avait faite dans son avis du 16 avril 2013 concernant l'incohérence d'ordre conceptuel entre la modification envisagée à l'endroit de l'article 31 du Code d'instruction criminelle permettant la saisie et la perquisition de données informatiques et celles proposées concernant les articles 496 et 509-5 du Code pénal, visant les concepts différents de clef électronique, de mot de passe ou de code d'accès.

Pour le surplus, le Conseil d'Etat peut suivre les auteurs des amendements dans leur volonté d'assurer une cohérence d'ordre terminologique entre les différentes dispositions.

Amendement 10

Le Conseil d'Etat renvoie à ses considérations à l'endroit de l'amendement précédent.

Amendement 11

Le Conseil d'Etat peut encore suivre les auteurs des amendements dans leur volonté d'assurer une cohérence d'ordre terminologique entre les différentes dispositions.

Amendement 12

Le Conseil d'Etat renvoie à ses observations précédentes.

Amendement 13

Le Conseil d'Etat a des difficultés à suivre l'argumentaire des auteurs de l'amendement. 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 n'exigeait aucune modification. 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. 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.

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, 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.

Amendement 14

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.

Ainsi délibéré en séance plénière, le 12 novembre 2013.

Le Secrétaire général,
Marc BESCH

Le Président,
Victor GILLEN

CTIE – Division Imprimés et Fournitures de bureau

6514/05

N° 6514⁵

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

* * *

SOMMAIRE:

	<i>page</i>
<i>Amendements adoptés par la Commission juridique</i>	
1) Dépêche du Président de la Chambre des Députés au Président du Conseil d'Etat (20.3.2014).....	1
2) Texte coordonné.....	4

*

**DEPECHE DU PRESIDENT DE LA CHAMBRE DES DEPUTES
AU PRESIDENT DU CONSEIL D'ETAT**

(20.3.2014)

Monsieur le Président,

J'ai l'honneur de vous faire parvenir une série d'amendements au projet de loi mentionné sous rubrique, adoptés par la Commission juridique en date du 19 mars 2014.

Je joins en annexe, à toutes fins utiles, un texte coordonné du projet de loi sous rubrique reprenant les amendements proposés (figurant en caractères gras soulignés) et les propositions de texte du Conseil d'Etat que la commission a reprises (figurant en caractères soulignés).

Amendement n° 1 – Article 4, point 2) du projet de loi (modification de l'article 24-1, paragraphe (1) du Code d'instruction criminelle)

Il est proposé de modifier le point 2) de l'article 4 du projet de loi n° 6514 comme suit:

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

„Pour les infractions visées à l'alinéa qui précède ou si les faits 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:

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, conformément à l'article 67-1 et 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.

Commentaire

Deux nouveaux paragraphes sont rajoutés par rapport au projet de loi initial et l'article 24-1 du Code d'Instruction criminelle (ci-après CIC) renvoie désormais directement à l'article 67-1 du même Code.

Cependant, le renvoi est uniquement fait aux paragraphes 1 et 2 de l'article 67-1 du CIC et le paragraphe 3 de ce même article est repris en substance dans l'article 24-1 du CIC lui-même, tel que proposé par le Conseil d'Etat dans son avis complémentaire du 12 novembre 2013.

Un tel renvoi limité est nécessaire pour 2 raisons : 1) Il ne faut pas faire double emploi, c'est-à-dire renvoyer à l'article 67-1 du CIC en entier et recopier en substance une partie de ce même article dans l'article 24-1. 2) Il faut éviter de renvoyer de l'article 24-1 du CIC à „l'instruction“, aucune instruction n'étant ouverte dans le cas de l'article 24-1 du CIC.

La crainte du parquet est la même à ce sujet que pour la „saisine in rem“ ci-dessous c.-à-d. qu'un juge d'instruction puisse interpréter un renvoi „illimité“ à l'article 67-1 du CIC comme contradictoire à l'article 24-1 du CIC.

Amendement n° 2 – Article 4, point 8) du projet de loi (article 67-1 du Code d'instruction criminelle)

Il est proposé de modifier le point 8) de l'article 4 du projet de loi n° 6514 comme suit:

L'article 67-1 du Code d'instruction criminel est modifié comme suit:

„Art. 67-1. (1) Lorsque le juge d'instruction saisi de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, 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, **si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.**

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 ou 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. 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 135-13 135-4 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, ou à l'article 24-1 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."

Commentaire

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 CIC 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 n'est pas donnée dans le cadre de l'article 24-1 du CIC et donc si l'article 24-1 du CIC renvoie dorénavant à l'article 67-1 du CIC (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 sinon certains juges risquent de ne pas appliquer l'article 24-1 du CIC en combinaison avec l'article 67-1 CIC parce qu'ils les estimeront contradictoires.

Les ajoutes au paragraphe 3 „ou de l'enquête préliminaire“ et „ou à l'article 24-1 du Code d'instruction criminel“ prévues 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 CIC.

*

Au nom de la Commission juridique, je vous saurais gré de bien vouloir faire aviser dans les meilleurs délais par le Conseil d'Etat les amendements exposés ci-avant.

J'envoie copie de la présente, pour information, au Premier Ministre, Ministre d'Etat, au Ministre de la Justice et au Ministre aux Relations avec le Parlement.

J'envoie copie de la présente, pour information, au Premier Ministre, Ministre d'Etat avec prière de transmettre les amendements parlementaires ci-avant à la Chambre de Commerce, et au Ministre de la Justice ainsi qu'au Ministre aux Relations avec le Parlement.

Veuillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

Le Président de la Chambre des Députés,
Mars DI BARTOLOMEO

*

TEXTE COORDONNE

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

Visualisation des modifications textuelles:

- (i) caractères **gras** et soulignés pour l'amendement parlementaire;
- (ii) caractères soulignés pour les rectifications techniques légistiques

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 231bis du Code pénal libellé comme suit:

„**Art. 231bis.**– 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 électroniques, 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 (1) de l’article 24-1 du Code d’instruction criminelle est complété comme suit:
- „Pour les infractions visées à l’alinéa qui précède **ou si les faits 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:**
- 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, conformément à l’article 67-1 et 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 laissé 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:

„12. enlèvement de mineurs au sens des articles 368 à 371-1 du Code pénal,

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 saisi de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, 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, **si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.**

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 ou 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. 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 ~~135-4~~ 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, ou à l'article 24-1 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).“

CTIE – Division Imprimés et Fournitures de bureau

6514/06

N° 6514⁶**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**

* * *

**DEUXIEME AVIS COMPLEMENTAIRE
DU CONSEIL D'ETAT**

(4.4.2014)

Par dépêche du 20 mars 2014, le Président de la Chambre des Députés a saisi le Conseil d'Etat d'une série d'amendements au projet de loi sous rubrique, adoptés par la Commission juridique en date du 19 mars 2014.

Amendement 1er

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*“.

Amendement 2

Le Conseil d'Etat 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 vise, sans discussion aucune, les compétences propres du juge d'instruction. Pour pouvoir agir, au titre de l'article 67-1, 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 et précise qu'une instruction préparatoire n'est pas ouverte. La modification de

l'article 67-1 retenue par l'amendement est encore le résultat d'un mélange non justifié entre les deux dispositions.

Ainsi délibéré en séance plénière, le 4 avril 2014.

Le Secrétaire général,
Marc BESCH

Le Président,
Victor GILLEN

6514/07

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 LORSCHKE, 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 4^{ème} 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 remplies 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 détenteurs 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

6514

Bulletin de Vote (Vote Public)

Page 1/2

Date: 04/06/2014 15:48:58
 Scrutin: 2
 Vote: PL 6514 Cybercriminalité
 Description: Projet de loi 6514

Président: M. Di Bartolomeo Mars
 Secrétaire A: M. Frieseisen Claude
 Secrétaire B: Mme Barra Isabelle

	Oui	Abst	Non	Total
Présents:	56	0	2	58
Procuration:	2	0	0	2
Total:	58	0	2	60

Nom du député	Vote	(Procuration)	Nom du député	Vote	(Procuration)
déi gréng					
M. Adam Claude	Oui		Mme Lorsché Josée	Oui	
Mme Loschetter Viviane	Oui		M. Traversini Roberto	Oui	
Mme Wickler Christiane	Oui		M. Kaes Henri	Oui	

CSV					
Mme Adehm Diane	Oui		Mme Andrich-Duval Sylv	Oui	
Mme Arendt Nancy	Oui		M. Eicher Emile	Oui	
M. Eischen Félix	Oui		M. Frieden Luc	Oui	
M. Gloden Léon	Oui		M. Halsdorf Jean-Marie	Oui	
Mme Hansen_ Martine	Oui		Mme Hetto-Gaasch Franç	Oui	
M. Juncker Jean-Claude	Oui		M. Kaes Aly	Oui	
M. Lies Marc	Oui		M. Meyers Paul-Henri	Oui	
Mme Modert Octavie	Oui		M. Mosar Laurent	Oui	
M. Oberweis Marcel	Oui		M. Roth Gilles	Oui	
M. Schank Marco	Oui		M. Spautz Marc	Oui	
M. Wilmes Serge	Oui		M. Wiseler Claude	Oui	
M. Wolter Michel	Oui	(Mme Arendt Nancy)			

LSAP					
M. Angel Marc	Oui		M. Arndt Fränk	Oui	
M. Bodry Alex	Oui		Mme Bofferding Taina	Oui	
Mme Burton Tess	Oui		M. Cruchten Yves	Oui	
Mme Dall'Agnol Claudia	Oui		M. Di Bartolomeo Mars	Oui	
M. Engel Georges	Oui		M. Fayot Franz	Oui	
M. Haagen Claude	Oui		Mme Hemmen Cécile	Oui	
M. Negri Roger	Oui				

DP					
M. Arendt Guy	Oui		M. Bauler André	Oui	
M. Baum Gilles	Oui		Mme Beissel Simone	Oui	
M. Berger Eugène	Oui		Mme Brasseur Anne	Oui	
M. Delles Lex	Oui		Mme Elvinger Joëlle	Oui	
M. Graas Gusty	Oui		M. Hahn Max	Oui	
M. Krieps Alexander	Oui		M. Mertens Edy	Oui	
Mme Polfer Lydie	Oui				

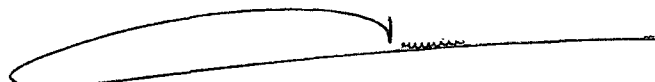
ADR					
M. Gibéryen Gast	Oui	(M. Kartheiser Fernan)	M. Kartheiser Fernand	Oui	
M. Reding Roy	Oui				

déi Lénk					
M. Turpel Justin	Non		M. Urbany Serge	Non	

Le Président:



Le Secrétaire général:



Bulletin de Vote (Vote Public)

Page 2/2


Date: 04/06/2014 15:48:58	Président: M. Di Bartolomeo Mars
Scrutin: 2	Secrétaire A: M. Frieseisen Claude
Vote: PL 6514 Cybercriminalité	Secrétaire B: Mme Barra Isabelle
Description: Projet de loi 6514	

	Oui	Abst	Non	Total
Présents:	56	0	2	58
Procuration:	2	0	0	2
Total:	58	0	2	60

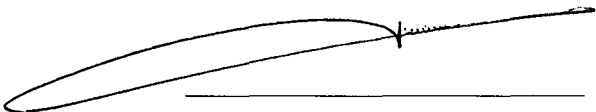
n'ont pas participé au vote:

Nom du député	Nom du député
M. Kox Henri	déi gréng

Le Président:



Le Secrétaire général:



6514/08

N° 6514⁸**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

* * *

**DISPENSE DU SECOND VOTE CONSTITUTIONNEL
PAR LE CONSEIL D'ETAT**

(24.6.2014)

Le Conseil d'Etat,

appelé par dépêche du Premier Ministre, Ministre d'Etat, du 6 juin 2014 à délibérer sur la question de dispense du second vote constitutionnel du

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

qui a été adopté par la Chambre des députés dans sa séance du 4 juin 2014 et dispensé du second vote constitutionnel;

Vu ledit projet de loi et les avis émis par le Conseil d'Etat en ses séances des 16 avril 2013 et 12 novembre 2013 et 4 avril 2014;

se déclare d'accord

avec la Chambre des députés pour dispenser le projet de loi en question du second vote prévu par l'article 59 de la Constitution.

Ainsi décidé en séance publique du 24 juin 2014.

Le Secrétaire général,
Marc BESCH

Le Président,
Victor GILLEN



Commission juridique

Procès-verbal de la réunion du 28 mai 2014

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 21 mai 2014
2. 6514 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- Rapporteur: Monsieur Guy Arendt
- Présentation et adoption d'un projet de rapport
3. 6172A Projet de loi portant
 - a) réforme du Titre II.- du Livre Ier du Code civil "Des actes de l'état civil" et modifiant les articles 34, 47, 57, 63, 70, 71, 73, 75, 76, 79, 79-1 et 95;
 - b) réforme du Titre V.- du Livre Ier du Code civil "Du mariage", rétablissant l'article 143, modifiant les articles 144, 145, 147, 148, 161 à 164, 165 à 171, 173 à 175, 176, 177, 179, 180 à 192, 194 à 199, 201, 202, 203 à 206, 212 à 224, 226, 227, introduisant les articles 146-1, 146-2, 175-1, 175-2 nouveaux et abrogeant les articles 149 à 154, 158 à 160bis, 178, le Chapitre VIII et l'article 228.
 - c) modification des articles 295, 351, 379, 380, 383, 390, 412, 496 alinéa 1er, 509-1 alinéa 2, 730, 737, 791, 847 à 849, 852 alinéa 3, 980 alinéa 2, 1405, 1409 et 1676 alinéa 2 et abrogation des articles 296, 297 et 1595 du Code civil;
 - d) modification de l'article 66 du Code de commerce ;
 - e) modification des articles 265 alinéa 1er, 278 et 521 du Nouveau Code de procédure civile ;
 - f) introduction d'un Titre VI.bis nouveau dans la Deuxième Partie du Nouveau Code de procédure civile;
 - g) introduction d'un Chapitre VII.-I nouveau au Titre VII du Livre Ier du Code pénal;

- h) abrogation de la loi du 23 avril 1827 concernant la dispense des prohibitions du mariage prévues par les articles 162 à 164 du Code civil; et
 - i) abrogation de la loi du 19 décembre 1972 portant introduction d'un examen médical avant mariage
- Rapporteur: Monsieur Paul-Henri Meyers
 - Présentation et adoption d'un projet de rapport

4. Divers

*

Présents : M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Alex Bodry, M. Franz Fayot, Mme Martine Hansen remplaçant M. Léon Gloden, Mme Josée Lorsché, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Octavie Modert, M. Laurent Mosar, M. Roy Reding, M. Gilles Roth

M. Felix Braz, Ministre de la Justice

Mme Jeannine Dennewald, M. Laurent Thyès, du Ministère de la Justice

M. Laurent Besch, de l'Administration parlementaire
Mme Tania Sonnetti, de l'Administration parlementaire

Excusés : M. Léon Gloden, Mme Lydie Polfer

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission

*

1. **Approbation du projet de procès-verbal de la réunion du 21 mai 2014**

Le projet de procès-verbal sous référence recueille l'accord unanime des membres de la commission.

2. **6514 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

Présentation du projet de rapport

M. le Rapporteur présente succinctement son projet de rapport.

Echange de vues

- ❖ Mme la Présidente précise, eu égard aux arrêts de la Cour de Justice de l'Union européenne dans l'affaire C-293/12 et C-594/12 *Digital Rights Ireland et Seitlinger e.a.* du 8 avril 2014 (invalidation de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006) et dans l'affaire C-131/12 Google Spain SL, Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González du 13 mai 2014 (droit à l'oubli numérique), rappelle la décision de principe de la Commission juridique de convoquer une réunion jointe avec la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace.

La date exacte de la réunion (un mercredi matin) sera communiquée en temps utile aux membres des deux commissions.

De même, eu égard à la demande du groupe politique CSV du 14 mai 2014 d'organiser une réunion en présence de M. le Président de la Commission nationale pour la protection des données (CNPD), une réunion en ce sens sera organisée.

- ❖ M. le Ministre de la Justice informe qu'à l'ordre des jour des prochaines réunions des 5 et 6 juin 2014 du Conseil JAI ayant lieu au Luxembourg figurera l'examen des deux arrêts précités de la Cour de Justice de l'Union européenne.

L'orateur explique qu'il est en train de définir ensemble avec les acteurs institutionnels concernés une position du Gouvernement luxembourgeois.

Il estime que le point relatif à une nouvelle initiative européenne dans le domaine de la protection des données à caractère personnel devient un sujet à traiter dans le cadre de la présidence luxembourgeoise de l'Union européenne (2^e semestre 2015).

Vote

Le projet de rapport recueille l'accord unanime des membres de la commission.

Temps de parole

Les membres de la commission proposent le modèle n°1 pour le débat en séance publique.

3. 6172A **Projet de loi portant** **a) réforme du Titre II.- du Livre I^{er} du Code civil "Des actes de l'état civil" et**

- modifiant les articles 34, 47, 57, 63, 70, 71, 73, 75, 76, 79, 79-1 et 95;
- b) réforme du Titre V.- du Livre Ier du Code civil "Du mariage", rétablissant l'article 143, modifiant les articles 144, 145, 147, 148, 161 à 164, 165 à 171, 173 à 175, 176, 177, 179, 180 à 192, 194 à 199, 201, 202, 203 à 206, 212 à 224, 226, 227, introduisant les articles 146-1, 146-2, 175-1, 175-2 nouveaux et abrogeant les articles 149 à 154, 158 à 160bis, 178, le Chapitre VIII et l'article 228.
- c) modification des articles 295, 351, 379, 380, 383, 390, 412, 496 alinéa 1er, 509-1 alinéa 2, 730, 737, 791, 847 à 849, 852 alinéa 3, 980 alinéa 2, 1405, 1409 et 1676 alinéa 2 et abrogation des articles 296, 297 et 1595 du Code civil;
- d) modification de l'article 66 du Code de commerce ;
- e) modification des articles 265 alinéa 1er, 278 et 521 du Nouveau Code de procédure civile ;
- f) introduction d'un Titre VI.bis nouveau dans la Deuxième Partie du Nouveau Code de procédure civile;
- g) introduction d'un Chapitre VII.-I nouveau au Titre VII du Livre Ier du Code pénal;
- h) abrogation de la loi du 23 avril 1827 concernant la dispense des prohibitions du mariage prévues par les articles 162 à 164 du Code civil; et
- i) abrogation de la loi du 19 décembre 1972 portant introduction d'un examen médical avant mariage

Présentation du projet de rapport

M. le Rapporteur présente succinctement son projet de rapport.

Echange de vues

- ❖ Un membre du groupe politique LSAP, tout en soulignant que le projet de rapport résume de manière objective et exhaustive les travaux de la commission, estime qu'il ne comporte pas de développements au sujet de la position politique de la Commission juridique.
- ❖ M. le Ministre de la Justice, quant au nombre des adoptions nationales et internationales et aux pays autorisant les adoptions internationales (informations demandées lors de la réunion de la commission du 21 mai 2014;), précise qu'on observe pour l'adoption internationale, depuis 2013, une tendance au rétrécissement du nombre de pays autorisant l'adoption (cf. document figurant en annexe au présent procès-verbal) d'un enfant résidant sur son territoire. De même et de manière concomitante, le nombre des dépôts de candidatures à l'adoption en Europe est en progression constante. On assiste ainsi à un allongement des délais de procédures (de deux à trois ans).

Ainsi, le nombre des adoptions nationales varie entre 1 à 3 par an. Pour l'adoption internationale, le chiffre est de quatre pour 2013.

Actuellement (depuis 2013), pour le Luxembourg, quatre pays restent ouverts pour recevoir des candidatures à l'adoption, à savoir l'Afrique du Sud, la Bulgarie, la Corée du Sud et l'Inde. De ces quatre pays, seule l'Afrique du Sud accepte des dossiers émanant d'un couple composé de deux personnes de même sexe.

En ce qui concerne les adoptions internationales, la procédure judiciaire diffère en fonction de la mise en vigueur ou non de la Convention de la Haye du 29 mai 1993 (ratifiée par le Luxembourg par la loi du 14 avril 2002) dans le pays d'origine.

Ladite Convention instaure un système de coopération entre les Etats signataires afin d'assurer le respect de garanties. L'Etat d'origine de l'enfant à adopter a la faculté de déterminer des conditions préalables devant être remplies pour que jugement d'adoption puisse être prononcé (le jugement d'adoption est prononcé par une juridiction du pays d'origine de l'enfant adopté et reconnu au Luxembourg et transcrit au registre de l'état civil de la Ville de Luxembourg). Ainsi, un Etat peut refuser l'adoption si les adoptants constituent un couple de deux personnes de même sexe.

- ❖ M. le Rapporteur explique que chaque dossier d'adoption internationale (comme sur le plan national) fait sujet d'un examen détaillé et minutieux. Il s'agit, somme tout, d'une appréciation au cas par cas.

On ne peut dès lors pas affirmer que l'ouverture du droit au mariage aux personnes de même sexe aura comme conséquence générale de conduire à limiter davantage le nombre potentiel des adoptions internationales.

- ❖ Un membre du groupe politique CSV rappelle que le Luxembourg a conclu, au niveau de l'adoption internationale, des accords avec le Vietnam. Or, à l'état actuel, les autorités luxembourgeoises n'ont pas encore enregistré une candidature à l'adoption visant ce pays.

Vote

Le projet de rapport recueille l'accord majoritaire de la commission, le représentant de la sensibilité politique ADR votant contre.

Temps de parole

La commission propose le modèle n°3 pour le débat en séance publique avec l'aménagement que le rapporteur disposera de 60 minutes pour exposer son rapport.

4. Divers

Création de deux sous-commissions au sein de la Commission juridique (en application de l'article 22, paragraphe (2) du Règlement de la Chambre des Députés)

1. La sous-commission, dénommée «*Sous-commission Création d'un droit européen des contrats pour les consommateurs et les entreprises de la Commission juridique (SCCJ)*» aura pour vocation de continuer les travaux déjà entamés par la sous-commission ayant porté la même dénomination et ayant été constituée au cours de la législature précédente (2009-2013). Il s'agit principalement de continuer les travaux parlementaires portant sur la proposition de Règlement du Parlement européen et du Conseil relatif à un droit commun européen de la vente (2011/0284/COD).
2. La sous-commission, dénommée «*Sous-commission modernisation du droit luxembourgeois des sociétés de la Commission juridique (SCDS)*», aura pour vocation de continuer l'examen et l'instruction parlementaire du projet de loi n°5730

portant modernisation de la loi modifiée du 10 août 1915 concernant les sociétés commerciales.

