

ECRI

European Commission against Racism and Intolerance
Commission européenne contre le racisme et l'intolérance

PC.DEL/609/03
19 June 2003

FRENCH
Original: ENGLISH
FRENCH

CRI (2003) 41

Commission européenne contre le racisme et l'intolérance

Conférence de l'OSCE
sur l'antisémitisme
19-20 juin 2003, Vienne

Documents d'information fournis par la
Commission européenne contre le racisme et
l'intolérance

Strasbourg, Mai 2003



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Secrétariat de l'ECRI
Direction Générale des Droits de l'Homme – DG II
Conseil de l'Europe
F - 67075 STRASBOURG Cedex
Tel.: +33 (0) 3 88 41 29 64
Fax: +33 (0) 3 88 41 39 87
E-mail: combat.racism@coe.int

Visitez notre site web : www.coe.int/ecri

Texte du Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003..... 5

Texte du Rapport explicatif 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 tel qu'adopté par le Comité des Ministres le 7 novembre 2002 15

Texte de la Convention sur la cybercriminalité, 23 novembre 2001 23



Série des traités européens n° 189

**PROTOCOLE ADDITIONNEL A LA
CONVENTION SUR LA
CYBERCRIMINALITE, RELATIF A
L'INCRIMINATION D'ACTES DE
NATURE RACISTE ET XENOPHOBE
COMMIS PAR LE BIAIS DE SYSTEMES
INFORMATIQUES**

Strasbourg, 28.I.2003

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sont convenus de ce qui suit :

Chapitre I – Dispositions communes

Article 1 – But

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

Article 2 – Définition

1 Aux fins du présent Protocole, l'expression :

« *matériel raciste et xénophobe* » désigne tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la

religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes.

- 2 Les expressions et termes employés dans ce Protocole sont interprétés de la même manière qu'ils le sont dans la Convention.

Chapitre II – Mesures à prendre au niveau national

Article 3 – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques

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

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

- 2 Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.
- 3 Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.

Article 4 – Menace avec une motivation raciste et xénophobe

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

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

Article 5 – Insulte avec une motivation raciste et xénophobe

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

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

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

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

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

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

- 2 Une Partie peut :

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

Article 7– Aide et complicité

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

Chapitre III – Relations entre la Convention et ce Protocole

Article 8– Relations entre la Convention et ce Protocole

- 1 Les articles 1, 12, 13, 22, 41, 44, 45 et 46 de la Convention s'appliquent, *mutatis mutandis*, à ce Protocole.
- 2 Les Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole.

Chapitre IV – Dispositions finales

Article 9– Expression du consentement à être lié

- 1 Le présent Protocole est ouvert à la signature des Etats signataires de la Convention, qui peuvent exprimer leur consentement à être liés par :
 - a la signature sans réserve de ratification, d'acceptation ou d'approbation ; ou
 - b la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.
- 2 Un Etat ne peut signer le présent Protocole sans réserve de ratification, d'acceptation ou d'approbation ni déposer un instrument de ratification, d'acceptation ou d'approbation s'il n'a pas déjà déposé ou ne dépose pas simultanément un instrument de ratification, d'acceptation ou d'approbation de la Convention.
- 3 Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

Article 10– Entrée en vigueur

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

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

Article 11 – Adhésion

- 1 Après l'entrée en vigueur du présent Protocole, tout Etat qui a adhéré à la Convention pourra adhérer également au Protocole.
- 2 L'adhésion s'effectuera par le dépôt, près le Secrétaire Général du Conseil de l'Europe, d'un instrument d'adhésion qui prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de son dépôt.

Article 12 – Réserves et déclarations

- 1 Les réserves et les déclarations formulées par une Partie concernant une disposition de la Convention s'appliqueront également à ce Protocole, à moins que cette Partie n'exprime l'intention contraire au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion.
- 2 Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou des réserves prévues aux articles 3, 5 et 6 du présent Protocole. Une Partie peut aussi formuler, par rapport aux dispositions de ce Protocole, les réserves prévues à l'article 22, paragraphe 2, et à l'article 41, paragraphe 1, de la Convention, sans préjudice de la mise en œuvre faite par cette Partie par rapport à la Convention. Aucune autre réserve ne peut être formulée.
- 3 Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la possibilité de prévoir des éléments additionnels, tels que prévus à l'article 5, paragraphe 2.a, et à l'article 6, paragraphe 2.a, de ce Protocole.

