

N° 6514

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: (Monsieur François Biltgen, Ministre de la Justice): 12.12.2012

Transmis en copie pour information

- aux Membres de la Commission juridique
- aux Membres de la Conférence des Présidents

Luxembourg, le 12 décembre 2012

Le Secrétaire général de la Chambre des Députés,



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

(s.) Henri

Le Ministre de la Justice,
(s.) François BILTGEN

POUR EXPEDITION CONFORME

Pour le Ministre de la Justice,



Guy SCHLEDER
Administrateur général

*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.**

I. - 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 1^{er} 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. ».

¹ Projet de loi n° 6388

- 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 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 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 :

« 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).».

*

II. - Exposé 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 sus-mentionnés. 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 la 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 1^{er} 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 ;
- 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 1^{er} 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 que des qu'il n'y a pas de modifications législatives à prévoir.

*

III.- Commentaire des articles

Article 1^{er} 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 où 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 1^{er} 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 manœuvres 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 illégal, 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 1^{er} de la directive : « *un accès, une atteinte à l'intégrité, une interception, ou tout autre comportement visé dans la présente*

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

Ad article 67-1 du Code d'instruction criminelle

Cette modification est le corolaire 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.

*

IV. – 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 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 enfantine

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 enfantine en vue de sa diffusion par le biais d'un système informatique;
- b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» 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 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 constituants 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.

*

V. – 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 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.

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 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.



Fiche d'évaluation d'impact

Mesures législatives, réglementaires et autres

Intitulé du projet:	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.
Ministère initiateur:	Ministère de la Justice
Auteur(s) :	Laurent THYES, Attaché de Gouvernement 1 ^{er} en rang
Tél :	247 88529
Courriel :	laurent.thyes@mj.etat.lu
Objectif(s) du projet :	Ratification de la Convention du Conseil de l'Europe sur la cybercriminalité et de son protocole
Autre(s) Ministère(s)/Organisme(s)/Commune(s) impliqué(e)s :	Ministère de l'Economie et du Commerce extérieur, Ministère d'Etat (Service des Médias et des Communications)
Date :	09/11/2012

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s) : Oui Non

Si oui, laquelle/lesquelles : Parquet général, Parquet TA Luxembourg, Cabinet d'instruction Luxembourg, Police Grand-Ducale

Remarques/Observations :

2. Destinataires du projet :

- Entreprises/Professions libérales :
- Citoyens :
- Administrations :

Oui Non
Oui Non
Oui Non

3. Le principe « Think small first » est-il respecté ?
(c.à d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Oui Non N.a.

Remarques/Observations :

4. Le projet est-il lisible et compréhensible pour le destinataire ?
Existe-t-il un texte coordonné ou un guide pratique, mis à jour

Oui Non
Oui Non

¹ N.a. : non applicable.

et publié d'une façon régulière ?

Remarques/Observations :

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ?

Oui Non

Remarques/Observations :

6. Le projet contient-il une charge administrative² pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui Non
- Si oui, quel est le coût administratif³ approximatif total ?
(nombre de destinataires x coût administratif par destinataire)
7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui Non N.a.
- Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
- b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel⁴ ? Oui Non N.a.
- Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
8. Le projet prévoit-il :
- une autorisation tacite en cas de non réponse de l'administration ? Oui Non N.a.
 - des délais de réponse à respecter par l'administration ? Oui Non N.a.
 - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui Non N.a.
9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui Non N.a.
- Si oui, laquelle :
10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Sinon, pourquoi ? Oui Non N.a.
11. Le projet contribue-t-il en général à une :
- a. simplification administrative, et/ou à une Oui Non
 - b. amélioration de la qualité réglementaire ? Oui Non
- Remarques/Observations :
12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui Non N.a.
13. Y-a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui Non
- Si oui, quel est le délai pour disposer du nouveau système ?
14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui Non N.a.
- Si oui, lequel ?
- Remarques/Observations :

² Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en œuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

³ Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple : taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

⁴ Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

Egalité des chances

15. Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? Oui Non
- positif en matière d'égalité des femmes et des hommes ? Oui Non
Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? Oui Non
Si oui, expliquez pourquoi :

- négatif en matière d'égalité des femmes et des hommes ? Oui Non
Si oui, expliquez de quelle manière :

16. Y a-t-il un impact financier différent sur les femmes et les hommes ?

Oui Non N.a.

Si oui, expliquez de quelle manière :

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation ⁵? Oui Non N.a.

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers ⁶? Oui Non N.a.

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

⁵ Article 15 paragraphe 2 de la directive « services » (cf. Note explicative, p.10-11)

⁶ Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p.10-11)