Une lettre afférente sera envoyée à la présidence de la Chambre des Députés en vue de l'approbation de la création des deux sous-commissions précitées par la Chambre des Députés réunie en séance plénière.

Ordre du jour de la prochaine réunion

La continuation de l'examen du projet de loi n°6518 sur la transaction en matière pénale et de l'avis afférent du Conseil d'Etat figureront à l'ordre du jour de la réunion de la commission du 4 juin 2014.

Le secrétaire-administrateur,
Laurent Besch

La Présidente,
Viviane Loschetter

Annexe: document relatif aux statistiques annuelles (2013) d'adoptions pour les Etats d'accueil établi par le Ministère de la Justice

Statistiques annuelles d'adoption pour les États d'accueil

État : Luxembourg
Année : 2013

État d'origine	Nombre total d'adoptions finalisées [1]	Âge et sexe de l'enfant à l'adoption [2]								Nombre d'adoptions d'enfants ayant des besoins spéciaux [3]	Nombre d'adoptions intrafamiliales [4]
		<1		1 à 4		5 à 9		>10			
		M	F	M	F	M	F	M	F		
<i>Afrique du Sud</i>	5			2	2	1	2				
<i>Bulgarie</i>											
<i>Cap Vert</i>											
<i>Corée du Sud</i>	9			3							
<i>Colombie</i>											
<i>Haïti</i>	3				1						
<i>Inde</i>											
<i>Luxembourg</i>	2	2									
<i>Népal</i>											
<i>Pérou</i>											
<i>Portugal</i>											
<i>Ukraine</i>											
<i>Divers</i>											
Nombre total d'adoptions internationales	17			5	3	1	2				
Nombre total d'adoptions nationales	2	2									
Nombre total d'adoptions	19	2		5	3	1	2				

Note [1] : Ce nombre comprend les adoptions finalisées dans l'État d'origine et les adoptions finalisées dans votre État.

Note [2] : Si vos statistiques nationales sont recueillies selon d'autres tranches d'âge, veuillez adapter le tableau en conséquence : par exemple, si vous ne comptabilisez que le nombre d'enfants de moins de cinq ans, il faudra fusionner les deux colonnes consacrées aux enfants de moins d'un an et aux enfants de un à quatre ans.

Note [3] : Les enfants ayant des besoins spéciaux peuvent souffrir de troubles du comportement ou d'un traumatisme, être atteints d'un handicap physique ou mental, être plus âgés (généralement plus de sept ans), ou faire partie d'une fratrie.

15



CHAMBRE DES DEPUTES

Session extraordinaire 2013-2014

CC/vg

Commission juridique

Procès-verbal de la réunion du 23 avril 2014

ORDRE DU JOUR :

1. Approbation des projets de procès-verbal des réunions du 26 mars 2014 et du 2 avril 2014
2. 6514 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- Rapporteur: Monsieur Guy Arendt
- Examen de l'avis complémentaire du Conseil d'Etat (4 avril 2014)
3. 6641 Projet de loi portant modification de l'article 491 du Code pénal
 - Désignation d'un rapporteur
 - Présentation du projet de loi
 - Examen de l'avis du Conseil d'Etat
4. Divers

*

Présents : M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Alex Bodry, M. Franz Fayot, M. Léon Gloden, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth
Mme Claudine Konsbruck, du Ministère de la Justice
M. Gilles Hermann, du Parquet de Luxembourg

Mme Carole Closener, de l'Administration parlementaire

Excusée : Mme Josée Lorsché

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission

*

1. Approbation des projets de procès-verbal des réunions du 26 mars 2014 et du 2 avril 2014

Les projets de procès-verbal des réunions du 26 mars 2014 et du 2 avril 2014 sont approuvés.

2. 6514 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**

Examen de l'avis complémentaire du Conseil d'Etat

Dans son deuxième avis complémentaire du 4 avril 2014, le Conseil d'Etat marque son accord avec le premier amendement.

Toutefois au sujet du deuxième amendement, le Conseil d'Etat 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 vise, sans discussion aucune, les compétences propres du juge d'instruction. Pour pouvoir agir, au titre de l'article 67-1, 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 et précise qu'une instruction préparatoire n'est pas ouverte. Selon le Conseil d'Etat, la modification de l'article 67-1 retenue par l'amendement est encore le résultat d'un mélange non justifié entre les deux dispositions.

En réponse à ces observations, le représentant du Parquet de Luxembourg expose une note intitulée « Motivation de la modification de l'article 67-1 CIC », pour les détails de laquelle il est renvoyé au document distribué au cours de la réunion.

L'orateur souligne 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 CIC 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, étant donné que l'article 24-1 CIC, tel que modifié par le projet de loi, prévoit désormais expressément, à côté des perquisitions, saisies, auditions et expertises, aussi la possibilité de retraçages et de repérages, sans saisine in rem, et qu'il renvoie dorénavant à l'article 67-1 du CIC, il est préférable de supprimer les termes « saisi de faits » qui risquent de donner lieu à des difficultés d'interprétation.

Les membres de la Commission partagent l'avis du Parquet et décident de maintenir la suppression des termes « saisi de faits ».

Dès lors, le texte du projet de loi ne fera plus l'objet de modifications, et le projet de rapport pourra être préparé en vue de son adoption lors d'une prochaine réunion.

3. 6641 Projet de loi portant modification de l'article 491 du Code pénal

Désignation d'un rapporteur

Les membres de la Commission désignent M. Alex Bodry comme rapporteur du projet de loi.

Présentation du projet de loi

L'article 491 du Code pénal sur l'abus de confiance prévoit dans son alinéa 2 actuel, datant d'une loi du 2 juillet 1980, entre autres le cas particulier de la grivèlerie d'essence. Selon l'exposé des motifs, cette incrimination spécifique a une origine historique alors que la jurisprudence considérait jadis que la filouterie ne constituait ni un vol ou une escroquerie, ni un abus de confiance.

Or, la jurisprudence en la matière a évolué, l'appropriation de carburant dans une station d'essence, sans paiement, étant considérée aujourd'hui comme un vol. De plus, l'application de la disposition sur la grivèlerie d'essence suscite de nombreux problèmes dans la mise en œuvre des poursuites, en particulier en relation avec la disposition qui prévoit que l'action publique sera éteinte par le paiement de la dette qui peut intervenir même en cours de procédure judiciaire.

Pour ces différentes raisons, le projet de loi, pour les détails duquel il est renvoyé au document parlementaire 6641¹, vise à modifier l'article 491, alinéa 2 en enlevant l'hypothèse de la grivèlerie d'essence et en supprimant la dernière phrase de l'alinéa 2 actuel sur l'extinction de l'action publique. Il est spécifié que la grivèlerie d'essence demeure couverte par les articles du Code pénal sur le vol à l'étalage.

Examen de l'avis du Conseil d'Etat

M. le rapporteur présente les grandes lignes de l'avis du Conseil d'Etat du 25 février 2014, pour les détails duquel il est renvoyé au document parlementaire afférent.

En premier lieu, le Conseil d'Etat soulève l'hypothèse où le chauffeur se fait servir de l'essence et quitte les lieux sans avoir payé le prix. Si la qualification de vol en station self-service peut aisément être retenue, par assimilation avec le vol à l'étalage, la discussion est ouverte pour le non-paiement de produits „livrés“ par l'exploitant ou le gérant de la station.

Pour couvrir ce cas de figure, selon le Conseil d'Etat, il faudrait se limiter à supprimer, dans le texte actuel, les mots „aura rempli“, ce qui laisse subsister le cas de figure où l'on fait remplir le réservoir par l'exploitant.

En deuxième lieu, le Conseil d'Etat attire l'attention des auteurs sur une difficulté résultant du nouvel alinéa 3 de l'article 491, tel qu'articulé par le projet de loi sous examen. Placé dans un troisième alinéa propre, la phrase selon laquelle l'action publique est éteinte par le désistement de la partie plaignante, signifie que cette extinction pourrait également s'appliquer à l'alinéa 1^{er} relatif à l'abus de confiance traditionnel. Si telle n'est pas l'intention des auteurs du projet, il conseille de rattacher cette phrase à la fin de l'alinéa 2 en marquant d'ores et déjà son accord avec un tel amendement.

Les membres de la Commission approuvent la pertinence de cette suggestion. Toutefois, étant donné l'observation suivante du Conseil d'Etat, ils décident de supprimer la disposition, plutôt que de la rattacher à l'alinéa 2.

En troisième lieu, le Conseil d'Etat s'interroge en effet sur le maintien du cas de figure du désistement tel qu'il est inscrit dans la loi actuelle. Selon le Conseil d'Etat, si le parquet est informé du paiement avant de lancer une citation, il y a de fortes chances qu'il renonce à des poursuites pour des considérations d'opportunité, qu'il y ait ou non désistement formel du plaignant. Si la citation est lancée, le parquet ne peut plus arrêter l'action publique, même en cas de paiement; par contre ce droit est reconnu au plaignant, du bon vouloir duquel dépendra le sort de l'action publique. Si les auteurs considèrent qu'il y a lieu d'exclure tout arrêt de l'action publique une fois qu'elle est entamée, il faudrait refuser cette prérogative également au plaignant.

Les membres de la Commission décident de suivre le Conseil d'Etat en supprimant cette disposition. Cette suppression ne devrait pas constituer un amendement dans la mesure où elle fait suite à une suggestion du Conseil d'Etat. Une lettre sera adressée dans ce sens au Conseil d'Etat.

Examen de l'avis de la Chambre des Métiers

Dans son avis du 22 avril 2014, la Chambre des Métiers ne formule aucune observation particulière relative au projet de loi qu'elle approuve.

Echange de vues

De l'échange de vues subséquent, il y a lieu de retenir les points suivants :

- La représentante du Ministère de la Justice fournira aux membres de la Commission juridique le rapport de la Police sur la problématique de la grivèlerie d'essence qui liste le nombre de grivèleries d'essence.
- Selon ce rapport, les exploitants de stations d'essence devraient s'engager à prendre eux-mêmes des mesures préventives, par exemple en installant des barrières, ou en instaurant un système de prépaiement de l'essence.

4. Divers

Sous réserve de la disponibilité de M. le Ministre de la Justice, les membres de la Commission proposent de convoquer, le 30 avril à 9 heures, une réunion jointe avec les membres de la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des

Communications et de l'Espace, au sujet de l'arrêt du 8 avril 2014 de la Cour de Justice de l'Union européenne (CJUE) concernant la directive 2006/24/CE sur la conservation des données.

Le Secrétaire-administrateur,
Carole Closener

La Présidente,
Viviane Loschetter

12



Commission juridique

Procès-verbal de la réunion du 19 mars 2014

Ordre du jour :

1. Approbation des projets de procès-verbal des réunions du 26 février 2014 et du 5 mars 2014
2. 6172A Projet de loi portant
 - a) réforme du Titre II.- du Livre Ier du Code civil «Des actes de l'état civil» et modifiant les articles 34, 47, 57, 63, 70, 71, 73, 75, 76, 79, et 95;
 - b) réforme du Titre V.- du Livre Ier du Code civil «Du mariage» et rétablissant l'article 143 et modifiant les articles 144, 145, 147 à 154, 158 à 160, 160bis à 171, 173 à 175, 176 à 192, 194 à 199, 201 à 205, 212, 213, 223, 227, 228, 295 et introduisant les articles 146-1, 146-2, 175-1, 175-2 nouveaux;
 - c) modification des articles 108, 169, 295, 313, 315 et abrogation des articles 296 et 297 du Code civil;
 - d) introduction d'un Titre VI.bis nouveau dans la Deuxième Partie du Nouveau Code de procédure civile;
 - e) introduction d'un Chapitre VII.bis nouveau au Titre VII du Livre Ier du Code pénal;
 - f) abrogation de la loi du 23 avril 1827 concernant la dispense des prohibitions du mariage prévues par les articles 162 à 164 du Code civil; et
 - g) abrogation de la loi du 19 décembre 1972 portant introduction d'un examen médical avant mariage- Rapporteur: Monsieur Paul-Henri Meyers
- Présentation et adoption d'une série d'amendements parlementaires
3. 6514 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- Rapporteur: Monsieur Guy Arendt
- Présentation et adoption d'une série d'amendements parlementaires
4. 6647 Projet de loi modifiant les articles 15 (2) et 16 (2) de la loi modifiée du 10 août 1991 sur profession d'avocat

- Désignation d'un Rapporteur
- Présentation du projet de loi et examen de l'avis du Conseil d'Etat du 11 mars 2014

5. 6666 Projet de loi concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2014
- Rapporteur: Monsieur Eugène Berger
 - Présentation du volet budgétaire du Ministère de la Justice (demande de la sensibilité politique ADR)
6. Divers

*

Présents : M. Guy Arendt, Mme Simone Beissel, M. Roger Negri remplaçant M. Alex Bodry, M. Franz Fayot, M. Léon Gloden, Mme Josée Lorsché, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth

M. Félix Braz, Ministre de la Justice

Mme Jeannine Dennewald, Mme Nancy Karier, Mme Marie-Anne Ketter, M. Laurent Thyès, du Ministère de la Justice

M. Laurent Besch, de l'Administration parlementaire

Excusés : M. Marc Angel, M. Alex Bodry

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission

*

1. Approbation des projets de procès-verbal des réunions du 26 février 2014 et du 5 mars 2014

Les projets de procès-verbal repris sous référence n'appellent pas d'observations et recueillent l'accord unanime des membres de la commission.

2. 6172A Projet de loi portant

a) réforme du Titre II.- du Livre Ier du Code civil «Des actes de l'état civil» et modifiant les articles 34, 47, 57, 63, 70, 71, 73, 75, 76, 79, et 95;

b) réforme du Titre V.- du Livre Ier du Code civil «Du mariage» et rétablissant l'article 143 et modifiant les articles 144, 145, 147 à 154, 158 à 160, 160bis à 171, 173 à 175, 176 à 192, 194 à 199, 201 à 205, 212, 213, 223, 227, 228, 295 et introduisant les articles 146-1, 146-2, 175-1, 175-2 nouveaux;

c) modification des articles 108, 169, 295, 313, 315 et abrogation des articles 296 et 297 du Code civil;

d) introduction d'un Titre VI.bis nouveau dans la Deuxième Partie du Nouveau Code de procédure civile;

e) introduction d'un Chapitre VII.bis nouveau au Titre VII du Livre Ier du

Code pénal;

f) abrogation de la loi du 23 avril 1827 concernant la dispense des prohibitions du mariage prévues par les articles 162 à 164 du Code civil; et

g) abrogation de la loi du 19 décembre 1972 portant introduction d'un examen médical avant mariage

Présentation des propositions d'amendement (*document envoyé par courrier électronique du 14 mars 2014 aux membres de la Commission juridique*)

M. le Rapporteur présente succinctement les *points 1. à 5. du point I. Observations préliminaires* du projet de lettre d'amendement.

Au sujet de l'abrogation proposée de l'article 1595 du Code civil (prohibition de la vente entre époux) et des éventuelles conséquences et implications sur le plan fiscal (fiscalité directe et indirecte), M. le Ministre de la Justice propose d'envoyer un courrier afférent au Ministre des Finances afin que ce dernier procède aux vérifications qui s'imposent.

Le représentant de la sensibilité politique ADR informe les membres de la commission qu'il s'oppose à l'ouverture du mariage, institution familiale, aux couples homosexuels. Il ajoute qu'il est uniquement disposé à participer aux travaux parlementaires en ce qui concerne les seuls points d'ordre technique.

Vote

Soumises au vote, les propositions d'amendement parlementaires recueillent la majorité des voix avec une abstention de la part du représentant de la sensibilité politique ADR.

3. 6514 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**

Présentation des propositions d'amendement (*document envoyé par courrier électronique du 17 mars 2014 aux membres de la Commission juridique*)

M. le Rapporteur présente succinctement les deux propositions d'amendement parlementaires.

Le représentant du ministère de la Justice informe les membres de la commission que le ministère de la Justice est en train de rédiger le commentaire des articles qui portera tant sur les articles de la future loi que sur les articles de la Convention du Conseil de l'Europe du 23 novembre 2001.

Vote

Lesdites propositions d'amendement recueillent l'accord unanime des membres de la commission.

4. 6647 Projet de loi modifiant les articles 15 (2) et 16 (2) de la loi modifiée du 10 août 1991 sur profession d'avocat

Désignation d'un rapporteur

La commission unanime désigne M. Guy Arendt comme rapporteur du projet de loi.

Présentation du projet de loi

Le représentant du ministère de la Justice explique qu'il est proposé de porter le mandat des membres du Conseil de l'ordre des avocats des deux barreaux d'un an à deux ans. Il est proposé de modifier en ce sens le paragraphe (2) respectif des articles 15 et 16 de la loi modifiée du 10 août 1991 sur la profession d'avocat.

Ainsi, la durée du mandat du Bâtonnier et des membres du Conseil de l'ordre des avocats est alignée sur celle du mandat des membres du Conseil disciplinaire et administratif et sur celle des membres du Conseil disciplinaire et administratif d'appel qui est de deux ans.

Il convient de préciser que le Bâtonnier, une fois son mandat terminé, continue à siéger pour un mandat de deux ans au sein du Conseil de l'ordre des avocats du Barreau respectif en sa qualité de Bâtonnier sortant (article 16, paragraphe (1) de la loi modifiée précitée de 1991).

Ces modifications reflètent une demande afférente des Conseils de l'ordre des avocats des Barreaux de Diekirch et de Luxembourg.

Examen de l'avis du Conseil d'Etat

Le Conseil d'Etat, qui a rendu son avis en date du 11 mars 2014, approuve le texte de loi proposée et n'a pas d'observations à formuler.

Echange de vues

De l'échange de vues qui s'ensuit, il y a lieu de retenir ce qui suit:

- Au préalable à la réforme de la profession d'avocat opérée par le biais de l'adoption de la loi (modifiée) du 10 août 1991 sur la profession d'avocat, la durée du mandat du Bâtonnier était bel et bien de deux ans.
- A l'heure actuelle, il est de coutume que le Bâtonnier élu une première fois se présente une seconde fois de sorte que le mandat effectivement exercé sera de quatre ans, durée à laquelle il convient d'ajouter le mandat de deux ans en tant que Bâtonnier sortant qui est d'office membre du Conseil de l'ordre des avocats.
- Il y a lieu de mentionner qu'il existe certaines difficultés de recrutement quant à la composition du Conseil de l'ordre des avocats et notamment pour la fonction de Bâtonnier, étant donné la charge de travail qui incombe au Bâtonnier. En effet, la charge de travail et la présence requise de la part du Bâtonnier font que les études

d'avocats de plus modeste taille hésitent à ce qu'un de leurs associés puisse être libéré pour assumer la fonction de Bâtonnier.

- L'augmentation de la durée du mandat à deux ans répond à une nécessité réelle permettant au titulaire de prendre amplement connaissance de ses tâches multiples et d'exercer le mandat lui confié en parfaite connaissance de cause.
- Dans les pays limitrophes, la durée du mandat du Bâtonnier est en principe de deux ans.

La présentation et l'adoption d'un projet de rapport figureront à l'ordre du jour de la réunion de la commission du mercredi 2 avril 2014.

5. 6666 Projet de loi concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2014

Ce point est reporté, à la demande de M. le Ministre de la Justice (Conseil de Gouvernement à 10h00), à la réunion du mercredi 2 avril 2014 à 09h00.

Le secrétaire,
Laurent Besch

La Présidente,
Viviane Loschetter

09



CHAMBRE DES DEPUTES

Session extraordinaire 2013-2014

LB/pk

Commission juridique

Procès-verbal de la réunion du 26 février 2014

ORDRE DU JOUR :

1. Approbation du projet de procès-verbal de la réunion du 12 février 2014
2. 6562 Projet de loi renforçant le droit des victimes de la traite des êtres humains et portant modification
 - (1) du Code pénal;
 - (2) de la loi modifiée du 12 mars 1984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse;
 - (3) de la loi du 8 mai 2009 sur l'assistance, la protection et la sécurité des victimes de la traite des êtres humains et modifiant le Nouveau Code de procédure civile;
 - (4) de la loi du 29 août 2008 portant sur la libre circulation des personnes et l'immigration
 - Rapporteuse: Madame Viviane Loschetter
 - Examen du 2e avis complémentaire du Conseil d'Etat du 25 février 2014
 - Présentation et adoption définitive d'un projet de rapport
3. 6514 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
 - Rapporteur: Monsieur Guy Arendt
 - Examen de l'avis complémentaire du Conseil d'Etat du 12 novembre 2013
4. Divers

*

Présents : M. Marc Angel, M. Guy Arendt, Mme Simone Beissel, M. Alex Bodry, M. Franz Fayot, Mme Viviane Loschetter, M. Paul-Henri Meyers, Mme Diane Adehm remplaçant Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Roy Reding, M. Gilles Roth

Mme Claudine Konsbruck, Mme Pascale Millim, M. Laurent Thyès, du Ministère de la Justice

M. Laurent Besch, de l'Administration parlementaire

Excusés : M. Léon Gloden, Mme Octavie Modert

*

Présidence : Mme Viviane Loschetter, Présidente de la Commission

*

1. **Approbation du projet de procès-verbal de la réunion du 12 février 2014**

Le projet de procès-verbal modifié (corrections apportées au texte des pages 4, 6 et 7) recueille l'accord unanime des membres de la commission.

*

Le représentant de la sensibilité politique ADR regrette que le point 5. de l'ordre du jour de la réunion afférente – examen de trois documents COM soumis au test de subsidiarité – n'a pas pu être entamé.

Sa proposition que l'examen de documents COM soumis au test de subsidiarité figurera à l'avenir en tant que premier point à l'ordre du jour rencontre l'accord unanime des membres de la commission.