Article 13 – Statut et retrait des réserves

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

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

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

Article 14 – Application territoriale

- 1 Toute Partie peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera le présent Protocole.
- 2 Toute Partie peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de ce Protocole à tout autre territoire désigné dans la déclaration. Le Protocole entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.
- 3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 15 – Dénonciation

- 1 Toute Partie peut, à tout moment, dénoncer le présent Protocole par notification au Secrétaire Général du Conseil de l'Europe.
- 2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 16 – Notification

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

- a toute signature ;

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

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé le présent Protocole.

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

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 [STE n° 189]

Rapport explicatif

(tel qu'adopté par le Comité des Ministres le 7 novembre 2002)

Le texte de ce Rapport explicatif ne constitue pas un instrument d'interprétation authentique du texte du Protocole, bien qu'il puisse faciliter la compréhension des dispositions qui y sont contenues. Le Protocole a été ouvert à la signature à Strasbourg, le 28 janvier 2003, à l'occasion de la Première Partie de la session 2003 de l'Assemblée parlementaire.

INTRODUCTION

1. Depuis l'adoption de la Déclaration universelle des droits de l'homme en 1948 la communauté internationale a réalisé des progrès importants dans la lutte contre le racisme, la discrimination raciale, la xénophobie et l'intolérance qui y est associée. Des règles ont été adoptées aux niveaux national et international et un certain nombre d'instruments internationaux de protection des droits de l'homme a été mis en place, notamment la Convention internationale de New York de 1965 sur l'élimination de toute forme de discrimination raciale (CERD) qui a été élaborée dans le cadre des Nations Unies. En dépit de ces progrès, le rêve d'un monde sans haine ni discrimination raciale ne s'est que partiellement concrétisé.
2. Alors que les développements technologiques, économiques et commerciaux rapprochent les peuples du monde entier, la discrimination raciale, la xénophobie et d'autres formes d'intolérance continuent d'exister dans nos sociétés. La mondialisation présente des risques pouvant conduire à l'exclusion et à l'accroissement des inégalités, très souvent sur une base raciale et ethnique.
3. En particulier, l'apparition de réseaux de communication globale comme Internet offre à certaines personnes des moyens modernes et puissants pour soutenir le racisme et la xénophobie et pour diffuser facilement et largement des contenus exprimant de telles idées. Pour pouvoir mener des enquêtes et poursuivre ces personnes, la coopération internationale est essentielle. La Convention sur la cybercriminalité (STE 185), appelée ci-après «la Convention», a été élaborée pour permettre une entraide concernant les crimes informatiques au sens large du terme, conçue de manière souple et moderne. Ce Protocole poursuit deux objectifs : premièrement, harmoniser le droit pénal matériel dans la lutte contre le racisme et la xénophobie sur l'Internet et deuxièmement, améliorer la coopération internationale dans ce domaine. Une harmonisation de ce type facilite la lutte contre cette criminalité aux niveaux national et international. Prévoir des infractions correspondantes dans le droit interne peut prévenir l'abus des systèmes informatiques à des fins racistes dans des Parties qui n'ont pas une législation très bien définies dans ce domaine. La coopération internationale (en particulier l'extradition et l'entraide judiciaire) se trouve facilitée, par exemple en ce qui concerne la règle de la double incrimination.
4. Le comité chargé de rédiger la Convention a examiné la possibilité d'inclure des infractions liées au contenu autres que la pornographie infantile, comme la diffusion de propagande raciste par le biais de systèmes informatiques. Toutefois, le comité n'a pas pu parvenir à un consensus concernant l'incrimination d'un tel comportement. Alors que beaucoup de délégations se sont déclarées favorables à l'idée d'en faire une infraction pénale, plusieurs se sont dites très préoccupées par cette démarche qui porterait atteinte à la liberté d'expression. En raison de la complexité de cette question, il a été décidé que le comité saisisrait le Comité européen pour les problèmes criminels (CDPC) de la question de la rédaction d'un protocole additionnel à la Convention.

5. L'Assemblée parlementaire, dans son Avis no 226(2001), a recommandé la rédaction sur le champ d'un protocole additionnel à la future Convention, intitulé «élargissement du champ d'application de la Convention à de nouvelles formes d'infractions», qui définisse et incrimine notamment la diffusion de propagande raciste.

6. Le Comité des Ministres a donc confié au Comité européen pour les problèmes criminels (CDPC), et notamment à son Comité d'experts sur l'incrimination des actes de nature raciste et xénophobe par le biais de systèmes informatiques (PC-RX), le soin de rédiger un projet de protocole additionnel, instrument juridique obligatoire ouvert à la signature et à la ratification des Parties contractantes à la Convention, pour traiter en particulier des questions suivantes :

i. la définition et l'étendue d'éléments en vue de l'incrimination des actes de nature raciste et xénophobe commis à travers les réseaux informatiques, y compris la production, l'offre, la diffusion ou d'autres formes de dissémination de matériels ou de messages avec un tel contenu, à travers les réseaux informatiques ;

ii. la mesure dans laquelle les dispositions de droit matériel, procédural et de coopération internationale contenues dans la Convention sur la cybercriminalité s'appliquent aux enquêtes et aux poursuites relatives aux infractions à établir dans le Protocole additionnel.

7. Ce protocole comporte un élargissement de la portée de la Convention, y compris de ses dispositions sur le fond, la procédure et la coopération internationale, de manière à couvrir également les infractions concernant la propagande raciste et xénophobe. Ainsi, outre l'harmonisation des éléments de droit matériel concernant ces comportements, le Protocole vise à améliorer la possibilité qu'ont les Parties d'utiliser dans ce domaine les moyens de coopération internationale prévus par la Convention.

COMMENTAIRES CONCERNANT LES ARTICLES DU PROTOCOLE

Chapitre I – Dispositions communes

Article 1 – Objet

8. Le but du présent Protocole est de compléter, pour les Parties au Protocole les dispositions de la Convention par l'incrimination des actes de nature raciste et xénophobe commis par le biais des systèmes informatiques.

9. Les dispositions du Protocole ont un caractère obligatoire. Pour satisfaire à ces obligations, les Etats parties doivent non seulement promulguer une législation appropriée, mais aussi veiller à ce qu'elle soit correctement mise en œuvre.

Article 2 – Définition

Paragraphe 1 - «Matériel raciste et xénophobe»

10. De nombreux instruments juridiques ont été élaborés aux niveaux international et national pour lutter contre le racisme ou la xénophobie. Les rédacteurs de ce Protocole ont notamment pris en compte i. la Convention internationale sur l'élimination de toutes les formes de discrimination raciale; ii. le Protocole no 12 (STE 177) à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (CEDH); (iii) 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 des actions pour combattre le racisme et la xénophobie ; iv. la Conférence mondiale contre le racisme, la discrimination raciale, la xénophobie et l'intolérance qui y est associée (Durban, 30 août-8 septembre 2001); v. les conclusions de la Conférence européenne contre le racisme (Strasbourg, 13 octobre 2000); vi. l'étude complète publiée en août 2000 par la Commission européenne contre le racisme et l'intolérance (ECRI) (ECRI(2000)27) et vii. la proposition de la Commission européenne de novembre 2001 pour une décision-cadre du Conseil de l'Union européenne sur la lutte contre le racisme et la xénophobie.

11. L'article 10 de la CEDH reconnaît le droit à la liberté d'expression, qui inclut la liberté d'avoir une opinion et de recevoir et de transmettre des informations et des idées. Comme l'a précisé la Cour dans sa jurisprudence « l'article 10 de la CEDH vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'Etat ou une fraction quelconque de la population (1) ». Toutefois, la Cour a établi que les actions des Etats visant à restreindre le droit à la liberté d'expression étaient

justifiées au regard du paragraphe 2 de l'article 10 de la CEDH, notamment lorsque ces idées et ces expressions portent atteinte aux droits des tiers. Ce Protocole, sur la base des instruments nationaux et internationaux, établit dans quelle mesure la diffusion d'expressions et d'idées racistes et xénophobes porte atteinte aux droits des individus.

12. La définition contenue à l'article 2 fait référence au matériel écrit (par exemple, textes, livres, magazines, déclarations, messages, etc.), aux images (par exemple, illustrations, photos, dessins, etc.) ou à toute autre représentation d'idées ou de théories, de nature raciste et xénophobe, dans un format tel qu'il puisse être conservé, traité et transmis par le biais d'un système informatique.

13. La définition contenue à l'article 2 de ce Protocole se réfère à un comportement auquel le contenu du matériel peut mener, plutôt qu'à l'expression de sentiments/de convictions/d'aversion contenue dans le matériel en question. La définition est fondée, dans la mesure du possible, sur les définitions et les documents nationaux et internationaux existants (NU, UE).

14. Ce matériel doit préconiser et encourager la haine, la discrimination ou la violence ou inciter à de tels actes. « Préconiser » se réfère à un plaidoyer en faveur de la haine, de la discrimination ou de la violence, « encourager » se réfère à promouvoir ou aider la haine, la discrimination ou la violence et « inciter » se réfère à presser d'autres à agir avec haine, discrimination ou violence.