- ## 2. **6562 Projet de loi renforçant le droit des victimes de la traite des êtres humains et portant modification**
- (1) du Code pénal;**
 - (2) de la loi modifiée du 12 mars 1984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse;**
 - (3) de la loi du 8 mai 2009 sur l'assistance, la protection et la sécurité des victimes de la traite des êtres humains et modifiant le Nouveau Code de procédure civile;**
 - (4) de la loi du 29 août 2008 portant sur la libre circulation des personnes et l'immigration**

Mme la Rapportrice explique que le projet de rapport, approuvé en son principe lors de la réunion de la commission du 12 février 2014, a dû être adapté pour tenir compte du 2^e avis complémentaire du Conseil d'Etat que ce dernier a rendu sur sa propre initiative le 25 février 2014. L'information que le Conseil d'Etat émettra un 2^e avis complémentaire en complément

à son premier avis complémentaire du 4 février 2014 a été reçue peu après la réunion précitée du 12 février 2014 de la Commission juridique, de sorte qu'il a été décidé d'adapter le rapport (les propositions d'adaptation figurent en caractères jaunes surlignés dans le projet de rapport adapté envoyé aux membres de la commission par courrier électronique en date du 25 février 2014) et de le soumettre pour adoption définitive aux membres de la commission.

Le Conseil d'Etat, dans ledit 2^e avis complémentaire, constate que «[...] la disposition incriminant la vente des enfants, qu'il avait proposée d'insérer à l'endroit de l'article 382-3 du Code pénal, entraîne un décalage des articles subséquents qui risque de poser des problèmes au niveau des renvois existants dans d'autres textes et notamment dans le Code pénal même (articles 382-5 et 506-1 du Code pénal).».

Il propose dès lors, contrairement à ce qu'il avait suggéré dans son avis complémentaire précité, de ne pas ajouter un nouvel article dans le Code pénal, mais d'en compléter l'article 382-1 (article 2 du projet de loi) par un nouvel paragraphe (4) reprenant le texte relatif à la vente d'enfants.

Article 5 du texte de loi future – modification de l'article 15 de la loi du 12 mars 1984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse

Au sujet des conditions relatives à l'indemnisation de certaines victimes de dommages corporels telles que prévues par la loi du 12 mars 1984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse, il convient de rappeler que le droit à indemnisation est étendu aux victimes de la traite qui n'ont pas leur résidence régulière et habituelle au Luxembourg (nouvel alinéa 2 de l'article 15 de la loi du 12 mars 1984 précitée). La dispense de l'obligation d'une résidence régulière et habituelle résulte de la vocation globale et générale de la directive 2011/36/UE et plus particulièrement de son article 17.

Il importe de noter que ce droit à indemnisation, dans le cas de figure d'un fait dommageable tombant sous le champ de l'infraction de la traite telle que définie à l'endroit de l'article 382-1 modifié du Code pénal, n'est ouvert qu'à condition que la personne lésée à l'étranger n'est pas en droit d'être indemnisée par un autre Etat.

Le représentant de la sensibilité politique ADR réitère sa question si cette condition de résidence doit être remplie au moment des faits ayant été la cause des lésions corporelles subies par la personne victime ou si cette condition de résidence suffit à elle-même.

La représentante du Ministère de la Justice informe les membres de la Commission juridique qu'aucune demande d'indemnisation en ce sens n'a été introduite à ce jour.

Elle explique que dans le cadre de l'élaboration d'un projet de loi devant transposer une directive portant notamment sur le renforcement des droits de la personne victime d'un fait incriminé, la loi du 12 mars 1984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse devra être revue.

Le projet de rapport ainsi adapté recueille l'accord majoritaire des membres de la commission avec une abstention du représentant de la sensibilité politique ADR.

3. 6514 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

Examen de l'avis complémentaire du Conseil d'Etat du 12 novembre 2013

Amendement n°1

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

Amendement n°2

Le Conseil d'Etat n'a pas d'observation, sauf à rappeler sa préférence en vue d'une nouvelle approche devant consacrer le concept de bien incorporel.

Amendements n°3 à n°8

Ces amendements rencontrent l'accord du Conseil d'Etat.

Amendement n°9

Le Conseil d'Etat déclare réitérer *«[...] ses interrogations quant à la cohérence du système répressif [...] concernant l'incohérence d'ordre conceptuel entre la modification envisagée à l'endroit de l'article 31 du Code d'instruction criminelle permettant la saisie et la perquisition de données informatiques et celles proposées concernant les articles 496 et 509-5 du Code pénal visant les concepts différents de clef électronique, de mot de passe ou de code d'accès.»*

A ce sujet, il convient de noter qu'un groupe de travail ad hoc a été constitué afin de mener des réflexions approfondies à ce sujet en vue d'une introduction en droit luxembourgeois le concept de bien incorporel.

Amendements n°10 à n°12

Ces amendements ne donnent pas lieu à observation particulière de la part du Conseil d'Etat.

Amendement n°13

Paragraphe (1)

Au sujet du repérage, tel que visé par le point 1. du paragraphe (1), 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», alors que la restriction en termes de taux de peines y a été supprimée, mais a été maintenue à l'endroit du point 2. relatif à la localisation de l'origine ou de la destination de télécommunications.

Or, tel n'a pas été l'intention de la Commission juridique.

M. le Rapporteur propose partant de reformuler le paragraphe (1) comme suit:

«(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, **si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement**.

Dans les cas visés à l'alinéa 1^{er}, 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.»

Cette proposition d'amendement recueille l'accord unanime des membres de la commission.

Il convient de préciser, à l'endroit du commentaire des articles du rapport de la commission, 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 convient de rappeler 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.

[commentaire des articles, rapport de la commission]

Paragraphe (3)

Le Conseil d'Etat «ne peut pas davantage suivre les auteurs des amendements quant ils proposent, pour l'information de la personne concernée, d'ajouter une référence à l'enquête

préliminaire à l'article 67-1, paragraphe 3. 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.

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, de l'enquête préliminaire.»

Il invite dès lors les auteurs à reconsidérer leurs positions et renvoie, pour le surplus, aux propositions de texte formulées dans son avis du 16 avril 2013.

M. le Rapporteur propose d'amender tant l'article 24-1 (insertion d'un renvoi aux paragraphes (1) et (2) de l'article 67-1 du Code d'instruction criminelle) que l'article 67-1, paragraphe (3), alinéa 2 du Code d'instruction criminelle (suppression du renvoi à l'article 24-1 du Code d'instruction criminelle).

Amendement n°14

Compte tenu de la position du Conseil d'Etat de maintenir sa proposition de texte ainsi que la référence aux «*compétences prévues par le Code d'instruction criminelle*», il convient de rappeler 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.

Les membres de la Commission juridique soulignent la nécessité de disposer d'un commentaire des articles exhaustif. En effet, le Conseil d'Etat a eu, pour certains articles du projet de loi, une lecture différente des auteurs du projet de loi qui ont eu une concertation préalable intensive avec les autorités judiciaires.

L'adoption des trois propositions d'amendement figurera à l'ordre du jour de la réunion du 19 mars 2014. Dans le cas de figure où la présentation du rapport GRETA, actuellement prévue pour la réunion du 12 mars 2014, devrait être reportée, l'adoption des trois propositions d'amendement figurera à l'ordre du jour de la réunion du 12 mars 2014.

4. Divers

Mme la Présidente informe qu'une réunion jointe de la Commission des Libertés civiles, justice et affaires intérieures du Parlement européen et de la Commission de l'administration publique, de l'ordre public et de la justice du Parlement grecque (dans le cadre de la présidence grecque du Conseil de l'Union européenne) portant sur le thème «*Priorités futures au niveau des libertés civiles, de la justice et des affaires intérieures*» aura lieu le mercredi 19 mars 2014 de 09h00 à 18h30 au siège du Parlement européen à Bruxelles.

Le Bureau de la Chambre des Députés a autorisé deux membres de la Commission juridique, à savoir un membre de la majorité et un membre de l'opposition, à y assister.

Les personnes intéressées sont priées d'en informer le secrétariat de la commission (l'inscription prendra fin le 10 mars 2014).

Le secrétaire,
Laurent Besch

La Présidente,
Viviane Loschetter



Commission juridique

Procès-verbal de la réunion du 05 juin 2013

Ordre du jour :

1. 6514 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- Rapporteur: Monsieur Gilles Roth
- Examen d'une série d'amendements gouvernementaux

2. Divers

*

Présents : M. Marc Angel, M. Xavier Bettel, M. Alex Bodry, M. Félix Braz, Mme Christine Doerner, M. Léon Gloden, M. Jacques-Yves Henckes, M. Jean-Pierre Klein, M. Paul-Henri Meyers, Mme Lydie Polfer, M. Gilles Roth

Mme Octavie Modert, Ministre de la Justice
M. Laurent Thyès, du Ministère de la Justice
M. Gilles Herrmann, du Parquet de Luxembourg

Mme Carole Closener, de l'Administration parlementaire

Excusé : M. Lucien Weiler

*

Présidence : M. Gilles Roth, Président de la Commission

*

1. **6514** **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

Présentation et adoption d'une série d'amendements parlementaires

Le rapporteur du projet de loi, M. Gilles Roth présente une série d'amendements parlementaires pour le détail desquels il y a lieu de se référer au document annexé, qui a été envoyé par courrier électronique le 31 mai 2013.

Les amendements sont adoptés à l'unanimité, étant précisé qu'ils pourront faire l'objet d'aménagements techniques.

*

D'un commun accord, les membres de la Commission décident d'ajouter le point suivant à l'ordre du jour :

2. **6172 A** **Projet de loi portant**
- a) **réforme du Titre II.- du Livre Ier du Code civil «Des actes de l'état civil» et modifiant les articles 34, 47, 57, 63, 70, 71, 73, 75, 76, 79, et 95;**
 - b) **réforme du Titre V.- du Livre Ier du Code civil «Du mariage» et rétablissant l'article 143 et modifiant les articles 144, 145, 147 à 154, 158 à 160, 160bis à 171, 173 à 175, 176 à 192, 194 à 199, 201 à 205, 212, 213, 223, 227, 228, 295 et introduisant les articles 146-1, 146-2, 175-1, 175-2 nouveaux;**
 - b) **modification des articles 108, 169, 295, 313, 315 et abrogation des articles 296 et 297 du Code civil;**
 - c) **introduction d'un Titre VI.bis nouveau dans la Deuxième Partie du Nouveau Code de procédure civile;**
 - d) **introduction d'un Chapitre VII.bis nouveau au Titre VII du Livre Ier du Code pénal;**
 - e) **abrogation de la loi du 23 avril 1827 concernant la dispense des prohibitions du mariage prévues par les articles 162 à 164 du Code civil; et**
 - f) **abrogation de la loi du 19 décembre 1972 portant introduction d'un examen médical avant mariage**

Le Président de la Commission juridique propose de procéder à un échange de vues informel suite à une présentation par le rapporteur du projet de loi de l'avis complémentaire du Conseil d'Etat.

Examen de l'avis complémentaire du Conseil d'Etat

Le rapporteur du projet de loi, M. Paul-Henri Meyers, présente l'avis du Conseil d'Etat du 4 juin 2013, pour les détails duquel il est prié de se référer au document parlementaire afférent.

Il est rappelé qu'une série d'amendements a été soumise au Conseil d'Etat le 11 mars dernier. Par le biais d'un des amendements, la Commission juridique entendait se rallier à l'option prise par le Gouvernement ayant proposé « d'ouvrir les portes » de l'adoption dite simple, tant de l'adoption nationale que de l'adoption internationale, aux couples de même sexe, qu'ils soient mariés ou qu'ils vivent dans un partenariat enregistré. Un nouvel article 367-4 devait ainsi exclure l'adoption plénière dans le chef de deux conjoints de même sexe.

Or, dans son avis du 4 juin 2013, le Conseil d'Etat estime, sous peine de refuser la dispense du second vote constitutionnel, que la proposition d'écarter les conjoints homosexuels de l'adoption plénière exige un argumentaire justifiant la disparité envisagée cadrant avec les articles 10*bis* de la Constitution et 14 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Le Conseil d'Etat reconnaît que l'institution de l'adoption est à analyser dans la perspective de l'intérêt supérieur de l'enfant et non pas dans une optique d'un droit à l'adoption pour les adoptants. L'argumentaire en question doit établir que l'intérêt supérieur de l'enfant impose l'existence d'un référant maternel et paternel parmi ses parents adoptifs sinon biologiques.

D'après le rapporteur, le Conseil d'Etat serait cependant prêt à admettre que la Chambre vote le projet de loi avec l'ajout de l'article 367-4 (proposé par l'amendement 4), puisqu'il propose de compléter l'intitulé afin de tenir compte de ce dispositif. Toutefois le Conseil d'Etat indique qu'il « se voit dans l'impossibilité d'accorder la dispense du second vote constitutionnel à défaut pour les auteurs de fournir un autre argument susceptible de justifier la disparité envisagée au regard de l'article 10*bis* de la Constitution et de l'article 14 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. »

Or, cela paraît extrêmement difficile à établir, d'autant plus qu'en pratique il existe de nombreux cas d'enfants élevés par un parent seul (mère ou père célibataire) soit par deux personnes de même sexe vivant en communauté.

Par ailleurs, le Conseil d'Etat attire encore l'attention sur un autre problème discuté en France et tenant à la situation des adoptés par rapport à la divulgation de leurs origines biologiques.

Le Conseil d'Etat français a en effet rendu en octobre 2012 un avis sur l'ouverture au mariage des couples de personnes de même sexe dans lequel il a considéré que l'adoption plénière a pour effet de supprimer juridiquement la filiation par le sang pour lui substituer un nouveau lien de filiation découlant du jugement qui l'a prononcé. Par la suite, l'acte de naissance d'origine de l'enfant est remplacé par un nouvel acte établi à partir du jugement d'adoption sans aucune référence à la filiation réelle de l'intéressé. L'état civil ainsi reconstitué mettra en évidence, par la référence à des parents de même sexe, la fiction juridique sur laquelle repose cette filiation. Le Conseil d'Etat français a donc appelé l'attention du gouvernement, d'une part, sur les conséquences de cette situation, délicate et toujours en débat, au regard de l'accès aux origines et, d'autre part, sur les précautions qu'il conviendra de prendre dans la rédaction des actes de naissance en cause.

Enfin, le Conseil d'Etat recommande de manière générale de saisir l'occasion pour procéder à une réforme globale de l'adoption et de réfléchir sur le maintien de la dualité des régimes d'adoption. Par ailleurs, il propose de mettre en place, à l'instar de la loi française n° 2002-93 du 22 janvier 2002 relative à l'accès aux origines des personnes adoptées et pupilles de l'Etat, un dispositif qui permettrait à l'adopté de lever le secret sur ses origines, quel que soit le type d'adoption.

Pour le rapporteur du projet de loi, les trois alternatives suivantes s'offrent à la Commission :

- soit la Commission maintient son texte et le vote à deux reprises, vu le refus du Conseil d'Etat d'accorder la dispense du second vote. Cette option présente toutefois le risque d'engendrer des recours devant la Cour constitutionnelle ;
- soit la Commission examine le projet de loi portant réforme de l'adoption et effectue une analyse de droit comparé (basée notamment sur les législations belge et française), afin de déterminer s'il est possible de réformer l'adoption à court terme dans le sens indiqué par le Conseil d'Etat, en retenant un seul régime d'adoption qui préserve l'intérêt supérieur de l'enfant et le droit de connaître ses origines biologiques;
- soit le projet de loi est voté sans l'article 367-4. Cela a pour conséquence que les couples homosexuels ont accès, dans une période intermédiaire (jusqu'à l'adoption de la réforme de l'adoption) aux deux régimes d'adoption. Cette alternative présente l'inconvénient de ne pas résoudre toute la problématique liée à l'adoption.

Echange de vues :

De l'échange de vues informel subséquent, il y a lieu de retenir les points suivants :

- Le représentant du groupe parlementaire « déi gréng », M. Félix Braz, rappelle, en réponse aux remarques du Conseil d'Etat, que la Commission juridique n'entendait pas se limiter à la réforme du mariage. Si elle avait décidé dans un premier temps d'ouvrir l'adoption simple aux couples homosexuels, elle avait l'intention d'entamer la réforme de l'adoption tout de suite après l'évacuation du projet de loi portant réforme du mariage. L'orateur souhaite que la Commission s'engage sur un calendrier fixe à respecter. Si l'option retenue consiste à traiter, dans un premier temps, le volet mariage, le projet de loi serait idéalement voté au début de la session parlementaire 2013-2014. La Commission traiterait ensuite le volet adoption comme une priorité. Par ailleurs, le groupe parlementaire « déi gréng » ne voit pas d'inconvénient à ce qu'un seul régime d'adoption soit retenu. En outre, le fait de maintenir le texte dans sa forme actuelle, quitte à se voir refuser la dispense du second vote, peut être une option.
- Selon le représentant du groupe parlementaire LSAP, M. Alex Bodry, il n'est pas souhaitable de passer outre les remarques du Conseil d'Etat eu égard aux risques de recours, à moins de disposer d'un argumentaire.
Concernant les régimes d'adoption, les opinions sont divergentes, même au sein de son groupe politique, d'où la difficulté de trouver un accord dans un délai raisonnable.
D'après l'orateur, la réforme du mariage ne doit en aucun cas être bloquée en raison de l'absence d'un consensus sur l'adoption. Aussi est-il souhaitable que le projet de loi portant réforme du mariage soit évacué avant la fin de l'année, même si la complexité du dossier risque de retarder la réforme.
L'orateur rappelle par ailleurs que la réforme en Belgique a été réalisée en deux étapes : le mariage d'abord, puis, quelques années après, l'adoption. Partant il serait intéressant d'analyser ces documents afin de voir les arguments qui ont poussé le législateur belge à retenir cette démarche.
- Le représentant du groupe parlementaire DP, M. Xavier Bettel, rappelle que le projet de loi n°6172 a été déposé en 2010. Or en France le projet de loi a pu être évacué dans un délai très rapproché, et ce malgré les nombreux recours. Partant, afin

d'avancer rapidement, l'orateur propose d'examiner les législations des pays voisins dès la semaine prochaine. Par ailleurs, il soulève la question du délai d'entrée en vigueur qui a été porté à six mois. La conséquence en est que si le projet de loi est voté à la rentrée parlementaire, les premiers mariages seront célébrés en pleine campagne électorale.

- Selon le député indépendant, M. Jacques-Yves Henckes, il convient d'évacuer rapidement le projet de loi n°6172A et de trouver en outre un consensus sur l'adoption.
- Selon M. Léon Gloden, représentant du groupe parlementaire CSV, dans la mesure où le mariage homosexuel et l'adoption sont des sujets sensibles sur le plan de politique sociale, il importe de poser un cadre juridique clair, et d'éviter des risques de recours. Il paraît par ailleurs souhaitable de ne pas les associer à la campagne électorale.
En outre, l'orateur rappelle qu'il y a eu un changement de paradigme en matière d'adoption qui devrait aboutir une forme unique d'adoption. A l'époque du Code civil, l'adoption devait en effet permettre de rompre tout lien avec la famille biologique, alors qu'actuellement l'intérêt supérieur de l'enfant et son droit de connaître ses origines prédominent.
- Vu la technicité du sujet, il semble difficile de respecter le délai de fin 2013 pour la réforme de l'adoption.
- Le droit de l'enfant de connaître ses origines biologiques est inscrit dans le projet de loi n° 6568 portant réforme du droit de la filiation.
- Quant à l'opportunité de voter le projet de loi 6172A avant la conclusion des travaux parlementaires concernant l'adoption, une piste pourrait consister à trouver un consensus sur la réforme de l'adoption, ensuite évacuer la réforme du mariage - sans l'adoption - et finalement procéder au vote de la réforme de l'adoption.
- Pendant la période intermédiaire, durant laquelle les couples homosexuels auraient accès aux deux régimes d'adoption, les demandes d'adoption continueraient à être examinées au cas par cas, sur base de dossier.
- Cette façon de procéder semble recueillir l'approbation de Madame la Ministre.
- Selon le rapporteur du projet de loi, il faut néanmoins d'abord étudier la possibilité de garder le lien entre les deux réformes. Si l'examen des textes lors des prochaines réunions devait conduire à la conclusion qu'il n'est pas possible d'évacuer les deux réformes ensemble, alors la scission peut constituer une alternative.

Il est proposé aux membres de la Commission de concerter leurs groupes parlementaires respectifs sur les différentes questions abordées lors de la présente réunion et de revenir sur le sujet lors de la prochaine réunion.

En vue de cette réunion, le Ministère de la Justice fournira aux membres de la Commission une documentation contenant une étude de droit comparé concernant le mariage homosexuel et l'adoption, ainsi qu'un recueil de jurisprudence et de doctrine.

3. Divers

Les membres de la Commission décident de convoquer la prochaine réunion le mercredi 12 juin 2013 avec l'ordre du jour suivant :

- Projet de loi n°6172A : Continuation de l'examen du projet de loi
- Projet de loi n°6172B : Examen du projet de loi

Luxembourg, le 5 juin 2013

La secrétaire,
Carole Closener

Le Président,
Gilles Roth



Commission juridique

Procès-verbal de la réunion du 15 mai 2013

Ordre du jour :

1. 6514 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- Rapporteur: Monsieur Gilles Roth
- Continuation de l'examen du projet de loi et de l'avis du Conseil d'Etat
2. Approbation des projets de procès-verbal des réunions des 10, 17 et 24 avril 2013
3. Divers

*

Présents : M. Marc Angel, M. Xavier Bettel, M. Alex Bodry, M. Félix Braz, Mme Christine Doerner, M. Léon Gloden, M. Jean-Pierre Klein, M. Paul-Henri Meyers, Mme Lydie Polfer, M. Gilles Roth, M. Lucien Weiler

Mme Octavie Modert, Ministre de la Justice
M. Laurent Thyès, du Ministère de la Justice
M. Gilles Herrmann, du Parquet de Luxembourg

Mme Carole Closener, de l'Administration parlementaire

Excusé : M. Jacques-Yves Henckes

*

Présidence : M. Gilles Roth, Président de la Commission

*

1. 6514 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**

En réponse aux questions soulevées par les membres de la Commission au cours de la réunion du 8 mai 2013, les représentants du Ministère de la Justice et du Parquet exposent une note, pour les détails de laquelle il est prié de se référer à l'annexe, diffusée par courrier électronique le 14 mai 2013.