15. L'expression « violence » se réfère à l'usage illégal de la force, alors que le mot « haine » correspond à une extrême aversion ou volonté d'offenser.

16. En interprétant le terme « discrimination », la CEDH (article 14 et Protocole n° 12) et la jurisprudence pertinente, ainsi que l'article 1 du CERD (qui contient des détails sur la notion de « discrimination raciale »), devraient être gardés à l'esprit. L'interdiction de discriminer contenue dans la CEDH garantit à toute personne relevant de la juridiction d'un Etat Partie l'égalité dans l'exercice des droits et libertés contenus dans la CEDH. L'article 14 de la CEDH établit une obligation générale pour les Etats d'interdire la discrimination, accessoire aux droits et libertés qui sont garantis par la CEDH. Dans ce contexte, la « discrimination » évoque un traitement différent injustifié réservé à des personnes ou à un groupe de personnes en fonction de certaines caractéristiques. Dans plusieurs arrêts (par exemple, l'arrêt Linguistique belge, l'arrêt Abdulaziz, Cabales et Balkandali [\(2\)](#)), la Cour européenne des Droits de l'Homme déclare: « une distinction est discriminatoire si elle "manque de justification objective et raisonnable", c'est-à-dire si elle ne poursuit pas un "but légitime" ou s'il n'y a pas de "rapport raisonnable de proportionnalité entre les moyens employés et le but visé" » (arrêt du 28 mai 1985, série A, no 94, paragraphe 72). Le point de savoir si un traitement est ou non discriminatoire doit être examiné à la lumière des circonstances particulières. En ce qui concerne plus particulièrement la discrimination raciale, une indication pour l'interprétation de ce terme peut être trouvée à l'article 1 du CERD qui établit que « discrimination raciale » vise « toute distinction, exclusion, restriction ou préférence fondée sur la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, qui a pour but ou pour effet de détruire ou de compromettre la reconnaissance, la jouissance ou l'exercice, dans des conditions d'égalité, des droits de l'homme et des libertés fondamentales dans les domaines politique, économique, social et culturel ou dans tout autre domaine de la vie publique ».

17. La haine, la discrimination ou la violence peuvent être dirigés contre une personne ou un groupe de personnes, en raison de leur appartenance à un groupe caractérisé par « 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 ».

18. Ces motifs ne sont pas exactement identiques à ceux énumérés à l'article 1 du Protocole no 12 à la CEDH, par exemple, car certains des motifs contenus dans cet article sont étrangers au concept de racisme ou de xénophobie, ni à ceux énoncés dans la Convention internationale sur l'élimination de toutes les formes de discrimination raciale, qui traite de la « discrimination raciale » en général et non du « racisme » en tant que tel. En général, ces motifs doivent être interprétés selon le droit et la pratique nationaux et internationaux. Toutefois, certains d'entre eux requièrent des explications supplémentaires quant à leur signification spécifique dans le contexte de ce Protocole.

19. « L'ascendance » se réfère essentiellement aux personnes ou groupes de personnes dont certains ascendants pouvaient être identifiées par des caractéristiques (telles que la race ou la couleur). Toutefois, même si ces caractéristiques n'existent pas nécessairement à l'heure actuelle, en raison de leur ascendance, ces personnes ou groupes de personnes peuvent encore être sujet à la haine, à la discrimination ou à la violence. « L'ascendance » ne se réfère pas à l'origine sociale.

20. La notion « d'origine nationale », doit être interprétée dans un large sens factuel. Il peut se référer à l'histoire d'une personne, non seulement quant à la nationalité ou l'origine de ses ancêtres, mais aussi par rapport à sa propre appartenance nationale, indépendamment du fait que cette personne possède ou non cette nationalité au sens juridique du terme. Lorsqu'une personne possède plusieurs nationalités ou est apatride, l'interprétation large de cette notion permet de la protéger si elle est discriminée sur la base de l'un de ces motifs. De plus, la notion « d'origine nationale » peut non seulement se référer à l'appartenance à un Pays qui est reconnu comme tel par la communauté internationale, mais aussi aux minorités ou à tout autre groupe de personne avec des caractéristiques similaires.