Face aux réserves exprimées par les membres de la Commission, il est proposé de renoncer à modifier l'article 231 du Code pénal. Par conséquent, le point 1 de l'article 3 sera retiré du projet de loi. Quant à l'article 213bis, sur lequel un consensus semble s'être dégagé, son libellé sera maintenu, tel que proposé par le point 2 de l'article 3 du projet de loi.

Le document annexé contient par ailleurs une nouvelle proposition de libellé pour le point 5 du projet de loi (qui a pour objet de modifier le point 1) de l'article 506-1 du Code pénal) qui vise à tenir compte des observations du Conseil d'Etat.

Etant donné que l'article 231, qui est rédigé au futur, ne sera pas modifié, il ne semble pas indiqué de conjuguer l'article 231 bis à l'indicatif présent. En effet, il n'y aurait alors plus de cohérence entre les deux articles.

Les membres de la Commission approuvent les propositions de modification

La réunion se poursuit par l'examen du projet de loi et de l'avis du Conseil d'Etat.

Point 8

Le nouvel article 509-5 du Code pénal introduit au point 8 est destiné à transposer en droit national l'article 6 de la Convention.

Le Conseil d'Etat émet des 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.

Concernant le critère du « mépris des droits d'autrui », le représentant du Parquet indique qu'il n'y a pas lieu de l'ajouter au premier tiret, dans la mesure où ce tiret

renvoie aux articles 509-1 à 509-4¹, qui eux consacrent le critère précité. L'objet étant de créer une double intention frauduleuse, la détention frauduleuse doit en plus nuire à un tiers. En revanche, le critère du « mépris des droits d'autrui » doit être ajouté au deuxième tiret, étant donné que ce tiret n'opère pas de renvoi.

Conformément à ce qui a été décidé lors de la réunion du 8 mai 2013, les membres de la Commission conviennent de supprimer les termes « mot de passe » et « code d'accès », qui étaient cités à titre d'exemples et de retenir le seul terme de « toute clé électronique ». Dans le commentaire des articles, il sera précisé que la notion de « clé électronique » englobe les notions de mot de passe et de code d'accès.

Quant à la suggestion du Conseil d'Etat de viser le « système informatique », il est rappelé que la terminologie de « système de traitement ou de transmission automatisé de données » correspond à celle déjà utilisée dans les articles 509-1 à 509-7. Partant, il est préférable, afin de préserver la cohérence des textes, de maintenir cette terminologie.

La Chambre de Commerce, dans son avis du 27 février 2013, s'étonne de l'abaissement de l'amende prévue à l'alinéa 2 à l'article 509-3 du Code pénal, actuellement de 1.250 euros à 30.000 euros, et de son remplacement par une amende de 251 euros à 5.000 euros seulement. Le représentant du Parquet explique que les auteurs du projet de loi souhaitaient initialement aligner les amendes sur celles de l'article 488 (qui fait l'objet du point 3 de l'article 3 du projet de loi). Toutefois il n'était pas dans leur intention de baisser le niveau actuel de l'amende. Il est important de prévoir des niveaux élevés pour les amendes afin de décourager les auteurs d'infractions. Partant, il paraît indiqué de relever le seuil des amendes prévues aux articles 488 et 509-5 à 30.000 euros, ce qui correspond au niveau actuel.

La Commission approuve ces modifications qui feront l'objet d'amendements.

Article 4

L'article 4 porte modification de diverses dispositions du Code d'instruction criminelle.

Point 1

L'article 7-4 du Code d'instruction criminelle qui consacre le principe « *aut dedere aut iudicare* » est complété par l'ajout des articles 509-1 à 509-7 du Code pénal sur les infractions en matière informatique.

¹**Art. 509-1.** (L. 14 août 2000) Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros.

Art. 509-2. (L. 15 juillet 1993) Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

Art. 509-3. (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

Art. 509-4. (L. 10 novembre 2006) Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros.

Encourent les mêmes peines, ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction visée à l'alinéa qui précède.

D'un point de vue formel, le Conseil d'Etat relève que la note de bas de page n° 1, qui figure dans le texte qui lui a été transmis et qui renvoie au projet de loi n° 6388, est à omettre compte tenu de la loi du 26 décembre 2012 qui a modifié l'article 7-4.

Le Conseil d'Etat rend encore attentif au fait que l'article 7-4 du Code d'instruction criminelle actuellement en vigueur, tel que modifié en dernier lieu par la loi précitée du 26 décembre 2012, n'a pas été correctement repris. Aussi y-a-t-il 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 décide de suivre le Conseil d'Etat.

Point 2

Les auteurs du projet de loi exposent que pour répondre 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 que le procureur d'Etat puisse demander au juge d'instruction d'ordonner les mesures prévues à l'article 67-1 du Code d'instruction criminelle sans ouvrir une instruction préparatoire.

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 1^{er} de l'article 24-1 du Code d'instruction criminelle et non le point 1 de cet article, ainsi que l'indiquent les auteurs.

Le représentant du Parquet indique 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. Une modification de l'article précité s'impose donc.

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

Point 3

L'article 31 du Code d'instruction criminelle relatif à la saisie en cas de flagrant crime est complété en vue de permettre la saisie de données informatiques. Le Conseil d'Etat approuve cette extension, tout en formulant une observation de fond et une observation de forme.

Il note qu'au 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 ou encore le nouvel article 509-5 du Code pénal, qui ont recours aux concepts de clé 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.

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, adoptant 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.

Selon le représentant du Parquet, il convient 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. Partant, il est préférable, afin de préserver la cohérence des textes, de maintenir cette terminologie.

En ce qui concerne la formule de « données stockées, traitées ou transmises », 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 la communication). Partant, il semble préférable de conserver la terminologie retenue par le projet de loi.

La Commission approuve cette approche.

Point 4

Ce point vise à élargir l'objet de la perquisition prévue à l'article 33 du Code d'instruction criminelle aux données informatiques. Etant donné que ce point est le corollaire du point 3, le Conseil d'Etat 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 1^{er} de l'article 33.

Le nouveau paragraphe 5 vise à permettre la saisie par voie d'établissement d'une copie. 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 le représentant du Parquet, il convient d'appliquer la même logique que pour l'article 31 du Code d'instruction criminelle et 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-dessus.

Au sujet du nouveau paragraphe 5, le représentant du Parquet explique 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. Partant, la décision d'effacement ne peut pas être assimilée à une sanction de confiscation anticipée.

En cas d'acquiescement ou de décision de ne pas procéder à des poursuites, les données saisies 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, ou encore l'incitation à la haine.

Partant, la Commission décide de maintenir le libellé, tel qu'il figure dans le projet de loi.

Point 5

Le point 5 vise à compléter la liste des infractions pour lesquelles une infiltration peut être décidée en incluant les infractions en matière informatique. Le Conseil d'Etat n'a pas d'observation à formuler, sauf à préciser que c'est le paragraphe 1^{er} 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 1^{er} de l'article 48-17 du Code d'instruction criminelle qui est ainsi modifié. Elle décide en outre de supprimer le point 12.

Point 6

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.

Le Conseil d'Etat formule les observations suivantes.

En ce qui concerne le fond, le Conseil d'Etat marque 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 ». S'agissant d'une mesure grave dans le cadre d'une procédure d'enquête, d'instruction ou d'entraide judiciaire en matière pénale, la mesure doit être décidée ou ordonnée par un magistrat et ne saurait être avalisée après coup. Au regard de la disponibilité 24 heures sur 24 de magistrats du parquet et du cabinet d'instruction, on ne saurait avancer des considérations tenant à la perte de temps due à l'intervention des autorités judiciaires. Il y a donc lieu d'écrire « le procureur d'Etat ou le juge d'instruction ... peut faire procéder... ».

La Commission décide de suivre le Conseil d'Etat.

En ce qui concerne la formulation du texte, le Conseil d'Etat renvoie à la suggestion déjà formulée de viser les données informatiques. Il propose, à la fin du texte, d'écrire « ces données » plutôt que de reprendre la formule complexe qui figure déjà au début du libellé.

En ce qui concerne les termes de « données stockées, traitées ou transmises dans un système informatique », il est renvoyé au commentaire sous le point 3 ci-dessus.

Point 7

L'article 66 du Code d'instruction criminelle est modifié pour étendre la saisie ordonnée par le juge d'instruction aux données informatiques. Les modifications proposées sont le corollaire de celles apportées à l'article 33. Le Conseil d'Etat renvoie à ses observations à l'endroit du point 4 y compris pour ce qui est du nouveau point 3 inséré dans l'article 66.

En réponse aux observations du Conseil d'Etat, la Commission renvoie aux commentaires sous le point 4. A l'instar des points 3 et 4, il convient de remplacer les termes « système informatique » par ceux de « système de traitement ou de transmission automatisé de données ».

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.

Le représentant du Parquet 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 coopérante, 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.

Point 8

Le point 8 prévoit la suppression, dans la première phrase du paragraphe 1^{er} 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 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 Code se suffit à elle-même et ne requiert aucune adaptation de l'article 67-1. Il s'agit d'une procédure spécifique permettant justement l'adoption des mesures prévues à l'article 67-1 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, il n'a pas été procédé à une adaptation des dispositions relatives aux actes d'instruction adoptés par le juge d'instruction.

Le représentant du Parquet indique qu'à défaut de supprimer les termes « saisi de faits » dans la première phrase du paragraphe 1^{er} de l'article 67-1, celui-ci est en contradiction avec l'article 24-1 alors que ce dernier renvoie à l'article 67-1. Partant, la Commission décide de maintenir le libellé du projet de loi.

Le Conseil d'Etat propose également d'omettre les adaptations prévues au paragraphe 3 de l'article 67-1, 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 sans qu'il ne faille introduire un renvoi à cette disposition à l'article 67-1. Le Conseil d'Etat reconnaît que se pose la question de l'information de la personne 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 à la suite des modifications proposées au point 2.

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 1^{er} 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. »

Selon le représentant du Parquet, dans la mesure où l'article 24-1 renvoie à l'article 67-1, la solution la plus simple est d'ajouter l'enquête préliminaire au paragraphe 3 de l'article 67-1.

En effet, l'article 67-1 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. 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.

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.

La Commission confirme 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.

D'un point de vue formel et à toutes fins utiles, le Conseil d'Etat rend attentif que les auteurs négligent d'indiquer le paragraphe 1^{er} en début du texte de l'article 67-1 nouveau 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 fait siennes les remarques du Conseil d'Etat.

Article 5

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 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'observation.

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'observation.

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'observation.

Le Conseil d'Etat voudrait néanmoins faire 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 représentant du Parquet explique qu'il a été décidé d'ajouter la référence à l'article 48-25, s'agissant d'un nouvel article. Dans la mesure où le Conseil d'Etat préconise une formule plus générale, cette proposition peut toutefois être retenue en la modifiant comme suit: « autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi ».

Le Conseil d'Etat note enfin que la référence expresse aux articles 88-1 et 88-4 peut être maintenue, parce qu'il ne s'agit pas de dispositions relatives à l'enquête préliminaire ou à la procédure d'instruction.

Lors d'une prochaine réunion, les membres de la Commission se verront présenter une série d'amendements au projet de loi.

2. Approbation des projets de procès-verbal des réunions des 10, 17 et 24 avril 2013

Ce point est reporté à une réunion ultérieure.

3. Divers

Les membres de la Commission décident de convoquer une réunion le 22 mai 2013 à 9h00 avec l'ordre du jour suivant :

- 6446 Proposition de loi relative à la modification de l'article 6 de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire
- Présentation générale
- 6376 Projet de loi portant réforme de la Commission des normes comptables et modification de diverses dispositions relatives à la comptabilité et aux comptes annuels des entreprises ainsi qu'aux comptes consolidés de certaines formes de sociétés et modifiant:
(1) le titre II du livre Ier du Code de commerce
(2) le titre II de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises
(3) la section XVI de la loi modifiée du 10 août 1915 concernant les sociétés commerciales
- Rapporteur: Monsieur Léon Gloden
- Présentation et adoption d'une série d'amendements parlementaires

Luxembourg, le 15 mai 2013

La secrétaire,
Carole Closener

Le Président,
Gilles Roth

Annexe :
Ministère de la Justice : Projet de loi n°6514



Projet de loi n°6514 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, faite 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.**

1. Articles 231 et 231bis du Code pénal

Le projet de loi n° 6514 propose de modifier l'article 231 dans le cadre de l'introduction de l'usurpation d'identité dans le Code pénal conformément à la nouvelle directive européenne sur la cybercriminalité. L'article proposé dans le projet de loi se lit de la façon suivante :

« **Art. 231.-** Quiconque aura publiquement pris un nom, ou une identification de quelque nature qu'elle soit, qui lui appartient pas sera puni d'un emprisonnement de huit jours à ~~trois mois un an~~ et d'une amende de 251 euros à 3000 euros ou d'une de ces peines seulement. »

Il est en outre introduit un nouvel article 231bis qui est libellé comme suit :

« **Art. 231bis.-** Quiconque dans le but de troubler la tranquillité d'un tiers, ou dans le but de porter atteinte à la mœurs ou à la considération d'un tiers, aura pris un nom ou une identification de quelque nature qu'elle soit qui lui appartient pas sera puni d'un emprisonnement de trois mois à 2 ans et d'une amende de 251 euros à 3000 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. »

Lors de la réunion de la commission juridique du 8 mai 2013 des réserves ont été émises par les membres de la commission contre la nouvelle formulation de l'article 231 concernant le fait que dans cet article (1) il n'y a pas d'élément intentionnel explicitement mentionné (intention de nuire), (2) la peine a été augmentée et (3) il n'y a pas, comme à l'article 231bis, la nécessité d'une plainte de la victime.

Les auteurs du texte ont expliqué que les modifications à l'article 231 avaient été faites surtout pour l'aligner sur le nouvel article 231bis et pour prendre en considération la position actuelle de

la jurisprudence luxembourgeoise. Etant donné les réserves exprimées les auteurs du texte proposent de n'apporter aucun changement à l'article 231 du Code pénal et partant de modifier le projet de loi existant par la voie d'un amendement grand-ducal en ce sens.

L'article 231bis sur lequel un consensus s'est dégagé sera maintenu dans sa forme actuelle.

2. Nouvelle version de l'article 506-1 du Code pénal.

Les remarques du Conseil d'Etat au point 5 de son avis du 16 avril 2013 sont prises en compte et l'article 506-1 est rédigé de la façon suivante :

Art. 506-1. (L. 12 août 2003) Sont punis d'un emprisonnement d'un à cinq ans et d'une amende de 1.250 euros à 1.250.000 euros, ou de l'une de ces peines seulement:

1) (L. 27 octobre 2010) 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,

- (L. 27 octobre 2010) (L. 26 décembre 2012) 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;

- (L. 21 juillet 2012) d'une infraction aux articles 368 à 370, 379, 379bis, 382-1, 382-2, **382-4 et 382-5** du Code pénal;

- (L. 12 novembre 2004) 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;

- (L. 17 juillet 2008) d'une infraction aux articles 184, 187, 187-1, 191 et 309 du Code pénal;

- (L. 17 juillet 2008) d'une infraction aux articles 463 et 464 du Code pénal;

- (L. 17 juillet 2008) 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 ;

- (L. 17 juillet 2008) 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;

- (L. 17 juillet 2008) d'une infraction à l'article 5 de la loi du 11 janvier 1989 réglant la commercialisation des substances chimiques à activité thérapeutique;

- (L. 17 juillet 2008) d'une infraction à l'article 18 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine;

- **(L. 21 juillet 2012) d'une infraction à l'article 382-4 du Code pénal;**

- (L. 17 juillet 2008) d'une infraction aux articles 82 à 85 de la loi du 18 avril 2001 sur le droit d'auteur;

- (L. 17 juillet 2008) 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;

- (L. 17 juillet 2008) 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;

- (L. 17 juillet 2008) d'une infraction à l'article 25 de la loi modifiée du 10 juin 1999 relative aux établissements classés;
 - (L. 17 juillet 2008) d'une infraction à l'article 26 de la loi du 29 juillet 1993 concernant la protection et la gestion de l'eau;
 - (L. 17 juillet 2008) 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;
 - (L. 17 juillet 2008) d'une infraction aux articles 220 et 231 de la loi générale sur les douanes et accises;
 - (L. 17 juillet 2008) d'une infraction à l'article 32 de la loi du 9 mai 2006 relative aux abus de marché;
 - (L. 17 juillet 2008) 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;
- 2) (L. 27 octobre 2010) ceux qui ont sciemment apporté leur concours à une opération de placement, de dissimulation, de déguisement, de transfert ou de conversion des biens visés à l'article 32-1, alinéa premier, sous 1), formant l'objet ou le produit, direct ou indirect, des infractions énumérées au point 1) de cet article ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions;
- 3) (L. 13 mars 2009) ceux qui ont acquis, détenu ou utilisé des biens visés à l'article 32-1, alinéa premier, sous 1), formant l'objet ou le produit, direct ou indirect, des infractions énumérées au point 1) de cet article ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions, sachant, au moment où ils les recevaient, qu'ils provenaient de l'une ou de plusieurs des infractions visées au point 1) ou de la participation à l'une ou plusieurs de ces infractions. (L. 27 octobre 2010)
- 4) La tentative des infractions prévues aux points 1 à 3 ci-avant est punie des mêmes peines.



Session ordinaire 2012-2013

CC/pk

P.V. J 33

Commission juridique

Procès-verbal de la réunion du 08 mai 2013

Ordre du jour :

1. 6550 Projet de loi modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat
- Rapporteur: Monsieur Gilles Roth
- Présentation et adoption d'un projet de rapport
2. 6514 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
- Rapporteur: Monsieur Gilles Roth
- Continuation de l'examen du projet de loi et de l'avis du Conseil d'Etat
3. Approbation des projets de procès-verbal des réunions des 10, 17 et 24 avril 2013
4. Divers

*

Présents : M. Marc Angel, M. Xavier Bettel, M. Alex Bodry, M. Félix Braz, Mme Christine Doerner, M. Léon Gloden, M. Jacques-Yves Henckes, M. Jean-Pierre Klein, M. Paul-Henri Meyers, Mme Lydie Polfer, M. Gilles Roth

Mme Octavie Modert, Ministre de la Justice
Mme Anne Ketter, M. Laurent Thyès, du Ministère de la Justice
M. Gilles Herrmann, du Parquet de Luxembourg

Mme Carole Closener, de l'Administration parlementaire

Excusé : M. Lucien Weiler

*

Présidence : M. Gilles Roth, Président de la Commission

*

Dans une remarque préliminaire, le Président de la Commission juridique souhaite, au nom de tous les membres, la bienvenue à Madame la Ministre de la Justice, à l'occasion de la première réunion à laquelle elle assiste dans ses nouvelles fonctions.

Il rappelle que les travaux de la Commission sont toujours guidés par la recherche d'un consensus.

En réponse à M. Gilles Roth, Madame la Ministre indique à son tour se réjouir à l'avance de la bonne coopération entre son ministère et la Commission. Sans établir de liste de priorités, elle rappelle la multiplicité et la diversité des différents projets de loi renvoyés à la Commission dont il conviendrait idéalement d'évacuer un certain nombre avant la fin de la législature.

Le représentant du groupe parlementaire DP, tout en rappelant l'existence d'un consensus sur le mariage, manifeste son souhait de concentrer les travaux parlementaires sur le projet de réforme du mariage.

1. 6550 Projet de loi modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat

L'adoption de ce projet de rapport, initialement prévue le 24 avril 2013, a été reportée à la présente réunion, étant donné que le document a fait l'objet de quelques modifications complémentaires.

Le projet de rapport, pour les détails duquel il est prié de se référer au document envoyé par courrier électronique le 24 avril 2013, est adopté à la majorité des voix moins une abstention (M. X. Bettel).

Les membres de la Commission proposent de porter le projet de loi à l'ordre du jour de la séance plénière du 14 mai 2013.

2. 6514 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**

Dans la continuité de la réunion du 24 avril 2013, les membres de la Commission reprennent l'examen du projet de loi et de l'avis du Conseil d'Etat.

Article 3

Points 1 et 2

Les représentants du Ministère de la Justice et du Parquet exposent le document annexé, réalisé à la demande des membres de la Commission, contenant des tableaux synoptiques, des jurisprudences et des explications. Pour les détails, il est prié de se référer à l'annexe, diffusée par courrier électronique le 2 mai 2013.

Le représentant du Parquet rappelle brièvement que la disposition de l'article 231, tel qu'il est proposé de la modifier, vise à étendre l'usurpation publique de nom à « toute identification de quelque nature qu'elle soit ». La disposition nouvelle de l'article 231*bis* vise, quant à elle, à introduire l'usurpation de nom ou d'identité en vue de nuire à un tiers. En revanche, le fait d'utiliser un ou plusieurs pseudonymes ne permettant pas l'identification d'une autre personne n'est pas punissable.

C'est la plainte de la victime qui déclenche la poursuite du délit.

Le libellé de l'article 231 suscite une série d'interrogations de la part des membres de la Commission, dont notamment :

- L'article 231 paraît très strict, dans la mesure où l'intention de nuire n'est pas expressément prévue alors que la peine d'emprisonnement peut atteindre un an.
- Le texte français, quant à lui, prévoit l'intention de nuire.
- De plus le délit peut être poursuivi en l'absence de plainte.
- Le fait de spécifier que c'est l'usurpation publique de nom ou d'identité « per se » qui est incriminée permettrait de clarifier le texte.

En réponse à ces interventions, le représentant du Parquet indique que :

- La jurisprudence exige que l'usurpation de nom, dans le cadre de l'article 231, soit commise avec l'intention de nuire. L'article 231 vise l'usurpation « publique ». Par ailleurs la peine d'emprisonnement est moins lourde que celle prévue à l'article 231*bis* (qui peut aller jusqu'à trois ans).
- L'article 231 ne vise pas les artistes qui mènent leur carrière (de peintre ou d'écrivain, par exemple) sous un pseudonyme, ni les agents spéciaux qui prennent une « couverture » pour mener à bien leur mission, dans la mesure où c'est l'« usurpation » qui est visée, et non pas la simple utilisation.

Mme la Ministre suggère de ne pas modifier, outre mesure, les libellés des articles 231 et 231*bis*. Si dans l'article 231, le remplacement des termes « identification de quelque nature que ce soit » par celui d'« identifiant » peut être envisagé, il ne paraît cependant pas souhaitable de reprendre la formulation du Code pénal français « données permettant d'identifier une autre personne », dans la mesure où le texte français suscite de nombreuses difficultés d'interprétation.

Elle propose d'analyser les différentes remarques exprimées par les membres de la Commission et d'y répondre au cours d'une réunion ultérieure.

Point 3

Le point 3 modifie les peines prévues à l'article 488 du Code pénal. Le Conseil d'Etat n'a pas d'observation particulière.

Point 4

Le Conseil d'Etat note qu'il est proposé de compléter l'article 496 du Code pénal par l'ajout, à la liste des objets remis ou délivrés, des clés électroniques. Il comprend le souci des auteurs qui font état d'un arrêt de la Cour d'appel n° 261/10 X du 14 juin 2010 dont il résulterait que l'article 496, dans sa teneur actuelle, ne permet pas d'appréhender « l'hameçonnage d'un mot de passe (en anglais « phishing ») ».

Il constate cependant 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 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.

De plus, le maintien du libellé de l'article 496, tel qu'il ressort du projet de loi, implique une 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 clé 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 il a rendu son avis le 12 mars 2012. Ce texte propose de remplacer le concept de marchandises par ceux de « bien corporel fongible » et d'ajouter une référence au « bien incorporel fongible ». Selon le Conseil d'Etat, 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.

Le Conseil d'Etat relève encore une certaine incohérence dans l'approche des auteurs du projet de loi qui, au point 4, retiennent le seul concept de clé électronique et, au point 8 relatif au nouvel article 509-5, visent le « mot de passe », le « code d'accès » ou « toute autre clé électronique ». Partant, le Conseil d'Etat recommande de retenir une même terminologie pour les deux textes. Il renvoie, dans ce contexte, à l'article 488 du Code pénal qui consacre déjà le concept de clé 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 décide de suivre le Conseil d'Etat en retenant la terminologie de « clé électronique » et en ajoutant cette notion dans la définition des objets visés aux articles 461, 470 ou 491 du Code pénal.

Quant à la terminologie du nouvel article 509-5, les termes « mot de passe » et « code d'accès » étaient cités à titre d'exemples. Les membres de la Commission conviennent de supprimer ces exemples du libellé et de retenir le seul terme de « clé électronique ». Dans le commentaire des articles, il sera précisé que la notion de « clé électronique » englobe les notions de mot de passe et de code d'accès.

Point 5

Sous le point 5, il est prévu de compléter l'article 506-1 du Code pénal sur le blanchiment en ajoutant à la liste des infractions primaires une série d'infractions nouvelles en matière informatique. Dans son avis du 16 avril 2013, le Conseil d'Etat relève le caractère extrêmement succinct du commentaire qui ne donne aucune indication des ajouts apportés à

l'article 506-1; seule une lecture comparée du texte actuel avec l'article tel que modifié permet de mettre en évidence les compléments apportés au texte actuel de l'article 506-1. Le Conseil d'Etat relève encore que la plupart des ajouts ne concernent en rien les nouvelles infractions en matière informatique et que la volonté des auteurs semble plutôt être d'étendre la liste des infractions primaires en matière de blanchiment. Il renvoie à la proposition qu'il a faite dans les considérations générales de son avis. Il indique par ailleurs que le texte proposé ne tient pas compte des modifications que la loi du 21 juillet 2012 (trafic illicite de migrants par terre, air et mer) a apportées à l'article 506-1 précité. Comme le relève le Conseil d'Etat, le troisième tiret du texte proposé omet de renvoyer aux articles 382-4 et 382-5 du Code pénal, et le dix-septième tiret 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. L'article 143 a d'ailleurs été abrogé par la loi précitée du 21 juillet 2012. La référence prévue au prédit treizième tiret dans sa formulation actuellement en vigueur peut d'ailleurs utilement être supprimée, alors qu'elle fait double emploi avec le troisième tiret, également introduit par la loi de 2012.

En réponse aux remarques ci-dessus, le représentant du Parquet rappelle que l'objet du point 5 était d'inclure les infractions aux articles 509-1 à 509-7 dans la liste des infractions primaires.

La modification du point 5, visant à tenir compte des observations du Conseil d'Etat, devra faire l'objet d'un amendement.

Point 6

Le point 6 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 note qu'au concept de données est ajouté le qualificatif « informatiques » qui ne figure pourtant pas dans les autres articles de la section VII relative aux « infractions en matière électronique ». Le Conseil d'Etat s'interroge encore sur la nécessité de la partie finale de la disposition nouvelle « ou (système) de transmission automatisé de données ». Outre le problème que le terme de transmission est utilisé à deux reprises, une fois pour qualifier l'opération et une fois pour décrire le système, ce qui n'est pas très logique, le respect de l'article 3 de la Convention est, de l'avis du Conseil d'Etat, garanti même si ce bout de phrase est omis. Le Conseil d'Etat a constaté que l'article 3 de la Convention vise le système informatique en tant que tel sans distinguer entre l'aspect traitement et transmission, la transmission étant au demeurant également un traitement. Une solution plus simple encore serait de reprendre tel quel le texte de la Convention et de viser le système informatique. Enfin, le Conseil d'Etat relève que la tentative est spécialement prévue, alors que tel n'est pas le cas pour les dispositions actuelles qui ne subiront pas de changement. La Convention n'impose d'ailleurs pas expressément d'incriminer la tentative. Eu égard à ces observations, le Conseil d'Etat propose de reprendre le texte de l'article 3 de la Convention. L'alinéa 2 de l'article 509-3 du Code pénal aurait ainsi la teneur suivante:

« Est puni des mêmes peines l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. »

(ad. Considérations générales)

A la question de savoir pourquoi les auteurs du projet de loi n'ont pas opté pour une intégration des infractions liées à la cybercriminalité dans la section spécifique du Code pénal (« De certaines infractions en matière informatique »), le représentant du Parquet

réplique que la cybercriminalité est très vaste : d'un côté elle comprend les infractions spécifiques aux ordinateurs, de l'autre côté elle englobe toutes les infractions commises dans le passé à l'aide de moyens classiques (par exemple une lettre), mais désormais commises par des moyens informatiques (par exemple un courriel). Partant il paraissait préférable d'adapter la législation actuelle ayant déjà fait ses preuves.

En réponse aux observations du Conseil d'Etat, le représentant du Parquet indique que la Convention, dans son article 11, prévoit la tentative. En revanche, il est envisageable de supprimer les termes « ou tenté d'intercepter », dans la mesure où l'article 509-6 incrimine la tentative générale.

L'orateur explique par ailleurs que les auteurs du projet de loi ont décidé de reprendre les termes « données informatiques » (et non pas « données »), étant donné qu'ils correspondent à la terminologie de la Convention. Quant au choix des termes « système de transmission automatisé de données », il s'explique par le fait que cette terminologie correspond à celle déjà utilisée dans les articles 509-1 à 509-7.

Point 7

Le Conseil d'Etat note que la suppression de l'alinéa 2 de l'article 509-3 faisant l'objet du point 7 s'explique par le point 8.

3. Approbation des projets de procès-verbal des réunions des 10, 17 et 24 avril 2013

Ce point est reporté à une réunion ultérieure.

4. Divers

Les membres de la Commission décident de poursuivre l'examen du projet de loi 6514 lors de la prochaine réunion qui aura lieu le 14 mai 2013 à 9h00.

Luxembourg, le 8 mai 2013

La secrétaire,
Carole Closener

Le Président,
Gilles Roth

Annexe :

Ministère de la Justice : Projet de loi n°6514 – tableaux synoptiques



Projet de loi n° 6514 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.

1. Tableau synoptique : usurpation d'identité

Texte du projet de loi	Texte français	Texte belge	Texte de la directive
<p>Art. 3.- Le Code pénal est modifié et complété comme suit :</p> <p>1) L'article 231 du Code pénal est modifié comme suit :</p> <p>« Quiconque aura publiquement pris un nom, <u>ou une identification de quelque nature qu'elle soit</u>, qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois <u>un an</u>, et d'une amende de 251 euros à 3.000</p>	<p>Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.</p> <p>Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un</p>	<p>La Belgique n'a pas de texte.</p>	<p>Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing personal data of another person, with the aim of gaining trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with relevant provisions of national law, be</p>

<p>euros, ou d'une de ces peines seulement. ».</p> <p>2) Il est introduit un article 231bis du Code pénal libellé comme suit :</p> <p><u>«Art. 231bis.- 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 une identification de quelque nature qu'elle soit, 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.</u></p> <p><u>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. ».</u></p>	<p>réseau de communication au public en ligne.</p>		<p>regarded as aggravating circumstances, unless these circumstances are already covered by another offence, punishable under the national legislation.</p>
--	--	--	---

2. Jurisprudences et explications

Le Conseil d'Etat estime que la prise d'un faux nom ou d'un faux identifiant dans des rapports particuliers ne serait pas visée par l'article 231 du Code pénal, la publicité faisant défaut.

Ce n'est cependant pas **la position de la jurisprudence luxembourgeoise**. En effet, « *la publicité exigée par l'article 231 du Code pénal existe si la prise de faux nom se réalise verbalement ou se manifeste dans un écrit ou un imprimé. « Le législateur se contente (...) à cet égard d'une publicité relative, le port du faux nom devant se faire ostensiblement »* (Cour d'appel, 16 juin 2009, n°312/09 V ; voir également Trib. arr. Lux., 30 septembre 2004, n°2643/2004, confirmé par Cour d'appel, 1^{er} février 2005, n°57/05 V.)

La jurisprudence a notamment retenu que l'utilisation d'un faux nom lors de l'inscription dans les fichiers d'un hôtel et lors de retraits d'espèces constitue l'infraction prévue par l'article 231 du Code pénal. (Trib. Arr. Lux., 30 septembre 2004 précité) Il en va de même pour l'utilisation frauduleuse de la carte de crédit et du nom y indiqué d'autrui, (Trib. Arr. Lux., 5 mars 2009, n°776/2009, LJUS 99865668) ainsi que de l'inscription sous le nom d'autrui dans les réseaux sociaux ou l'utilisation de ce nom pour ouvrir des boîtes de courrier électronique. (Trib. Arr. Lux., 5 avril 2011, n°1238/2011) » (Journal des tribunaux Luxembourg 2011, Doctrine, p.151)

La jurisprudence interprète la notion de « public » de manière très large. « *Il est admis que la publicité du port de faux nom est un élément de fait laissé à l'appréciation du juge du fond* » (Cass., 6.2.1939, R.D.P., 1939, 623 ; J.Nypels, Législ. Crim., II, p.255, no55). « *A) a utilisé le nom de B) pour s'identifier à l'égard de ses correspondants. L'utilisation du faux nom était suffisamment extériorisée pour être qualifié de public.* » (Trib. arr. Lux., 21 juin 2012, n°2234/2012) De même, « *(...) l'existence du délit de port de faux nom (...) n'est subordonnée qu'à la condition que le port illicite de faux nom ait eu lieu publiquement* » (CA 4 juin 1956, P.16, 488). « *En l'espèce X.) s'était, suite à une annonce de vente d'un immeuble publiée par A.) sur Internet, mis en contact avec ce dernier et se présenta sous le nom de Y.). Lors de tous les entretiens subséquents tant avec A.) qu'avec son épouse B.), le prévenu avait pris le nom de Y.). Dans la mesure où le nom de Y.) n'est pas le vrai nom du prévenu et qu'il l'a utilisé publiquement en se présentant sous ce nom dès le premier contact téléphonique avec A.) jusqu'à la perpétration de l'infraction d'escroquerie le 11 mai 2007, l'infraction est établie tant en fait qu'en droit.* » (Trib. Arr. Lux., 20 mai 2009, n°1565/2009)

Le texte, tel que proposé par les auteurs permet donc, à la vue de la jurisprudence constante, de rencontrer les problèmes visés dans le commentaire, de même que le cas de figure de l'utilisation d'un matricule qui n'appartient pas à celui qui l'utilise, cas de figure auquel les auteurs avaient pensé, mais qui a été oublié de mentionner dans le commentaire.

Ainsi, le fait de s'identifier avec un certificat Lux-Trust, ou un matricule, ou tout autre identifiant qui n'appartient pas à celui qui l'utilise, vis-à-vis d'une administration étatique ou d'un co-contractant, en vertu de la jurisprudence sus-énoncée, serait ainsi un port « *public* » d'un faux nom, respectivement d'un faux identifiant.

Les termes « *identification de quelque nature que ce soit* » avaient été choisis à dessein pour leur généralité, afin de ne pas exclure un identifiant. L'intention des auteurs est d'exiger que le nom, respectivement l'identifiant, permettent une identification effective, mais fautive, de celui qui l'utilise.

Si « Marc Schmit » utilise le nom de « Daniel Weber », il utilise un nom qui ne lui appartient pas et fait donc une « usurpation » d'identité et tout un chacun va penser qu'il a à faire à « Daniel Weber ». L'infraction de port public de faux nom est donc établie.

Si le même « Marc Schmit » utilise, au lieu du nom « Daniel Weber », le matricule d'un « Daniel Weber », le certificat Lux-Trust d'un « Daniel Weber », voire même un nom d'utilisateur combiné à un mot de passe l'identifiant comme « Daniel Weber », il n'y a pas de port public de faux nom sous la version actuelle du texte et suivant la jurisprudence qui exige l'usurpation d'un nom patronymique. Il est vrai que ces faits peuvent le cas échéant être punis par d'autres articles du Code pénal s'ils constituent un élément constitutif de l'infraction de faux ou de l'escroquerie par exemple. Cependant si « Marc Schmit » n'a pas l'intention de commettre une de ces infractions, mais uniquement d'usurper l'identité de « Daniel Weber » afin de ne pas être identifié comme « Marc Schmit », les faits ne sont pas punis actuellement.

L'utilisation d'un certificat Lux-Trust, ou d'un matricule, ou tout autre identifiant qui n'appartient pas à celui qui l'utilise, permet donc également une identification, mais fautive, de celui qui l'utilise et devrait en conséquence être sanctionnée de la même façon que l'utilisation d'un faux nom.

Il est tout-à-fait possible de remplacer les termes « *identification de quelque nature que ce soit* » par le seul mot « *identifiant* » tel que proposé par le Conseil d'Etat, tout en précisant dans le commentaire des articles que par ce mot est visée toute identification d'une personne autre que celui qui l'utilise et que l'identifiant peut être corporel ou incorporel.

Il est encore à noter qu'un pseudonyme peut aussi être un identifiant, mais qu'il faut bien distinguer entre un pseudonyme que l'on se donne pour ne pas faire apparaître sa véritable identité d'un côté et l'usurpation d'un pseudonyme d'un tiers de l'autre. En effet, si « Marc Schmit » se fait appeler dans un blog internet « Mickey », alors il ne commet pas l'infraction de port public de faux nom puisqu'il s'agit premièrement de « son » pseudonyme et non pas d'un pseudonyme « ne lui appartenant pas » et deuxièmement d'un pseudonyme non identifiant. Par contre, si « Marc Schmit » se fait appeler dans le même blog « Fausti », pseudonyme bien connu au Luxembourg qui ne lui appartient pas et identifiant une personne déterminée, alors il commet l'infraction de port public d'un identifiant ne lui appartenant pas.

En ce qui concerne **la proposition du Conseil d'Etat de reprendre la formulation du Code pénal français**, le libellé de ce texte pose problème à plusieurs niveaux.

Tout d'abord, comme l'écrit Madame Agathe LEPAGE, professeur à l'université Panthéon-Assas, dans son étude sur « Le délit d'usurpation d'identité : questions d'interprétation » publiée dans « La Semaine Juridique Edition Générale n°35, 29 Août 2011, doct. 913, « La rédaction sinueuse de l'incrimination et les notions riches de sens qu'elle contient débouchent sur un certain nombre de questions d'interprétation. »

Il est donc laissé à la jurisprudence d'interpréter les termes « d'usurpation d'identité », « troubler la tranquillité » et « atteinte à la considération ».

Ensuite il faut se demander pourquoi rajouter un deuxième alinéa au texte pour viser spécialement FACEBOOK (et autres réseaux similaires), alors qu'il n'y a aucune raison de penser que ces réseaux ne seraient pas visés par le premier alinéa. Cette critique est également partagée par Madame LEPAGE dans son étude lorsqu'elle regrette « l'existence du second alinéa, qui persiste à parler, **pour ne rien dire**, de l'internet ».

Finalement le texte français va beaucoup moins loin que celui proposé par les auteurs et ne couvre pas tous les cas de figure d'usurpation d'identité. En effet l'usurpation d'identité « per se » n'est pas visée par le texte français, mais par contre par la nouvelle rédaction de l'article

231 du Code pénal. Le texte français incrimine d'un côté l'usurpation d'identité si elle est commise en vue de porter atteinte à l'honneur ou à la considération de la personne dont l'identité est usurpée, mais d'un autre côté ne l'incrimine pas si elle commise en vue de porter atteinte à l'honneur ou à la considération d'un tiers. Pourquoi ?

Les nouveaux textes proposés incriminent de leur côté :

- L'usurpation **publique** de nom ou d'identité **per se** (Article 231 Code pénal) (Dans ce cas c'est l'atteinte à la sécurité juridique qui est réprimée)
- L'usurpation de nom ou d'identité **en vue de nuire** à un tiers (qu'il s'agisse de la personne dont l'identité est usurpée ou non, peu importe) (Article 231 bis Code pénal) (Dans ce cas c'est l'intention de nuire à autrui qui est réprimée)

Ainsi tous les cas de figure d'usurpation d'identité (en dehors de ceux qui existent déjà pour le faux ou l'escroquerie notamment) devraient être couverts.

Précisons une dernière fois pour être très clair : Le fait de se donner un ou plusieurs pseudonymes n'identifiant pas une autre personne n'est pas punissable !

Quant à la dernière interrogation du Conseil d'Etat sous le Point 1 de l'article 3, il est renvoyé d'abord à l'article 232bis du Code pénal qui punit en partie l'usage frauduleux y visé, de même qu'aux articles 275 et suivants du Code pénal qui punissent l'outrage à corps constitué. Dans les autres cas de figure imaginables il semble qu'un tel usage frauduleux serait fait en vue de commettre soit une escroquerie, soit un faux, et serait dans ces cas un élément constitutif de ces infractions.

3. Tableau synoptique : escroquerie

FRANCE	BELGIQUE	LUXEMBOURG	TEXTE PROPOSE
<p>Code pénal français</p> <p>Section 1 : De l'escroquerie.</p> <p>Article 313-1</p> <p>L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.</p> <p>L'escroquerie est punie de cinq ans d'emprisonnement et de 375000 euros d'amende.</p> <p>Article 313-2</p> <p>Les peines sont portées à sept ans d'emprisonnement et à 750000 euros d'amende lorsque l'escroquerie est réalisée :</p> <p>1° Par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, dans l'exercice ou à l'occasion de</p>	<p>Code pénal belge</p> <p>SECTION III. - DE L'ESCROQUERIE ET DE LA TROMPERIE.</p> <p>Art. 496. Quiconque, dans le but de s'approprier une chose appartenant à autrui, se sera fait remettre ou délivrer des fonds, meubles, obligations, quittances, décharges, 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 d'un mois à cinq ans et d'une amende de vingt-six [euros] à trois mille [euros].</p> <p>[¹ Si les faits visés à l'alinéa précédent ont été commis au préjudice d'une personne dont la situation de vulnérabilité en</p>	<p>Code pénal luxembourgeois</p> <p>Section III. - De l'escroquerie et de la tromperie.</p> <p>Art. 496. 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, 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 d'un mois à cinq ans et d'une amende de 251 euros à 30.000 euros.</p> <p>Le coupable pourra de plus être condamné à l'interdiction, conformément à l'article 24.</p>	<p>Art. 496. 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 d'un <u>quatre</u></p>

<p>l'exercice de ses fonctions ou de sa mission ;</p> <p>2° Par une personne qui prend indûment la qualité d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ;</p> <p>3° Par une personne qui fait appel au public en vue de l'émission de titres ou en vue de la collecte de fonds à des fins d'entraide humanitaire ou sociale ;</p> <p>4° Au préjudice d'une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de son auteur.</p> <p>Les peines sont portées à dix ans d'emprisonnement et à 1 000 000 Euros d'amende lorsque l'escroquerie est commise en bande organisée.</p> <p>Article 313-3</p> <p>La tentative des infractions prévues par la présente section est punie des mêmes peines.</p> <p>Les dispositions de l'article 311-12 sont applicables au délit</p>	<p>raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits, celui-ci sera puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six euros à trois mille euros.]¹</p> <p>(La tentative du délit prévu par l'alinéa 1 sera punie d'un emprisonnement de huit jours à trois ans et d'une amende de vingt-six [euros] à deux mille [euros].)</p> <p>(Dans les cas prévu par les alinéas précédents, le coupable pourra, de plus, être condamné à l'interdiction, conformément à l'article 33.)</p>		<p><u>mois</u> à cinq ans et d'une amende de 251 euros à 30.000 euros. »</p>
--	--	--	--

d'escroquerie.			
----------------	--	--	--



Commission juridique

Procès-verbal de la réunion du 24 avril 2013

Ordre du jour :

1. 5974 Projet de loi modifiant la loi modifiée du 10 août 1915 concernant les sociétés commerciales en vue de mettre en œuvre le Règlement (CE) no 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)
 - Rapporteur: Monsieur Léon Gloden
 - Présentation et adoption d'une série d'amendements
2. 6514 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
 - Rapporteur: Monsieur Gilles Roth
 - Présentation du projet de loi
 - Examen de l'avis du Conseil d'Etat
3. 6550 Projet de loi modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat
 - Rapporteur: Monsieur Gilles Roth
 - Présentation et adoption d'un projet de rapport
4. Divers

*

Présents : M. Marc Angel, M. Xavier Bettel, M. Félix Braz, Mme Christine Doerner, M. Léon Gloden, M. Jacques-Yves Henckes, M. Jean-Pierre Klein, M. Paul-Henri Meyers, Mme Lydie Polfer, M. Gilles Roth

Mme Marie-Anne Ketter, M. Daniel Ruppert, M. Laurent Thyès, du Ministère de la Justice

M. Gilles Herrmann, Substitut principal, Parquet de Luxembourg

Mme Carole Closener, de l'Administration parlementaire

Excusés : M. Alex Bodry, M. Lucien Weiler

*

Présidence : M. Gilles Roth, Président de la Commission

*

1. 5974 Projet de loi modifiant la loi modifiée du 10 août 1915 concernant les sociétés commerciales en vue de mettre en œuvre le Règlement (CE) no 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)

Présentation et adoption d'une série d'amendements

Le rapporteur du projet de loi présente aux membres de la Commission une série d'amendements pour le détail desquels il est prié de se référer au document diffusé par courrier électronique le 19 avril 2013, et annexé au présent procès-verbal.