21. La notion de « religion » se trouve souvent dans les instruments internationaux et dans la législation nationale. Ce terme se réfère à des convictions et à des croyances. Inclure ce terme en tant que tel dans la définition pourrait entraîner le risque de dépasser le champ d'application du Protocole. Toutefois, la religion peut être utilisée comme prétexte, alibi ou substitut aux autres facteurs énumérés dans la définition. Le terme « religion » doit donc être interprétée dans ce sens limité.

Paragraphe 2

22. En veillant à ce que les termes et les expressions utilisés dans le Protocole soient interprétés conformément à la Convention, cet article garantit une interprétation uniforme des deux textes. Ceci veut dire que les termes et les expressions employés dans ce Rapport explicatif sont interprétés de la même manière que dans le Rapport explicatif de la Convention.

Chapitre II – Mesures à prendre au niveau national

Considérations générales

23. Les infractions telles que définies dans ce Protocole contiennent un certain nombre d'éléments communs qui ont été repris de la Convention. Pour plus de clarté, les paragraphes correspondants du Rapport Explicatif de la Convention ont été reproduits ci-après.

24. Une caractéristique des infractions en question est que leurs auteurs doivent expressément avoir agi « sans droit ». Cette expression rend compte du fait que le comportement décrit n'est pas toujours punissable en soi, mais peut être légal ou justifié non seulement par des exceptions légales classiques (consentement, légitime défense ou nécessité), mais dans les cas où d'autres principes ou intérêts excluent toute responsabilité pénale (par exemple à des fins de maintien de l'ordre, de recherche ou académiques). L'expression « sans droit » tire son sens du contexte dans lequel elle est utilisée. Ainsi, sans restreindre la marge de manœuvre qu'ont les Parties pour interpréter ce concept dans leur droit interne, cette expression peut renvoyer à un comportement qui ne repose sur aucune compétence (législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou à un comportement qui n'est couvert ni par des exceptions légales, excuses et faits justificatifs établis, ni par des principes de droit interne pertinents. Le Protocole ne concerne pas, par conséquent, les comportements conformes aux compétences gouvernementales légales (par exemple, lorsque le gouvernement de la Partie concernée agit dans un but de maintien de l'ordre public, de protection de la sécurité nationale ou dans le cadre d'une instruction pénale). De plus, les activités légitimes et ordinaires inhérentes à la conception des réseaux ainsi que les pratiques d'exploitation ou de commerce légitimes ou ordinaires ne devraient pas être érigées en infractions pénales. Il appartient aux Parties de déterminer les modalités d'application desdites exceptions dans leur ordre juridique interne (en droit pénal ou autre).

25. Toutes les infractions énumérées dans le Protocole doivent être commises de façon « intentionnelle » pour que la responsabilité pénale soit engagée. Dans certains cas, un élément intentionnel spécifique supplémentaire fait partie intégrante de l'infraction. Les auteurs du Protocole, comme ceux de la Convention, se sont entendus pour considérer que l'interprétation du mot « intentionnellement » doit être laissée aux droits internes. Une personne ne peut être responsable pour une quelconque infraction contenue dans ce Protocole si elle n'a pas agi avec intention délictueuse. Il ne suffit pas, par exemple, pour que la responsabilité pénale d'un fournisseur de services soit engagée, que ce dernier sert d'intermédiaire pour la transmission de ce type de matériel par le biais d'un site Web ou d'un bavardoir, en l'absence de l'intention requise en droit interne dans le cas particulier. De plus, un fournisseur de service n'est pas tenu de surveiller le contenu pour éviter la responsabilité pénale.

26. En ce qui concerne la définition de « système informatique », elle est identique à celle contenue dans la Convention et expliquée dans son Rapport explicatif.

Article 3 – Diffusion de matériel raciste et xénophobe dans les systèmes informatiques

27. Cet article exige des Etats Parties d'incriminer la diffusion ou les autres formes de mise à disposition du public de matériel raciste et xénophobe par le biais d'un système informatique.

28. Par « diffusion », il faut entendre l'action consistant à disséminer du matériel raciste et xénophobe à autrui, tandis que la « mise à disposition » désigne l'action consistant à mettre du matériel raciste et xénophobe en ligne pour qu'il soit utilisé par autrui. Cette expression englobe par ailleurs la création ou la compilation d'hyperliens visant à faciliter l'accès à ce matériel.

29. Le terme « au/du public » utilisé à l'article 3 indique clairement que toute conversation ou expression privée communiquée ou transmise par le biais d'un système informatique ne rentre pas dans le champ d'application de cette disposition. En effet, de telles communications ou expressions, comme d'autres formes traditionnelles de correspondance, sont protégées par l'article 8 de la CEDH.