En complément des amendements figurant dans ce document, il y a lieu de compléter à l'article 137-58 les termes « réviseurs d'entreprises » par le terme « agréées ». Il semble en effet préférable d'utiliser les termes « réviseurs d'entreprises agréés désignés » dans la mesure où il s'agit de la terminologie qui a été retenue pour la transformation de la société européenne suite à l'adoption de la loi du 18 décembre 2009 relative à la profession de l'audit ayant modifié l'art. 31-3 (3) de la loi modifiée du 10 août 1915 concernant les sociétés commerciales.

Cette modification fera l'objet d'un amendement supplémentaire.

Les amendements sont adoptés à l'unanimité.

2. 6514 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**

Présentation du projet de loi

Le projet de loi, tel que décrit en détail par l'exposé des motifs du document parlementaire afférent, a pour objectif de renforcer la lutte contre la cybercriminalité, c'est-à-dire les actes de délinquance commis à l'aide des nouvelles technologies, (i) en ratifiant la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 ainsi que son Protocole additionnel du 28 janvier 2003 relatif à l'incrimination d'actes de nature raciste et xénophobe

commis par le biais de systèmes informatiques et (ii) en apportant les changements nécessaires à la législation luxembourgeoise pour la mettre en conformité avec la Convention et son Protocole additionnel.

Examen de l'avis du Conseil d'Etat

Le rapporteur du projet de loi, M. Gilles Roth, présente l'avis du Conseil d'Etat du 16 avril 2013, pour les détails duquel il est prié de se référer au document parlementaire afférent.

Le Conseil d'Etat relève que, selon l'exposé des motifs, dans un avenir très proche sera adoptée une directive de l'Union européenne en la matière et que cette directive sera donc «transposée avant la lettre dans le cadre du présent projet de loi ». Le Conseil d'Etat a déjà eu l'occasion de souligner 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, ce qui oblige le législateur national à des adaptations successives de son dispositif légal. Le Conseil d'Etat se demande si une loi globale et unique couvrant les trois instruments européens, la Convention, le Protocole et la directive, n'aurait pas été plus appropriée.

Le Conseil d'Etat relève par ailleurs 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 fût 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 regroupe les dispositions des articles 3 à 5.

En réponse à ces observations, le représentant du Ministère de la Justice indique que le Gouvernement a volontairement choisi de regrouper toutes les dispositions en un seul projet de loi, en vue de donner une certaine visibilité à la lutte contre la cybercriminalité.

Quant à la première remarque du Conseil d'Etat, il convient de préciser que la proposition de directive a d'ores et déjà été formellement adoptée par le Conseil de l'UE, le texte définitif attend simplement le feu vert du PE. La directive vise à remplacer la décision-cadre 2005/222/JAI relative aux attaques visant les systèmes d'information et se base sur la Convention du Conseil de l'Europe de 2001.

Il s'en suit que l'évacuation du projet de loi sous rubrique en l'état ne saurait remettre en cause la continuité et la sécurité juridique.

Articles 1^{er} et 2

Ces articles portent approbation de la convention et du protocole additionnel précités. Ils n'appellent pas d'observation.

Article 3

L'article 3 porte modification de toute une série de dispositions du Code pénal. Le Conseil d'Etat relève d'emblée que la plupart de ces modifications ont une portée autonome et ne sont pas liées à l'approbation de la convention précitée. Il renvoie à l'observation qu'il a faite dans les considérations générales.

Point 1

Sous le point 1, il est proposé de compléter l'article 231 actuel du Code pénal sur l'usurpation de nom par une référence à une « identification de quelque nature qu'elle soit ». Les auteurs exposent qu'il résulte de la jurisprudence que l'article 231, dans sa

teneur actuelle, ne permet pas de sanctionner l'usage de certificats type Luxtrust qui confèrent une identification d'une personne à une administration. Les auteurs exposent encore s'être inspirés de l'article 226-4-1 du Code pénal français figurant dans une section relative à « l'atteinte à la vie privée ».

Le Conseil d'Etat note, d'abord, que le texte tel que proposé ne permet pas de rencontrer tous les problèmes visés dans le commentaire. En effet, l'utilisation d'une signature électronique, d'un certificat type Luxtrust ou d'un identifiant numérique dans des relations commerciales ou bancaires s'inscrit dans des rapports particuliers avec l'entité qui a décerné ou accepté l'identifiant; il ne s'agit toutefois pas de la prise publique illicite d'une identification dès lors que l'usage frauduleux s'inscrit dans des rapports particuliers. Le Conseil d'Etat note encore que ce type de comportement est souvent sanctionné par le biais de l'infraction de faux. Le seul cas de figure couvert, mais qui n'est pas visé dans le commentaire, est l'utilisation d'un matricule national d'autrui. Se pose, par ailleurs, la question de savoir si un identifiant, plus ou moins abstrait, qu'une personne s'est donné à elle-même, en particulier dans le secteur de l'Internet et qui ne revêt pas une fonction d'identification par un opérateur qui décerne ou accepte l'identifiant, est à protéger.

Le Conseil d'Etat relève de même le caractère vague des termes « identification de quelque nature que ce soit ». L'incrimination d'actes par le biais de formules aussi peu précises n'est à tout le moins pas heureuse. Si le texte, malgré les interrogations formulées ci-dessus, devait être maintenu, il y aurait lieu d'écrire « identifiant » ou de reprendre la formulation du Code pénal français « données permettant d'identifier une autre personne ». Le Conseil d'Etat comprend que l'article 231*bis* nouveau, qui se réfère sans distinction au « tiers », vise la protection des personnes physiques et morales. Enfin, le Conseil d'Etat se demande ce qu'il en est de l'usage injustifié ou frauduleux, de la dénomination ou de l'intitulé officiel d'organes publics qui ne constituent pas des personnes juridiques différentes de l'Etat ou d'une commune.

Point 2

Le Conseil d'Etat rappelle que le nouvel article 231*bis* 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, 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, qui porte sur les atteintes à l'honneur et à la considération des personnes.

*

En réponse à ces observations, le représentant du Parquet indique que l'avant-projet de loi, élaboré par un groupe de travail ad hoc, ne contenait pas la notion d'usurpation d'identité, contrairement au texte de la directive qui a été adopté à cette période. D'où l'idée de s'inspirer du texte français qui contient cette notion. Après vérification, il s'est avéré qu'en pratique l'application du texte français soulève de multiples problèmes. La notion d'« usurpation d'identité » n'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 2^e 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 par le groupe de travail d'adapter le texte luxembourgeois, plutôt que de reprendre textuellement la disposition française.

Au sujet de la remarque du Conseil d'Etat concernant les termes « identification de quelque nature que ce soit », il est précisé que cette terminologie générale est sensée couvrir le fait de prendre aussi bien un nom patronymique, un nom d'utilisateur combiné à un mot de passe, qu'un matricule ou une identité d'un tiers, y compris l'utilisation d'une signature électronique, d'un certificat type Luxtrust ou d'un identifiant numérique.

Quant au terme « publiquement », contrairement au Conseil d'Etat, la jurisprudence interprète le terme « publiquement » comme « ostensiblement ».

Les termes « qui ne lui appartient pas » visent aussi bien les cas dans lesquels une personne a pris le nom d'un tiers, que les cas où le nom n'appartient à personne (à titre d'exemple un nom qui n'existe pas encore) sans qu'il ne soit nécessaire de prouver que le nom appartient à un tiers.

La disposition de l'article 231, telle que modifiée par le projet de loi, ne vise pas le recours à des pseudonymes, notamment ceux utilisés de façon fréquente pour la rédaction de commentaires sur des sites d'informations en ligne. Toutefois, le pseudonyme doit être perçu en tant que tel (p.ex. : Mickey Mouse, Superman) et ne pas présenter de risque de confusion avec une identification réelle.

En revanche l'usage d'un pseudonyme qui présente les caractéristiques du « port public de faux nom », c'est-à-dire un nom patronymique existant (p.ex. : Jean SCHMIT qui se fait appeler Jacques MULLER), est passible des peines énoncées à l'article 231 dans sa teneur actuelle¹.

L'article 231bis du projet de loi vise l'usage d'un nom ou identifiant « 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 ». La disposition de l'article 231bis vise ainsi tous les cas d'usage de noms ou identifiants, peu importe que l'identité soit prise « publiquement » ou non. En l'état actuel de la législation, ce type de comportement serait constitutif d'une calomnie ou d'une diffamation, voire d'un harcèlement.

Point 3

Dans la mesure où les articles 488² et 509-5 du Code pénal prévoient des infractions similaires, le point 3 aligne le seuil de peines de l'article 488 du Code pénal au seuil de peine prévu au nouvel article 509-5³ du Code pénal. Le Conseil d'Etat n'a pas d'observation particulière.

¹ **Art. 231.** Quiconque aura publiquement pris un nom qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement.

² **Art. 488.** (L. 14 août 2000) Quiconque aura frauduleusement contrefait ou altéré des clefs, y compris électroniques sera condamné à un emprisonnement de trois mois à deux ans et à une amende de 251 euros à 2.000 euros.

³ **Art. 509-5.** Sera puni de 4 mois à cinq ans d'emprisonnement et d'une amende de 251 euros à 5.000 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 – un mot de passe, 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."

Point 4

Il est proposé de compléter l'article 496 du Code pénal par l'ajout, à la liste des objets remis ou délivrés, des clés électroniques. Les auteurs font état d'un arrêt de la Cour d'appel n°261/10 X du 14 juin 2010 dont il résulterait que l'article 496, dans sa teneur actuelle, ne permet pas d'appréhender « l'hameçonnage d'un mot de passe (en anglais « phishing ») ».

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 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 clé électronique dans la définition des objets visés aux articles 461⁴, 470⁵ ou 491⁶ du Code pénal.

Le Conseil d'Etat voudrait encore attirer 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 ceux 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

⁴ **Art. 461.** Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol.

(L. 7 juillet 1977) Est assimilé au vol, le fait de soustraire frauduleusement un véhicule automoteur ou un cycle appartenant à autrui en vue d'un usage momentané et avec l'intention de le restituer.

⁵ **Art. 470.** (L. 29 juin 1984) Quiconque aura extorqué, par violences ou menaces, soit la remise de fonds, valeurs ou objets mobiliers, 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 ou objets mobiliers, 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.

La tentative de ce dernier délit sera punie d'un emprisonnement de six mois à trois ans et d'une amende de 251 euros à 10.000 euros.

⁶ **Art. 491.** Quiconque aura frauduleusement soit détourné, soit dissipé au préjudice d'autrui, des effets, deniers, marchandises, billets, quittances, 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.

(L. 2 juillet 1980) Quiconque, dans une intention frauduleuse, se sera fait servir des boissons ou des aliments qu'il aura consommés sur place en tout ou en partie, ou se sera fait donner un logement dans les établissements à ce destinés, ou se sera fait transporter sur les voies publiques par un voiturier qui fait du transport de personnes sa profession, ou aura rempli ou fait remplir, à une station exploitée par un professionnel de la distribution, les réservoirs d'un véhicule ou d'autres réservoirs, en tout ou en partie, de carburants ou lubrifiants, et sans avoir payé le prix, sera puni d'un emprisonnement de huit jours à six mois et d'une amende de 251 euros à 5.000 euros. Les délits prévus au présent alinéa ne pourront être poursuivies que sur la plainte de la personne lésée. L'action publique sera éteinte par le paiement de la dette ou par le désistement de la partie plaignante.

Le coupable pourra, de plus, être condamné à l'interdiction, conformément à l'article 24.

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 clé électronique et, au point 8 relatif au nouvel article 509-5, visent le « mot de passe », le « code d'accès » ou « toute autre clé électronique ». De deux choses l'une: ou bien le concept de clé électronique est le terme générique à consacrer, auquel cas il faudra adapter le texte du nouvel article 509-5 à celui de l'article 496; ou bien le concept de clé électronique est trop restreint, auquel cas il faudra reprendre, à l'article 496, tous les concepts de l'article 509-5. Le Conseil d'Etat renvoie encore, dans ce contexte, à l'article 488 du Code pénal qui consacre déjà le concept de clé 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 « clés électroniques », proposés par les auteurs, par l'expression « ou un bien quelconque (corporel ou incorporel) ».

*

Le représentant du Parquet indique que la modification de l'article 496 alinéa 1^{er} du Code pénal vise à inclure les clés électroniques dans la liste des objets que l'auteur de l'infraction s'est fait remettre afin de commettre l'escroquerie. Cette modification est motivée par un arrêt (n°261/10 X du 14 juin 2010) de la Cour d'appel, dans lequel la Cour n'a pas retenu l'escroquerie pour l'hameçonnage (« phishing ») en estimant que le mot de passe ne constituait pas un meuble au sens de l'article 496.

Plutôt que de créer un article séparé, il paraissait logique aux auteurs du texte de loi de rajouter les clés électroniques dans la liste des objets cités à l'article 496. Les auteurs ont volontairement opté pour cette solution « minimale », dans le cadre de la transposition de la Convention du Conseil de l'Europe. La réflexion sur la terminologie « biens corporels et biens incorporels » sera utilement menée dans le cadre de la réforme du Code pénal.

Quant à la remarque du Conseil d'Etat sur la terminologie utilisée dans le nouvel article 509-5 « un mot de passe, un code d'accès ou toute autre clé électronique », le représentant du Parquet est d'avis que le terme générique de « toute autre clé électronique » inclut d'office les mots de passe ainsi que les codes d'accès qui sont cités à titre d'exemples.

*

A la demande du Président de la Commission, les représentants du Ministère de la Justice et du Parquet réaliseront un tableau comparatif entre, d'une part, les dispositions du projet de loi et, d'autre part, les dispositions poursuivant les mêmes objectifs des législations française et belge. Par ailleurs, ils fourniront aux membres de la Commission les jurisprudences citées au cours de la réunion.

Echange de vues

De l'échange de vues subséquent, il y a lieu de retenir les points suivants :

- Au sein de la police judiciaire, il existe une section « nouvelles technologies », à laquelle sont affectés des OPJ hautement qualifiés qui ont la capacité de constater des infractions de ce type.

- La cybersécurité n'est pas déléguée à des sociétés privées. Il existe d'ores et déjà au Luxembourg différents CERT (cyber emergency response team), que ce soit au niveau du Ministère de l'Economie, des institutions de l'éducation (Fondation Restena) ou au niveau de l'administration centrale (GOV CERT).
- Lors de la rédaction des amendements, il faudra veiller à rédiger les nouveaux libellés à l'indicatif présent.
- Dans le cadre de la lutte contre la cybercriminalité, il sera possible de recourir au mandat d'arrêt européen.
- Les pseudonymes non identifiants (p.ex. : Mickey Mouse, Superman) ne sont pas visés par les dispositions des articles 231 et 231bis du code pénal concernant l'usurpation d'identité.

3. 6550 Projet de loi modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat

Etant donné que le projet de rapport fera l'objet de quelques modifications complémentaires, une version mise à jour sera diffusée, et son adoption est reportée à une réunion ultérieure.

4. Divers

Le 1^{er} mai étant férié, la prochaine réunion de la Commission juridique aura lieu le 8 mai 2013 à 9 heures. L'ordre du jour sera communiqué ultérieurement aux membres de la Commission.

Luxembourg, le 24 avril 2013

La secrétaire,
Carole Closener

Le Président,
Gilles Roth

Annexe :

Projet de loi n°5974 : Propositions d'amendements

Transmis pour information, dans le cadre de la réunion du 24 avril 2013, aux honorables membres de la

- Commission de la Commission juridique
- Conférence des Présidents

Luxembourg, le 19 avril 2013

Carole Closener
Secrétaire de la Commission juridique

5974 **Projet de loi modifiant la loi modifiée du 10 août 1915 concernant les sociétés commerciales en vue de mettre en œuvre le Règlement (CE) no 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)**

Propositions d'amendements

Remarque préliminaire

Le Conseil d'Etat critique la technique législative employée pour étendre aux sociétés coopératives nationales la possibilité de choisir entre un régime moniste et un régime dualiste.

Lors de la rédaction du projet de loi, la difficulté était que le projet de loi n°5730, déposé en 2007 et non encore avisé par le Conseil d'Etat en 2008, avait prévu de réformer le régime de la société coopérative nationale. Plutôt que de proposer des modifications dans un texte déjà en cours de modification, l'option a été choisie de créer une nouvelle sous-section relative aux sociétés coopératives européennes (SCE) dans la section relative aux sociétés coopératives nationales.

Le régime du règlement 1435/2003 (ci-après le 'règlement SCE') permet la mise en place – comme c'était déjà le cas pour les sociétés européennes – à côté d'un régime moniste, d'un régime dualiste.

A l'instar de ce qui avait été fait pour la société européenne, il a été proposé dans le projet de loi d'étendre aux sociétés coopératives nationales la possibilité de choisir entre le modèle moniste ou le modèle dualiste.

Compte tenu de la contrainte relevée ci-dessus, cette possibilité a été reprise dans l'un des articles intégrés dans la sous-section sur les SCE.

Compte tenu du fait que le projet de loi n°5730 a entretemps été avisé par le Conseil d'Etat et que des amendements gouvernementaux concernant le volet des sociétés coopératives nationales sont en cours de préparation, il semble préférable à la Commission juridique d'adopter la démarche suivante :

- limiter l'objet du présent projet de loi à la seule mise en œuvre du règlement SCE sans s'étendre à la coopérative nationale la possibilité de choisir une organisation dualiste;

- reprendre dans le projet de loi n°5730 les propositions du CE touchant à la société coopérative nationale en les combinant avec les autres éléments déjà prévus dans le projet de loi n°5730 pour ladite coopérative nationale.

Cette démarche présente le double avantage de permettre :

- l'évacuation rapide d'un texte en vue de la mise en œuvre effective du règlement SCE ;
- une démarche de rédaction cohérente du texte relative à la coopérative nationale dans le contexte du projet de loi n°5730.

Cela a pour conséquence que les modifications aux articles compris dans la sous-section relative aux sociétés coopératives nationales n'ont pas été reprises par la Commission juridique.

Par ailleurs, la Commission juridique a donné suite aux propositions du Conseil d'Etat de supprimer dans le texte les indications des articles du règlement SCE mis en application et de supprimer certains articles superfétatoires, à savoir les articles 137-11 paragraphe 2, 137-19, 137-24 et 137-65, ce qui implique une renumérotation des points au sein de l'article I.

Amendement 1 concernant le point 20 de l'article I

Au point 20, l'article 137-25 est modifié comme suit :

*« Art. 137-25.- Toute disposition légale ou réglementaire concernant les sociétés commerciales se référant au "conseil d'administration", "administrateur(s)" ou "gérant(s)" d'une société coopérative doit être entendue, dans le cadre d'une société coopérative **européenne (SEC)** dotée d'un directoire et d'un conseil de surveillance, comme se référant au directoire de la société concernée sauf si, d'après la nature de la mission confiée, il s'agit de l'entendre comme se référant au conseil de surveillance.»*

Commentaire

En ce qui concerne plus particulièrement l'article 137-25, les alinéas 1 et 2 ont été supprimés comme suite à la remarque préliminaire, et le 3^e alinéa a été corrigé pour faire référence à la société coopérative européenne.

Amendement 2 concernant le point 22 de l'article I

Au point 22, l'article 137-29 est modifié comme suit :

*« Art. 137-29.- ~~Sous réserve de l'article 42, paragraphe 2, du Règlement (CE) No 1435/2003, le~~ **Le** nombre minimal d'administrateurs est fixé à trois.»*

Commentaire

Le Conseil d'Etat relève à propos de l'article 137-29 initialement proposé que les auteurs proposent de fixer le nombre des administrateurs à trois, mais que si cette disposition constitue bien une mise en application de l'article 42, alinéa 2 du règlement SCE, elle est cependant en contradiction avec l'article 114 de la loi modifiée du 10 août 1915 concernant les sociétés commerciales, qui devrait dès lors être adapté.

Comme il a été retenu par la Commission juridique que les dispositions relatives à la société coopérative nationale ne seraient pas adaptées dans le présent projet de loi, le texte doit

être légèrement adapté en enlevant les termes 'Sous réserve de l'article 42, paragraphe 2, du règlement (CE) No 1435/2003'.

Amendement 3 concernant le point 38 de l'article I

L'article 137-44 est modifié comme suit :

« **Art. 137-44.-** Le conseil d'administration, le directoire, selon le cas, ainsi que le conseil de surveillance et le ou les commissaires réviseurs d'entreprises agréés désignés pour effectuer le contrôle légal des comptes annuels et, le cas échéant des comptes consolidés, sont en droit de convoquer l'assemblée générale. »

Commentaire

Cet article correspond à l'article 54 paragraphe 2 du règlement SCE qui donne pouvoir de convoquer l'assemblée générale à l'organe de direction, l'organe d'administration, l'organe de surveillance ou tout autre organe ou autorité compétente conformément à la loi nationale.

Le terme de 'commissaire' utilisé par l'article 137-44 et correspondant à celui d'autre organe ou autorité compétente conformément à la loi nationale peut causer un problème en suivant la ligne de la proposition du Conseil d'Etat de supprimer comme superfétatoire l'article 137-65 dans lequel il est précisé que l'autorité compétente au sens de l'article 54 est le réviseur d'entreprises agréé désigné pour effectuer le contrôle légal des comptes.

Sur la question du contrôle des comptes, les précisions suivantes sont peut être utiles :

L'article 70 du règlement SCE prévoit que le contrôle des comptes est effectué par un réviseur d'entreprises agréé. L'article 68 précise par ailleurs que le contrôle des comptes se fait sur base des dispositions législatives adoptées pour mettre en œuvre les 4e et 7e directives. La disposition qui nous intéresse ici est l'article 69 de la loi modifiée du 19 décembre 2002 qui prévoit 1) que les comptes des SA, SARL et SCA sont contrôlés par des réviseurs d'entreprises agréés, 2) que par exception les comptes des petites SA, SARL et SCA ne sont pas contrôlés par des réviseurs d'entreprises agréés et 3) que pour les sociétés ayant un commissaire, le commissaire est supprimé s'il y a un réviseur d'entreprises agréé.

En clair, pour la SCE, cela signifie 1) que les comptes des moyennes et grandes SCE sont contrôlés par un réviseur d'entreprises agréé, 2) que par exception ceux des petites SCE ne le sont pas et 3) que la disposition relative au commissaire ne trouve pas à s'appliquer parce que dans le cas des SCE cet organe n'existe pas.

La rédaction proposée en se tenant assez près du texte belge créerait un problème si on supprimait l'article 137-65 comme proposé par le Conseil d'Etat.

Ainsi, il est proposé de remplacer le terme « commissaire » par « réviseur d'entreprises agréé » ce qui permet alors de supprimer sans problème l'article 137-65 comme proposé par le Conseil d'Etat.



Session ordinaire 2012-2013

CC/pk

P.V. J 31

Commission juridique

Procès-verbal de la réunion du 17 avril 2013

Ordre du jour :

1. 5974 Projet de loi modifiant la loi modifiée du 10 août 1915 concernant les sociétés commerciales en vue de mettre en œuvre le Règlement (CE) no 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)
 - Rapporteur : Monsieur Léon Gloden
 - Présentation du projet de loi
 - Examen de l'avis du Conseil d'Etat

2. 6376 Projet de loi portant réforme de la Commission des normes comptables et modification de diverses dispositions relatives à la comptabilité et aux comptes annuels des entreprises ainsi qu'aux comptes consolidés de certaines formes de sociétés et modifiant:
 - (1) le titre II du livre Ier du Code de commerce
 - (2) le titre II de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises
 - (3) la section XVI de la loi modifiée du 10 août 1915 concernant les sociétés commerciales
 - Rapporteur: Monsieur Léon Gloden
 - Examen de l'avis complémentaire du Conseil d'Etat

3. 6514 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
 - Désignation d'un rapporteur

4. Approbation des projets de procès-verbal des réunions des 6, 13 et 20 mars 2013

5. Divers

*

Présents : M. Marc Angel, M. Xavier Bettel, M. Félix Braz, Mme Christine Doerner, M. Léon Gloden, M. Jacques-Yves Henckes, M. Jean-Pierre Klein, M. Paul-Henri Meyers, M. Gilles Roth, M. Lucien Weiler

M. Daniel Ruppert, du Ministère de la Justice

Mme Carole Closener, de l'Administration parlementaire

Excusés : M. Alex Bodry, Mme Lydie Polfer

*

Présidence : M. Gilles Roth, Président de la Commission

*

1. 5974 Projet de loi modifiant la loi modifiée du 10 août 1915 concernant les sociétés commerciales en vue de mettre en œuvre le Règlement (CE) no 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)

Présentation du projet de loi

Le projet de loi, tel que décrit en détail par l'exposé des motifs du document parlementaire afférent, a pour objectif essentiel d'assurer, dans le cadre de la loi modifiée du 10 août 1915 concernant les sociétés commerciales, une mise en œuvre des dispositions du règlement (CE) No 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)¹, qui est entré en vigueur le 18 août 2006.

Si le règlement est certes directement applicable en toutes ses dispositions, il réclame néanmoins des Etats membres un effort de mise en œuvre, notamment quant à la procédure de transfert du siège statutaire de la SEC et de son immatriculation, et ouvre en même temps une série d'options réglementaires (réceptivité plus ou moins large à la constitution de SEC, étendue du contrôle exercé par les autorités à l'occasion de la constitution, système moniste ou dualiste de gestion etc.) auxquelles il importe de répondre.

Echange de vues

- Jusqu'à présent il n'y a pas eu de constitutions de sociétés coopératives européennes au Luxembourg. Toutefois, s'il y avait eu des demandes, celles-ci auraient dû être traitées, le règlement européen étant directement applicable.
- Pour la mise en œuvre du règlement, il a été décidé de recourir à une loi (plutôt qu'à un règlement grand-ducal) pour plusieurs raisons. D'une part, les restrictions apportées à la liberté de commerce font partie des matières réservées à la loi. D'autre part, certaines dispositions devaient viser non seulement les SEC mais également les sociétés coopératives de droit interne (comme par exemple la possibilité de se doter soit d'un régime moniste soit d'un régime dualiste de gestion). Par ailleurs le projet de loi contient certaines dispositions complémentaires au

règlement SEC. Enfin le projet de loi contient des dispositions pénales qui auraient exclu la possibilité de recourir à un règlement grand-ducal.

Examen de l'avis du Conseil d'Etat

Le rapporteur du projet de loi, M. Léon Gloden, présente l'avis du Conseil d'Etat du 5 février 2013, pour les détails duquel il est prié de se référer au document parlementaire afférent.

Considérations générales

Le Conseil d'Etat note que, contrairement à ce qui a été proposé et retenu contre l'avis du Conseil d'Etat pour la société européenne (SE), les auteurs ne proposent actuellement pas une intégration des dispositions du règlement européen dans le texte existant, mais ils prévoient de créer dans la section VI. - *Des sociétés coopératives* une nouvelle sous-section 3 pour les sociétés coopératives européennes après la sous-section 1. - *Des sociétés coopératives en général* et la sous-section 2. - *Des sociétés coopératives organisées comme des sociétés anonymes*.

Le Conseil d'Etat relève que les auteurs se sont inspirés des textes belges de mise en application du règlement (CE) mais qu'ils ajoutent cependant la nouvelle réglementation des systèmes moniste et dualiste sous les articles 137-25 et suivants qui sont aussi applicables aux sociétés coopératives nationales, créant par là en fait, à côté de la société coopérative actuelle, une nouvelle réglementation pour les sociétés nationales en les faisant bénéficier de nouveaux organes de gestion et de contrôle.

Selon le Conseil d'Etat, cette façon de procéder ne manquera pas de créer un désordre et une incohérence dans les dispositions applicables aux sociétés coopératives suivant les organes de gestion et de surveillance choisis. Il faut par conséquent modifier les articles respectifs de la sous-section 1 de la section 6 de la loi modifiée du 10 août 1915 concernant les sociétés commerciales. De ce fait et pour assurer la cohérence du texte, il ne suffit pas seulement de mettre en application les dispositions qui accordent une option aux Etats membres, mais il faudra aussi copier des parties de texte du règlement européen, ce qui est normalement contraire à la technique de mise en application d'un règlement européen.

En réponse aux observations du Conseil d'Etat, il est rappelé que, lors de la rédaction du projet de loi, les auteurs se sont heurtés à la difficulté que le projet de loi n°5730 déposé en 2007 et non encore avisé par le Conseil d'Etat en 2008 avait prévu de réformer le régime de la société coopérative nationale. Plutôt que de proposer des modifications dans un texte déjà en cours de modification, l'option a été choisie de créer une nouvelle sous-section dans la section relative aux coopératives visant les sociétés coopératives européennes (SCE).

Le régime du règlement SCE permet la mise en place – comme c'était déjà le cas pour les SE – à côté d'un régime moniste d'organisation des organes, un régime dualiste. A l'instar de ce qui avait été fait pour la SE, il a été proposé dans le projet de loi d'étendre aux sociétés coopératives nationales la possibilité de choisir entre le modèle moniste ou le modèle dualiste. Compte tenu de la difficulté décrite ci-dessus, cette possibilité a été reprise dans l'un des articles intégré dans la sous-section sur les SCE.

Or c'est précisément ce que critique à présent le Conseil d'Etat.

Compte tenu du fait que le projet de loi n°5730 a entretemps été avisé par le Conseil d'Etat et que des amendements gouvernementaux sont en cours de préparation, il serait envisageable de limiter l'objet du présent projet de loi à la seule mise en œuvre

du règlement SCE sans ambitionner d'étendre à la coopérative nationale la possibilité de choisir une organisation dualiste, et de reprendre dans le projet de loi n°5730 les propositions du Conseil d'Etat touchant à la société coopérative nationale en les combinant avec les autres éléments déjà prévus dans le projet n°5730 pour ladite coopérative nationale.

Cette démarche présente le double avantage de permettre :

- l'évacuation rapide d'un texte en vue de la mise en œuvre effective du règlement SCE ;
- une démarche de rédaction cohérente du texte relative à la coopérative nationale dans le contexte du projet de loi n° 5730.

Cette démarche implique que les modifications aux articles compris dans la sous-section relative aux sociétés coopératives nationales n'ont pas été reprises par la Commission juridique.

Le Conseil d'Etat note que les auteurs ont pris comme base la législation belge.

Il indique qu'il aurait préféré l'insertion des références aux dispositions du règlement (CE) à celles de la loi belge, en notant que la mise en application d'un règlement européen n'est pas un exercice de droit comparé, mais une adaptation de la loi nationale au règlement européen.

Le Conseil d'Etat relève que le projet de loi introduit également pour les sociétés coopératives nationales les régimes moniste et dualiste. Comme le système dualiste est nouveau pour celles-ci, les auteurs proposent de coller le plus possible au texte du règlement européen afin de ne pas créer deux systèmes dualistes différents où le système national pourrait se révéler lacunaire par rapport au système européen. Le Conseil d'Etat n'y voit aucun obstacle, en notant qu'une uniformisation des systèmes pourra réduire bon nombre de problèmes et d'erreurs.

Du fait que les dispositions du règlement européen seront rendues applicables aux sociétés coopératives nationales, le Conseil d'Etat propose de reprendre les dispositions du règlement (CE) plutôt que de renvoyer à ce règlement, car les renvois rendent la rédaction opaque et la compréhension difficile. Comme l'article 42, paragraphe 4 du règlement européen autorise de toute façon l'adoption de mesures appropriées concernant les sociétés coopératives européennes, la reprise du texte des dispositions ne pourra être analysée comme une mise en application du règlement européen.

Comme les auteurs proposent d'introduire les dispositions du règlement européen aussi pour les sociétés coopératives nationales, le Conseil d'Etat propose de revoir en outre les articles de la loi modifiée du 10 août 1915 concernant les sociétés commerciales à partir de l'article 114, car autrement il y aura sur le plan national la société coopérative ancienne législation et la société coopérative nouvelle avec soit un régime moniste de gestion, soit un régime dualiste de gestion ainsi que la société coopérative européenne (SEC).

Il propose donc de réformer la législation nationale des sociétés coopératives en l'adaptant aux dispositions du règlement européen par la modification des articles 114 et suivants et d'introduire par la suite sous les articles 137-11 et suivants la société coopérative européenne (SEC). Cela entraînerait évidemment que le projet de loi soit retravaillé entièrement. La conséquence en sera cependant un texte cohérent tant pour la société coopérative nationale que pour la société coopérative européenne (SEC).

Selon le Conseil d'Etat, une telle structure permettra de mettre en application pour la société coopérative européenne (SEC) les seuls articles qui nécessitent une mise en application.

Quant à l'insertion des références à la loi belge dans le commentaire, le représentant du Ministère de la Justice indique qu'elle était justifiée afin de permettre utilement aux praticiens d'examiner les commentaires et la doctrine belge.

Observation préliminaire

Le Conseil d'Etat rappelle que, d'une façon générale, les indications des articles mis en application sont à omettre dans la rédaction des nouveaux articles à insérer dans la loi du 10 août 1915 et les nombres sont à écrire en toutes lettres.

Les renvois à « article .. de la présente loi » sont à éviter, car cela relève de l'évidence.

La Commission fait siennes les remarques de nature légistique du Conseil d'Etat.

Article I (Article unique)

Le Conseil d'Etat signale que, comme le projet de loi ne comporte qu'un seul article, il y a lieu d'écrire: « Article unique ».

La Commission décide de suivre le Conseil d'Etat.

Point 2

Article 137-11

Le Conseil d'Etat n'a pas d'observation à faire quant au paragraphe 1^{er} (alinéa unique selon le Conseil d'Etat), sauf qu'il y a lieu d'indiquer la date exacte du règlement européen qui est celle du 22 juillet 2003.

La Commission se rallie à la suggestion du Conseil d'Etat.

Quant au paragraphe 2, le Conseil d'Etat propose de le supprimer, car il est superfétatoire. Il s'agit d'une copie conforme de l'article 1^{er}, paragraphe 2, alinéa 3 du règlement européen qui ne nécessite pas de mise en application.

La Commission décide de suivre le Conseil d'Etat en supprimant le paragraphe 2.

Point 4

Article 137-13

Le Conseil d'Etat renvoie à son observation préliminaire en ce qui concerne le paragraphe 1^{er}.

Il constate que les auteurs n'ont pas choisi d'option quant à une éventuelle unicité obligatoire du siège statutaire et de l'administration centrale.

En réponse à cette dernière remarque, le représentant du Ministère indique que le projet de loi ne fait simplement pas usage de l'option permettant à un Etat membre d'imposer dans sa législation d'avoir le siège statutaire et l'administration centrale au même endroit (option figurant à l'article 6 du règlement SCE). Par contre, cela ne change rien au fait – et cela n'est pas une restriction optionnelle – que le siège

statutaire et l'administration centrale doivent être au moins situés au sein du même Etat membre, donc s'agissant d'une SCE 'luxembourgeoise' au Luxembourg. L'article 137-13 le prévoit en énonçant que le procureur d'Etat est l'autorité chargée de dénoncer à l'autre Etat membre concerné les cas où l'administration centrale et le siège statutaire ne se trouvent pas dans le même Etat membre.

La Commission se rallie à la première remarque du Conseil d'Etat quant à la suppression des indications des articles mis en application.

Point 6

Article 137-14

Le Conseil d'Etat renvoie à son observation préliminaire.

La Commission fait sienne la remarque du Conseil d'Etat.

Point 8

Article 137-16

Le Conseil d'Etat s'interroge sur les intentions des auteurs qui renvoient au seul alinéa 1^{er} de l'article 262 de la loi du 10 août 1915 concernant les sociétés commerciales. Il suppose qu'il y a lieu de lire "paragraphe 1^{er}".

La Commission décide de suivre le Conseil d'Etat en remplaçant le terme « alinéa » par « paragraphe ».

Point 10

Article 137-17

Le Conseil d'Etat renvoie à son observation préliminaire.

Article 137-18

Le Conseil d'Etat propose de regrouper les dispositions relatives à la désignation du notaire comme organe de contrôle de la fusion dans un seul article.

La Commission souhaite néanmoins maintenir la référence au notaire pour le contrôle de légalité, d'autant plus que le Conseil d'Etat propose de supprimer l'article 137-65.

Point 12

Article 137-19

Le Conseil d'Etat estime que les dispositions de l'article 31 du règlement européen ne requièrent pas de mise en application. L'adoption du texte national encourt le risque de modifier la disposition afférente dudit règlement européen.

La Commission approuve la remarque du Conseil d'Etat.

Point 18

Article 137-24

Selon le Conseil d'Etat, cet article, qui est une copie de l'article 18 du règlement européen, est superfétatoire et devra être supprimé.

La Commission fait sienne la remarque du Conseil d'Etat.

Point 20

Le Conseil d'Etat approuve la démarche des auteurs qui proposent de faire bénéficier la société coopérative nationale de la possibilité de choisir entre un régime moniste et un régime dualiste de gestion. Il note que les auteurs ne suivent cependant pas cette démarche dans l'architecture des dispositions y afférentes.

En réponse à cette remarque, la Commission indique que, dans la mesure où l'on décide d'introduire l'option entre le régime dualiste et le régime moniste pour la seule SCE, les seules adaptations à faire sont celles prévoyant l'extension du régime proposé aux SC de droit national.

Article 137-25

Comme le Conseil d'Etat a proposé de modifier la loi modifiée du 10 août 1915 à partir de l'article 114, une rédaction plus simple du texte à introduire dans l'article 114 l'article s'impose, car le bout de phrase du milieu n'ajoute rien à sa compréhension. Il suggère le libellé suivant:

« Une société coopérative peut être gérée par un ou plusieurs administrateurs ou par un directoire et un conseil de surveillance.

Les sociétés coopératives qui adoptent le régime du directoire et du conseil de surveillance sont régies par les dispositions qui suivent et les dispositions des articles 37 à 63 du règlement (CE) n° 1435/2003 relatif au statut de la société coopérative européenne (SEC). »

L'alinéa 3 proposé par les auteurs pourra être repris.

Dans la mesure où la restructuration proposée n'est pas reprise, la proposition du Conseil d'Etat pour l'article 114 peut être écartée.

La Commission propose de supprimer les deux premiers alinéas qui sont sans objet.

Le libellé aurait alors la teneur suivante :

Art. 137-25.- Une société coopérative qui n'a pas adopté la forme d'une société coopérative européenne (SEC) peut opter pour un régime moniste ou un régime dualiste tels qu'organisés par les articles qui suivent. Dans ce cas la société coopérative est soumise en outre aux dispositions du Règlement (CE) No 1435/2003 concernant les régimes moniste et dualiste de gestion.

Toute disposition légale ou réglementaire concernant les sociétés commerciales se référant au "conseil d'administration", "administrateur (s)" ou "gérant(s)" d'une société coopérative doit être entendue, dans le cadre d'une société coopérative **européenne (SEC)** dotée d'un directoire et d'un conseil de surveillance, comme se référant au directoire de la société concernée sauf si, d'après la nature de la mission confiée, il s'agit de l'entendre comme se référant au conseil de surveillance

Cette modification fera l'objet d'un amendement.

Article 137-26

Cet article est superfétatoire pour les sociétés commerciales à gestion dualiste, car le Conseil d'Etat propose une nouvelle version de l'article 137-25 qui rend les articles cités déjà applicables.

En ce qui concerne les sociétés coopératives nationales, cet article, modifié comme suit, suffira:

« Art. 137-26. Les membres des organes d'administration peuvent être, si les statuts le prévoient, des personnes morales, auquel cas les articles 51*bis* et 60*bis*-4 s'appliquent. »

Compte tenu de ce qui précède, le maintien de cet article reste nécessaire.

Point 21

Le Conseil d'Etat ne voit pas de raison de ne pas suivre l'exemple de la société européenne (SE) (articles 50 à 60*bis*-1) et de regrouper les dispositions concernant les systèmes moniste et dualiste sous deux subdivisions. Il propose de suivre plutôt la structure utilisée dans la loi modifiée du 10 août 1915 que d'aller s'inspirer dans la loi belge.

Sous réserve de cette observation, le Conseil d'Etat analyse les propositions de texte concernant les deux systèmes d'administration et de contrôle. Cette analyse pourra servir à revoir les dispositions de la loi nationale pour adapter celles-ci au règlement européen en ce qui concerne les organes.

Compte tenu de ce qui précède, la Commission est d'avis que la remarque du Conseil d'Etat n'est plus pertinente.

Point 22

Article 137-28

Sans observation, sauf que pour l'alinéa 2, le Conseil d'Etat propose de mettre tous les verbes à l'indicatif présent.

La Commission approuve cette proposition du Conseil d'Etat.

Article 137-29

Les auteurs proposent de fixer le nombre des administrateurs à trois. Si cette disposition constitue bien une mise en application de l'article 42, alinéa 2 du règlement européen, elle est cependant en contradiction avec l'article 114 de la loi modifiée du 10 août 1915 concernant les sociétés commerciales.

Comme le projet de loi entend adapter aussi la loi nationale aux dispositions du règlement européen, il y a lieu de modifier encore l'article 114 qui fixe le nombre des mandataires de l'organe d'administration à un ou plusieurs mandataires.

Comme il a été retenu par la Commission juridique que les dispositions relatives à la société coopérative nationale ne seraient pas adaptées dans le présent projet de loi,

elle propose d'adapter le libellé en supprimant les termes 'Sous réserve de l'article 42, paragraphe 2, du règlement (CE) No 1435/2003'.

Cette modification fera l'objet d'un amendement.

Point 24

Articles 137-30 à 137-33

Suite aux propositions du Conseil d'Etat, les dispositions respectives des articles de ce point sont à renvoyer sous les subdivisions relatives à chacun des régimes de gestion.

Compte tenu de ce qui précède (cf. point 21), la Commission est d'avis que la remarque du Conseil d'Etat n'est plus pertinente.

Point 25

Sans observation, sous réserve des considérations générales.

Point 36

Article 137-43

Sans observation, sauf à rédiger la fin de l'alinéa 1^{er} de la façon suivante afin que cette disposition s'applique aux sociétés coopératives tant nationales qu'européennes:
« ...résultant d'infractions aux dispositions de la loi, des statuts sociaux et, suivant le cas, du règlement européen. »

Compte tenu de ce qui précède (cf. point 21), la Commission est d'avis que la remarque du Conseil d'Etat n'est plus pertinente.

Point 38

Articles 137-44

Sans observation de la part du Conseil d'Etat.

La Commission juridique rappelle toutefois que cet article correspond à l'article 54 paragraphe 2 du règlement SCE qui donne pouvoir de convoquer l'assemblée générale à l'organe de direction, l'organe d'administration, l'organe de surveillance *ou tout autre organe ou autorité compétente conformément à la loi nationale*.

Le terme de « commissaire » utilisé par l'article 137-44 et correspondant à celui « d'autre organe ou autorité compétente conformément à la loi nationale » peut causer un problème, dans la ligne de la proposition du Conseil d'Etat de supprimer comme superfétatoire l'article 137-65 dans lequel il est précisé que l'autorité compétente au sens de l'article 54 est le réviseur d'entreprises agréé désigné pour effectuer le contrôle légal des comptes.