30. La question de déterminer si une communication de matériel raciste et xénophobe doit être considérée comme une communication privée ou une diffusion au public, doit être examinée à la lumière de circonstances spécifiques. En premier lieu, ce qui importe est la volonté de l'émetteur du message de le transmettre à une personne déterminée. La présence de cette intention subjective peut être établie sur la base d'un certain nombre de facteurs objectifs, tels que le contenu du message, la technologie employée, les mesures de sécurité appliquées, le contexte dans lequel celui-ci est émis. Lorsque ces messages sont envoyés à plusieurs récepteurs à la fois, le nombre de récepteurs et la nature de la relation entre l'émetteur et le récepteur sont des facteurs pertinents pour déterminer si une telle communication peut encore être considérée comme privée.

31. Echanger du matériel raciste et xénophobe dans un *chat-room*, le distribuer dans des newsgroups ou des forums de discussion, sont des exemples de mise à disposition du public d'un tel matériel. Dans ce cas, le matériel est accessible à toute personne. Même lorsque l'accès à ce matériel exigerait une autorisation par le biais d'un mot de passe, le matériel en question serait accessible au public lorsque cette autorisation est donnée à tout le monde ou à toute personne qui présente certains critères. Afin de déterminer si la mise à disposition ou la diffusion était ou non au public, la nature de la relation entre les personnes concernées devrait être prise en considération.

32. Les paragraphes 2 et 3 visent à prévoir une possibilité de réserve dans des cas tout à fait limités. Ces paragraphes devraient être lus ensemble et en séquence. Une Partie a, premièrement, la possibilité de ne pas imposer de responsabilité pénale aux comportements prévus dans cet article, lorsque le matériel préconise, encourage ou incite à la discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. Par exemple, ces recours peuvent être de nature civile ou administrative. Lorsqu'une Partie ne peut pas, à cause de principes établis dans son système juridique interne concernant la liberté d'expression, prévoir de tels recours, elle peut se réserver le droit de ne pas appliquer l'obligation contenue au paragraphe 1 de cet article, si elle concerne seulement le fait de préconiser, encourager ou inciter à une discrimination qui n'est pas associée à la haine ou à la violence. Une Partie peut aussi restreindre encore le champ d'application de cette réserve en prévoyant que la discrimination vise, par exemple, à insulter, dégrader ou menacer un groupe de personnes.

Article 4 – Menace avec une motivation raciste et xénophobe

33. La plupart des législations prévoient déjà l'incrimination de la menace en général. Les rédacteurs sont convenus de souligner dans le Protocole que, sans aucun doute, la menace avec une motivation raciste et xénophobe doit être pénalement sanctionnée.

34. La notion de « menace » peut se référer à une intimidation qui provoque la crainte chez la personne envers laquelle la menace est dirigée, qu'elle risque d'être victime d'une infraction pénale grave (par exemple, qui porte atteinte à la vie, à l'intégrité physique ou personnelle, aux biens, etc., de la victime ou de sa famille). Les Etats déterminent librement ce qui constitue une infraction pénale grave.

35. Selon cette disposition, la menace doit s'adresser soit (i) à une personne au motif qu'elle appartient à un groupe caractérisé 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, soit (ii) à un groupe de personnes défini par l'une de ces caractéristiques. La menace ne doit pas être nécessairement faite en public. En effet, cet article couvre aussi la menace privée.

Article 5 – Insulte avec une motivation raciste et xénophobe

36. L'article 5 traite de l'insulte en public, d'une personne ou d'un groupe au motif qu'ils appartiennent ou sont considérés comme appartenant à un groupe avec certaines caractéristiques. La notion « d'insulte » se réfère à toute expression outrageante, terme de mépris ou invective qui porte atteinte à l'honneur ou à la dignité de la personne. Il devrait clairement résulter de l'expression elle-même que l'insulte directement liée à l'appartenance à un groupe de la personne insultée. Contrairement au cas de la menace, l'insulte exprimée lors d'une communication privée n'est pas couverte par cette disposition.

37. Le paragraphe 2(i) permet aux Parties de prévoir que la conduite doit aussi avoir pour effet d'exposer, non seulement en théorie, mais aussi en pratique, la personne ou le groupe de personnes en question à la haine, au mépris ou au ridicule.

38. Le paragraphe 2(ii) permet aux Parties de formuler une réserve qui va encore plus loin, jusqu'à exclure l'application du paragraphe 1.