Sur la question du contrôle des comptes, les précisions suivantes peuvent être utiles :

L'article 70 du règlement prévoit que le contrôle des comptes est effectué par un réviseur d'entreprises agréé. L'article 68 précise par ailleurs que le contrôle des comptes se fait sur base des dispositions législatives adoptées pour mettre en œuvre la 4^e et la 7^e directives. La disposition qui nous intéresse ici est l'article 69 de la loi du

19 décembre 2002 qui prévoit 1) que les comptes des SA/SARL/SCA sont contrôlés par des réviseurs agréés, 2) que par exception les comptes des petites SA/SARL/SCA ne sont pas contrôlés par des réviseurs d'entreprises agréés et 3) que pour les sociétés ayant un commissaire, le commissaire est supprimé s'il y a un réviseur d'entreprises agréé.

En clair, pour la SCE, cela veut dire 1) que les comptes des moyennes et grandes SCE sont contrôlés par un réviseur d'entreprises agréé, 2) que par exception ceux des petites SCE ne le sont pas et 3) que la disposition relative au commissaire ne trouve pas à s'appliquer parce que dans le cas des SCE cet organe n'existe pas.

La rédaction proposée, assez proche du texte belge, créerait un problème si on supprimait l'article 137-65 comme proposé par le Conseil d'Etat.

La solution serait de remplacer le terme « commissaire » par celui de « réviseur d'entreprise agréé » ce qui permettrait alors de supprimer sans problème l'article 137-65 comme proposé par le Conseil d'Etat.

Cette modification fera l'objet d'un amendement.

Point 42

Article 137-47

Le Conseil d'Etat remarque que le texte met les dispositions de l'article 59 du règlement européen en application et propose de supprimer les indications de l'article et du paragraphe.

En outre il propose de diviser le paragraphe 1^{er} en trois alinéas conformément au texte du règlement européen.

La Commission fait sienne la remarque du Conseil d'Etat.

Point 46

Article 137-49

Le Conseil d'Etat propose de renvoyer tout simplement aux dispositions de l'article 59 :

« Art. 139-49. Les administrateurs, les membres du directoire et du conseil de surveillance sont responsables conformément aux dispositions de l'article 59. »

La Commission décide de suivre le Conseil d'Etat.

Point 56

Article 137-62

Concernant les dispositions pénales applicables à la société coopérative européenne, le Conseil d'Etat propose de renvoyer directement à la section XI de la loi. Cette disposition aurait alors la teneur suivante:

« Art 137-63. La section XI. – *Dispositions pénales* est applicable à la société coopérative européenne. »

La Commission est d'avis qu'en effet la formulation du Conseil d'Etat est plus lisible et décide de la reprendre.

Point 57

Sans observation, sous réserve des considérations générales.

Point 58

Article 137-64

Le Conseil d'Etat préférerait que le renvoi se fasse à l'article 130 qui concerne les sociétés coopératives.

Il propose cependant que cet article 130 soit modifié et renvoie à l'article 76 pour harmoniser les dispositions dans l'intérêt des tiers.

Compte tenu de ce qui précède, la Commission n'approuve pas la proposition du Conseil d'Etat.

L'alinéa 2 du paragraphe 1^{er} et le paragraphe 2 peuvent être supprimés, car ils sont superfétatoires.

La Commission fait sienne la remarque du Conseil d'Etat.

Article 137-65

Le Conseil d'Etat propose d'omettre cet article pour être superfétatoire, car les auteurs ont indiqué à l'endroit des articles les autorités compétentes pour établir les actes, certificats et contrôles.

La Commission décide de suivre le Conseil d'Etat, sous réserve des observations faites à l'endroit de l'article 137-44 sous le point 38).

2. **6376** **Projet de loi portant réforme de la Commission des normes comptables et modification de diverses dispositions relatives à la comptabilité et aux comptes annuels des entreprises ainsi qu'aux comptes consolidés de certaines formes de sociétés et modifiant:**
- (1) le titre II du livre Ier du Code de commerce**
 - (2) le titre II de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises**
 - (3) la section XVI de la loi modifiée du 10 août 1915 concernant les sociétés commerciales**

Examen de l'avis complémentaire du Conseil d'Etat

Le rapporteur du projet de loi, M. Léon Gloden, présente l'avis complémentaire du Conseil d'Etat du 16 avril 2013, pour les détails duquel il est prié de se référer au document parlementaire afférent.

Amendements gouvernementaux

Si le Conseil d'Etat approuve les objectifs de fond des amendements gouvernementaux à la loi en projet, il marque cependant son désaccord avec les auteurs des amendements quant à la réorganisation de la CNC sous la forme d'une fondation de droit privé.

Le Conseil d'Etat souligne que la forme juridique de la fondation telle que régie par le titre II de la prédite loi du 21 avril 1928, que les auteurs entendent adopter pour la structure juridique future de la CNC, ne convient pas, alors que la fondation est, dans l'esprit de la loi modifiée de 1928, une institution de droit privé à finalité philanthropique et que la CNC est destinée à associer des partenaires publics et privés. Par conséquent, le Conseil d'Etat s'oppose formellement aux amendements gouvernementaux.

Vu les objectifs du Gouvernement et les missions qui seront confiées à la future CNC, le Conseil d'Etat propose la constitution d'un groupement d'intérêt économique (GIE), au sens de la loi modifiée du 25 mars 1991 sur les groupements d'intérêt économique, qui regrouperait les acteurs publics et privés intervenant dans le domaine des normes comptables. Le Conseil d'Etat renvoie dans ce contexte au modèle du Registre de commerce et des sociétés constitué sous la forme juridique du GIE regroupant l'Etat, la Chambre de commerce et la Chambre des métiers.

Les membres de la Commission juridique conviennent d'élaborer des amendements parlementaires afin de tenir compte de l'opposition formelle du Conseil d'Etat.

Amendements parlementaires

Amendement 1

Sans observation.

Amendement 2

L'amendement sous avis n'appelle pas d'observation, sauf à écrire « la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif » et « la loi modifiée du 13 février 2007 relative aux fonds d'investissement spécialisés ».

La Commission fait sienne la remarque du Conseil d'Etat.

Amendement 3

L'amendement 3 vise à offrir aux sociétés de participation financière le choix entre le schéma de droit commun et un schéma particulier arrêté par règlement grand-ducal. Le commentaire des articles précise que l'expression « sociétés de participation financière » ne vise en fait que les sociétés de gestion de patrimoine familial au sens de la loi modifiée du 11 mai 2007.

Le Conseil d'Etat se demande si les sociétés de gestion de patrimoine familial relèvent vraiment du champ d'application de cette disposition, alors qu'historiquement la disposition a été introduite pour tenir compte de l'environnement spécifique des sociétés de participation financières dites « holding de 1929 », dont le statut a entretemps été aboli. Il s'y ajoute que les sociétés de gestion de patrimoine familial, telles que définies par la loi précitée, n'ont pas pour vocation première de détenir des participations financières. Le Conseil d'Etat doute également que les spécificités sectorielles des sociétés de gestion de patrimoine familial requièrent vraiment un schéma des comptes annuels qui leur soit propre. Il suggère dès lors que la CNC approfondisse son analyse, et il soulève également la question de l'opportunité d'une abolition pure et simple du règlement grand-ducal du 29 juin 1984 relatif au schéma des comptes annuels des sociétés de participation financière.

La Commission juridique propose néanmoins de maintenir le libellé du point 6, tel que proposé par l'amendement 3.

Amendements 4 à 15

Sans observation.

3. 6514 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**

Désignation d'un rapporteur

Les membres de la Commission désignent M. Gilles Roth comme rapporteur du projet de loi.

4. Approbation des projets de procès-verbal des réunions des 6, 13 et 20 mars 2013

Les projets de procès-verbal des réunions des 6, 13 et 20 mars 2013 sont approuvés.

5. Divers

Les membres de la Commission décident de convoquer une réunion le 24 avril 2013 à 9 heures avec l'ordre du jour suivant :

5974 Projet de loi modifiant la loi modifiée du 10 août 1915 concernant les sociétés commerciales en vue de mettre en œuvre le Règlement (CE) no 1435/2003 du Conseil du 22 juillet 2003 relatif au statut de la société coopérative européenne (SEC)

- Rapporteur : Monsieur Léon Gloden
- Présentation et adoption d'une série d'amendements

6514 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
- Rapporteur : Monsieur Gilles Roth

- Présentation du projet de loi
- Examen de l'avis du Conseil d'Etat

Divers

Luxembourg, le 17 avril 2013

La secrétaire,
Carole Closener

Le Président,
Gilles Roth

6514

MEMORIAL
Journal Officiel
du Grand-Duché de
Luxembourg



MEMORIAL
Amtsblatt
des Großherzogtums
Luxemburg

RECUEIL DE LEGISLATION

A — N° 157

12 août 2014

S o m m a i r e

**CYBERCRIMINALITÉ
LOI; CONVENTION ET PROTOCOLE**

Republication de la loi du 18 juillet 2014 portant

- 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001,
- 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003,
- 3) modification du Code pénal,
- 4) modification du Code d'instruction criminelle,
- 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques page **2406**

Republication de la loi du 18 juillet 2014 portant

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

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

Notre Conseil d'Etat entendu;

De l'assentiment de la Chambre des Députés;

Vu la décision de la Chambre des Députés du 4 juin 2014 et celle du Conseil d'Etat du 24 juin 2014 portant qu'il n'y a pas lieu à second vote;

Avons ordonné et ordonnons:

Art. 1^{er}. 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 231bis du Code pénal libellé comme suit:

«**Art. 231bis.**– 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 1 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 électroniques, 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 1 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 1 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, 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.»
- 2) Le paragraphe 1^{er} 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'État 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 laissé 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 1^{er} 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 laissé 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 1, 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 1 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).»

Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

Le Ministre de la Justice,
Félix Braz

Cabasson, le 18 juillet 2014.
Henri

Doc. parl. 6514; sess. ord. 2012-2013; sess. extraord. 2013 et sess. extraord. 2013-2014; Dir. 2013/40/UE.



Série des Traités européens - n 185

**CONVENTION
SUR LA CYBERCRIMINALITÉ**

Budapest, 23.XI.2001

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberspace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999);

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberspace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21^e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23^e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2^e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit:

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,

- a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
- b l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
- c l'expression «fournisseur de services» désigne:
 - i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
 - ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
- d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
- 2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:
 - a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:
 - i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
 - ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et
 - b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.
- 2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.
- 3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

*Titre 2 – Infractions informatiques***Article 7 – Falsification informatique**

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

*Titre 3 – Infractions se rapportant au contenu***Article 9 – Infractions se rapportant à la pornographie infantine**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie infantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie infantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie infantine par le biais d'un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie infantine par le biais d'un système informatique;

e la possession de pornographie infantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie infantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

- b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
 - c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.
- 3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.
- 4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
- 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
- 3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

- 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.
- 3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:
 - a sur un pouvoir de représentation de la personne morale;
 - b sur une autorité pour prendre des décisions au nom de la personne morale;
 - c sur une autorité pour exercer un contrôle au sein de la personne morale.
- 2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présente Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.
- 3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.
- 4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.
- 2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

- 2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:
- a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;
 - b à toutes les autres infractions pénales commises au moyen d'un système informatique; et
 - c à la collecte des preuves électroniques de toute infraction pénale.
- 3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.
- b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:
- i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
 - ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

- 1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
- 2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
- 3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

*Titre 2 – Conservation rapide de données informatiques stockées***Article 16 – Conservation rapide de données informatiques stockées**

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.
- 2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.
- 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic

- 1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:
 - a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et
 - b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.
- 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

*Titre 3 – Injonction de produire***Article 18 – Injonction de produire**

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

- a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et
 - b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
- 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
- 3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:
- a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
 - b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
 - c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:
- a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et
 - b à un support du stockage informatique permettant de stocker des données informatiques
- sur son territoire.
- 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

- a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;
 - b réaliser et conserver une copie de ces données informatiques;
 - c préserver l'intégrité des données informatiques stockées pertinentes;
 - d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.
- 4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.
- 5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:
- a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et
 - b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:
 - i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.
- 2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.
- 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :
 - a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et
 - b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:
 - i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.
- 2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.
- 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence**Article 22 – Compétence**

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:
 - a sur son territoire; ou
 - b à bord d'un navire battant pavillon de cette Partie; ou
 - c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou
 - d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
- 2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

- 3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.
- 4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.
- 5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

- 1
 - a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.
 - b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.
- 2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.
- 3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

- 4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.
- 5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.
- 6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.
- 7
 - a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.
 - b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

- 1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.
- 2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.
- 3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.
- 4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.
- 5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette

condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

- 1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.
- 2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

*Titre 4 – Procédures relatives aux demandes d'entraide
en l'absence d'accords internationaux applicables*

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

- 1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.
- 2
 - a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;
 - b Les autorités centrales communiquent directement les unes avec les autres;
 - c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;
 - d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.
- 3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.
- 4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:
 - a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

- b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.
- 5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.
- 6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.
- 7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.
- 8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.
- 9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.
- b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).
- c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.
- d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.
- e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

- 1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

- 2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:
 - a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou
 - b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.
- 3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.
- 4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

- 1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.
- 2 Une demande de conservation faite en application du paragraphe 1 doit préciser:
 - a l'autorité qui demande la conservation;
 - b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;
 - c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;
 - d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;
 - e la nécessité de la mesure de conservation; et
 - f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.
- 3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

- 4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.
- 5 En outre, une demande de conservation peut être refusée uniquement:
 - a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
 - b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.
- 6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.
- 7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

- 1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.
- 2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:
 - a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
 - b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

- 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au

moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

- 2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.
- 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:
 - a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou
 - b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

- a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
- b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

- 1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.
- 2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

- 1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

- a apport de conseils techniques;
 - b conservation des données, conformément aux articles 29 et 30;
 - c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.
- 2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.
b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.
- 3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

- 1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.
- 2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.
- 3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.
- 4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

- 1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.
- 2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

- 1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.
- 2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.
- 3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

- 1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:
 - de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24);
 - de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30);
 - du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).
- 2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.
- 3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

- 1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constitutants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.
- 2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.
- 3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constitutants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constitutants, en les encourageant à adopter les mesures appropriées pour les mettre en oeuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

- 1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.
- 2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.
- 3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

- 1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.
- 2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.
- 3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.
- 4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.
- 5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

- 1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.
- 2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

- 1 Les Parties se concertent périodiquement, au besoin, afin de faciliter:
 - a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;
 - b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;
 - c l'examen de l'éventualité de compléter ou d'amender la Convention.
- 2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

- 3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.
- 4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.
- 5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

- 1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.
- 2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

- a toute signature;
- b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;
- c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37;
- d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42;
- e tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.



Série des traités européens n° 189

**PROTOCOLE ADDITIONNEL A LA
CONVENTION SUR LA
CYBERCRIMINALITE, RELATIF A
L'INCRIMINATION D'ACTES DE
NATURE RACISTE ET XENOPHOBE
COMMIS PAR LE BIAIS DE SYSTEMES
INFORMATIQUES**

Strasbourg, 28.I.2003

Les Etats membres du Conseil de l'Europe et les autres Etats parties à la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, signataires du présent Protocole ;

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Rappelant que tous les êtres humains sont nés libres et égaux en dignité et en droits ;

Soulignant la nécessité de garantir une mise en œuvre exhaustive et efficace de tous les droits de l'homme sans distinction ni discrimination, tels qu'énoncés dans les instruments européens et autres instruments internationaux ;

Convaincus que des actes de nature raciste et xénophobe constituent une violation des droits de l'homme, ainsi qu'une menace pour l'Etat de droit et la stabilité démocratique ;

Considérant que le droit national et le droit international nécessitent de prévoir une réponse juridique adéquate à la propagande de nature raciste et xénophobe diffusée par le biais des systèmes informatiques ;

Conscients que la propagande de tels actes est souvent criminalisée par les législations nationales ;

Ayant égard à la Convention sur la cybercriminalité qui prévoit des moyens flexibles et modernes de coopération internationale, et convaincus de la nécessité d'harmoniser la lutte contre la propagande raciste et xénophobe ;

Conscients de ce que les systèmes informatiques offrent un moyen sans précédent de faciliter la liberté d'expression et de communication dans le monde entier ;

Reconnaissant que la liberté d'expression constitue l'un des principaux fondements d'une société démocratique, et qu'elle est l'une des conditions essentielles de son progrès et de l'épanouissement de chaque être humain ;

Préoccupés toutefois par le risque que ces systèmes informatiques soient utilisés à mauvais escient ou de manière abusive pour diffuser une propagande raciste et xénophobe ;

Convaincus de la nécessité d'assurer un bon équilibre entre la liberté d'expression et une lutte efficace contre les actes de nature raciste et xénophobe ;

Reconnaissant que ce Protocole ne porte pas atteinte aux principes établis dans le droit interne concernant la liberté d'expression ;

Tenant compte des instruments juridiques internationaux pertinents dans ce domaine, et en particulier de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales et de son Protocole n° 12 relatif à l'interdiction générale de la discrimination, des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, en particulier de la Convention sur la cybercriminalité et de la Convention internationale des Nations Unies du 21 décembre 1965 sur l'élimination de toutes les formes de discrimination raciale, l'Action commune du 15 juillet 1996 de l'Union européenne adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne concernant l'action contre le racisme et la xénophobie ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la cybercriminalité, ainsi que celle contre le racisme et la xénophobie ;

Prenant également en compte le Plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet, tenu à Strasbourg les 10 et 11 octobre 1997, afin de chercher des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit :

Chapitre I – Dispositions communes

Article 1 – But

Le but du présent Protocole est de compléter, pour les Parties au Protocole, les dispositions de la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001 (appelé ci-après « la Convention ») eu égard à l'incrimination des actes de nature raciste et xénophobe diffusés par le biais de systèmes informatiques.

Article 2 – Définition

- 1 Aux fins du présent Protocole, l'expression :

« *matériel raciste et xénophobe* » désigne tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes.

- 2 Les expressions et termes employés dans ce Protocole sont interprétés de la même manière qu'ils le sont dans la Convention.

Chapitre II – Mesures à prendre au niveau national

Article 3 – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants :

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe.

- 2 Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.
- 3 Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.

Article 4 – Menace avec une motivation raciste et xénophobe

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant :

la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 5 – Insulte avec une motivation raciste et xénophobe

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant :

l'insulte en public, par le biais d'un système informatique, (i) d'une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.

- a soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule ;
- b soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Article 6 – Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité

- 1 Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants :

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.

- 2 Une Partie peut :
 - a soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ;
 - b soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Article 7 – Aide et complicité

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, en vertu de son droit interne, lorsqu'il est commis intentionnellement et sans droit, le fait d'aider à perpétrer une infraction telle que définie dans ce Protocole, ou d'en être complice, avec l'intention qu'une telle infraction soit commise.

Chapitre III – Relations entre la Convention et ce Protocole

Article 8 – Relations entre la Convention et ce Protocole

- 1 Les articles 1, 12, 13, 22, 41, 44, 45 et 46 de la Convention s'appliquent, *mutatis mutandis*, à ce Protocole.
- 2 Les Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole.

Chapitre IV – Dispositions finales

Article 9 – Expression du consentement à être lié

- 1 Le présent Protocole est ouvert à la signature des Etats signataires de la Convention, qui peuvent exprimer leur consentement à être liés par :
 - a la signature sans réserve de ratification, d'acceptation ou d'approbation ; ou
 - b la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.
- 2 Un Etat ne peut signer le présent Protocole sans réserve de ratification, d'acceptation ou d'approbation ni déposer un instrument de ratification, d'acceptation ou d'approbation s'il n'a pas déjà déposé ou ne dépose pas simultanément un instrument de ratification, d'acceptation ou d'approbation de la Convention.
- 3 Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

Article 10 – Entrée en vigueur

- 1 Le présent Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats auront exprimé leur consentement à être liés par le Protocole conformément aux dispositions de l'article 9.
- 2 Pour tout Etat qui exprimera ultérieurement son consentement à être lié par le Protocole, celui-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de sa signature sans réserve de ratification, d'acceptation ou d'approbation ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation.

Article 11 – Adhésion

- 1 Après l'entrée en vigueur du présent Protocole, tout Etat qui a adhéré à la Convention pourra adhérer également au Protocole.
- 2 L'adhésion s'effectuera par le dépôt, près le Secrétaire Général du Conseil de l'Europe, d'un instrument d'adhésion qui prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de son dépôt.

Article 12 – Réserves et déclarations

- 1 Les réserves et les déclarations formulées par une Partie concernant une disposition de la Convention s'appliqueront également à ce Protocole, à moins que cette Partie n'exprime l'intention contraire au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion.
- 2 Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou des réserves prévues aux articles 3, 5 et 6 du présent Protocole. Une Partie peut aussi

formuler, par rapport aux dispositions de ce Protocole, les réserves prévues à l'article 22, paragraphe 2, et à l'article 41, paragraphe 1, de la Convention, sans préjudice de la mise en œuvre faite par cette Partie par rapport à la Convention. Aucune autre réserve ne peut être formulée.

- 3 Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la possibilité de prévoir des éléments additionnels, tels que prévus à l'article 5, paragraphe 2.a, et à l'article 6, paragraphe 2.a, de ce Protocole.

Article 13 – Statut et retrait des réserves

- 1 Une Partie qui a fait une réserve conformément à l'article 12 ci-dessus retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception d'une notification de retrait par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.
- 2 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves en application de l'article 12 des informations sur les perspectives de leur retrait.

Article 14 – Application territoriale

- 1 Toute Partie peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera le présent Protocole.
- 2 Toute Partie peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de ce Protocole à tout autre territoire désigné dans la déclaration. Le Protocole entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.
- 3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 15 – Dénonciation

- 1 Toute Partie peut, à tout moment, dénoncer le présent Protocole par notification au Secrétaire Général du Conseil de l'Europe.
- 2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 16 – Notification

Le Secrétaire Général du Conseil de l'Europe notifiera aux Etats membres du Conseil de l'Europe, aux Etats non-membres ayant participé à l'élaboration du présent Protocole, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

- a toute signature ;
- b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion ;
- c toute date d'entrée en vigueur du présent Protocole conformément à ses articles 9, 10 et 11 ;
- d tout autre acte, notification ou communication ayant trait au présent Protocole.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé le présent Protocole.

Fait à Strasbourg, le 28 janvier 2003, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non-membres ayant participé à l'élaboration du présent Protocole et à tout Etat invité à y adhérer.