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

39. Ces dernières années, diverses affaires ont été traitées par des tribunaux nationaux où des personnes (dans le public, dans les médias, etc.) ont élaboré des idées ou des théories visant à minimiser, nier ou justifier les crimes graves commis au cours de la seconde guerre mondiale (en particulier l'Holocauste). La motivation de tels comportements est souvent présentée sous le prétexte de la recherche scientifique, alors qu'en réalité, le but exact est de soutenir et d'encourager la motivation politique qui avait donné lieu à l'Holocauste. De plus, ces comportements ont aussi inspiré ou même stimulé et développé les activités illégales de groupes racistes et xénophobes, y compris par le biais de systèmes informatiques. L'expression de ces idées insulte (la mémoire de) toute personne qui a été victime de l'Holocauste, ainsi que leur famille. Elle porte en outre atteinte à la dignité de la communauté humaine.

40. L'article 6 du Protocole, qui a une structure similaire à celle de l'article 3, traite ce problème. Les rédacteurs s'entendent qu'il est important d'incriminer toute expression 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 avril 1945. Ceci à cause du fait que les actes qui ont donné lieu à des génocides et à des crimes contre l'humanité, se sont déroulés entre 1940 et 1945. Toutefois, les rédacteurs ont relevé que, depuis lors, d'autres cas de génocide et de crimes contre l'humanité, qui étaient motivés par des idées et des théories de nature raciste et xénophobe, ont été perpétrés. Les rédacteurs ont dès lors considéré qu'il était nécessaire de ne pas limiter le champ d'application de cette disposition aux seuls crimes commis par le régime nazi pendant la seconde guerre mondiale, et établis comme tels par le Tribunal de Nürnberg, mais de l'étendre aussi aux génocides et crimes contre l'humanité constatés par d'autres tribunaux internationaux établis après 1945 par des instruments internationaux pertinents (par exemple, des Résolutions du Conseil de Sécurité des Nations Unies, des traités multilatéraux, etc.). De tels tribunaux pourraient être, par exemple, les Tribunaux pénaux pour l'ex-Yougoslavie, pour le Rwanda, la Cour Pénale Internationale. Cet article permet de se référer à des décisions finales et obligatoires de tribunaux internationaux futurs, dans la mesure où la juridiction de tels tribunaux est reconnue par la Partie à ce Protocole.

41. Cette disposition vise à poser clairement le principe que des faits, dont la vérité historique a été judiciairement établie, ne peuvent pas être niés, minimisés de manière grossière, approuvés ou justifiés pour soutenir ces théories et ces idées détestables.

42. La Cour européenne des Droits de l'Homme a d'ailleurs indiqué clairement que la négation ou la révision de « faits historiques clairement établis – tel que l'Holocauste – [...] se verrait soustraite par l'article 17 à la protection de l'article 10 » de la CEDH (voir à cet égard l'arrêt *Lehideux et Isorni* du 23 septembre 1998 [\(3\)](#)).

43. Le paragraphe 2 de l'article 6 donne la faculté aux Parties (i) soit d'exiger, à travers une déclaration, que la négation ou la minimisation grossière mentionnées au paragraphe 1 de l'article 6, 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, 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, (ii) soit de formuler une réserve, qui leur permettrait de ne pas appliquer, en tout ou en partie, cette disposition.

Article 7 – Aide et complicité

44. Cet article vise à ériger en infraction pénale tout acte de complicité en vue de la perpétration d'une des infractions établies en vertu des articles 3 à 6 du Protocole. Contrairement à la Convention, le Protocole n'incrimine pas la tentative de commission des infractions contenues dans le Protocole, car la plupart des conduites qui y sont criminalisées ont une nature préparatoire.

45. La responsabilité est engagée en cas de complicité lorsque la personne qui commet une infraction établie par le Protocole est aidée par une autre personne qui a également l'intention que l'infraction soit commise. Ainsi, par exemple, bien que la transmission par le biais de l'Internet de matériel raciste et xénophobe requière l'assistance de fournisseurs de services agissant comme intermédiaires, un fournisseur de services qui n'a pas d'intention criminelle ne peut être tenu responsable au titre de cette section. Les fournisseurs de services ne sont donc pas tenus de surveiller activement le contenu pour éviter la responsabilité pénale en application de cette disposition.

46. Comme pour toutes les infractions établies en vertu du Protocole, l'acte de complicité doit être commis intentionnellement.

Chapitre III – Relations entre la Convention et ce Protocole

Article 8 – Relations entre la Convention et ce Protocole

47. L'article 8 concerne les relations entre la Convention et ce Protocole. Il évite d'inclure un certain nombre de dispositions de la Convention dans le Protocole. Il indique que certaines des dispositions de celle-ci s'appliquent, *mutatis mutandis*, à ce Protocole (par exemple, celles qui concernent la responsabilité et les sanctions, la compétence et une partie des dispositions finales). Le paragraphe 2 de l'article 8 rappelle aux Parties que les mesures définies dans la Convention devraient être appliquées aux infractions prévues par ce Protocole. Pour plus de clarté, les articles pertinents ont été précisés.

Chapitre IV – Dispositions finales

48. Les dispositions contenues dans ce chapitre sont, pour l'essentiel, tirées du «Modèle de clauses finales des conventions et accords conclus au sein du Conseil de l'Europe» approuvé par le Comité des Ministres du Conseil de l'Europe lors de la 315^e réunion des Délégués des Ministres en février 1980. Etant donné que la majorité des articles 9 à 16 utilise le vocabulaire normalisé du modèle de clauses ou est fondée sur la longue pratique du Conseil de l'Europe en matière de traités, ces articles n'appellent aucun commentaire particulier. Toutefois, certaines modifications des clauses types ou certaines clauses nouvelles requièrent une explication. On notera à cet égard que les clauses types ont été adoptées en tant qu'ensemble non contraignant de dispositions. Comme indiqué dans l'introduction aux clauses types, « les présentes clauses finales types ne visent qu'à faciliter la tâche des comités d'experts et éviter des différences de libellé qui n'auraient aucune justification réelle. Les clauses types ne sont nullement contraignantes : des clauses différentes peuvent être adaptées à des situations différentes » (voir aussi dans ce contexte les paragraphes 304-330 du rapport explicatif de la Convention).

49. Le paragraphe 2 de l'article 12 spécifie que les Parties peuvent utiliser les réserves telles que définies aux articles 3, 5 et 6 de ce Protocole. Aucune autre réserve ne peut être formulée.

50. Ce Protocole est ouvert à la seule signature des signataires de la Convention. Il entrera en vigueur trois mois après sa ratification par cinq Parties à la Convention qui ont exprimés leur consentement pour être liées au Protocole (articles 9-10).

51. La Convention permet des réserves concernant certaines de ces dispositions qui, à travers la clause de connexion de l'article 8 du Protocole, peuvent aussi avoir un effet sur les obligations d'une Partie au titre de ce Protocole. Toutefois, une Partie peut notifier le Secrétaire Général qu'elle n'appliquera pas une réserve à ce Protocole. Ceci est expressément prévu par l'article 12 paragraphe 2 du Protocole.

52. Cependant, lorsqu'une Partie n'a pas utilisé une réserve ou une déclaration au titre de la Convention, elle peut avoir besoin de restreindre ses obligations par rapport aux infractions contenues dans ce Protocole. Le paragraphe 2 de l'article 12 permet aux Parties de le faire, concernant l'article 22, paragraphe 2, et l'article 41, paragraphe 1, de la Convention.

Notes :

(1) Voir dans ce contexte, par exemple, l'arrêt de l'affaire Handyside du 7 décembre 1976, série A, n°24, page 23, paragraphe 49.

(2) Abulaziz, Cabales et Balkandali, arrêt du 28 mai 1985, Série A no. 94, p. 32, para. 62; Arrêt linguistique belge, arrêt du 23 juillet 1968, Série A no. 6, p. 34, para. 10.

(3) Lehideux et Isorni arrêt du 23 septembre 1998, publié dans les Rapports 1998-VII, paragraphe 47.



Série des Traités européens - n° 185

**CONVENTION
SUR LA CYBERCRIMINALITÉ**

Budapest, 23.XI.2001

Préambule

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

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

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

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

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

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

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

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

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en 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 partielle rapides de données relatives au trafic

- 1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:
 - a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et
 - b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.
- 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:
 - a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et
 - b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
- 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
- 3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

- a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
- b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
- c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:
 - a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et
 - b à un support du stockage informatique permettant de stocker des données informatiques
 sur son territoire.
- 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:
 - a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;
 - b réaliser et conserver une copie de ces données informatiques;
 - c préserver l'intégrité des données informatiques stockées pertinentes;
 - d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.
- 4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.
- 5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:
 - a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et
 - b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:
 - i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.
- 2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
- 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.
- 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :
 - a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et
 - b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:
 - i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

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

- 2 Lorsque'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.

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 constituants 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 constituants, 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.