N° 321

SÉNAT

SESSION ORDINAIRE DE 2004-2005

Annexe au procès-verbal de la séance du 4 mai 2005

RAPPORT

FAIT

au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur le projet de loi, ADOPTÉ PAR L'ASSEMBLÉE NATIONALE*, autorisant l'approbation de la* **convention** *sur la* **cybercriminalité** *et du* **protocole additionnel** *à cette convention, relatif à l'incrimination d'***actes** *de nature* **raciste** *et* **xénophobe** *commis par le biais de* **systèmes informatiques**,

Par M. Robert DEL PICCHIA,

Sénateur.

(1) Cette commission est composée de : M. Serge Vinçon, *président* ; MM. Jean François-Poncet, Robert Del Picchia, Jacques Blanc, Mme Monique Cerisier-ben Guiga, MM. Jean-Pierre Plancade, Philippe Nogrix, Mme Hélène Luc, M. André Boyer, *vice-présidents* ; MM. Simon Loueckhote, Daniel Goulet, Jean-Guy Branger, Jean-Louis Carrère, André Rouvière, *secrétaires* ; MM. Bernard Barraux, Jean-Michel Baylet, Mme Maryse Bergé-Lavigne, MM. Pierre Biarnès, Didier Borotra, Didier Boulaud, Robert Bret, Mme Paulette Brisepierre, M. André Dulait, Mme Josette Durrieu, MM. Jean Faure, Jean-Pierre Fourcade, Mmes Joëlle Garriaud-Maylam, Gisèle Gautier, MM. Francis Giraud, Jean-Noël Guérini, Michel Guerry, Robert Hue, Joseph Kergueris, Robert Laufoaulu, Louis Le Pensec, Philippe Madrelle, Pierre Mauroy, Louis Mermaz, Mme Lucette Michaux-Chevry, MM. Charles Pasqua, Jacques Pelletier, Daniel Percheron, Jacques Peyrat, Xavier Pintat, Yves Pozzo di Borgo, Jean Puech, Yves Rispat, Josselin de Rohan, Roger Romani, Gérard Roujas, Mme Catherine Tasca, MM. André Trillard, André Vantomme, Mme Dominique Voynet.

Voir les numéros :
Assemblée nationale (**12ème** législ.) **: 905**, **1978** et T.A. **398**
Sénat : **248** (2004-2005)

Traités et conventions.

S O M M A I R E

Pages

INTRODUCTION

Mesdames, Messieurs,

La révolution numérique n'a pas seulement bouleversé les économies et le fonctionnement des bourses du monde entier. Elle a aussi accru la délinquance dont les auteurs savent tirer profit des réseaux informatiques. De nouveaux délits ont surgi qui menacent autant les individus que les entreprises ou les Etats.

Avec la première Convention internationale de lutte contre la cybercriminalité, les pays membres du Conseil de l'Europe et leurs partenaires (Etats-Unis, Canada, Japon, Afrique du sud) se sont engagés sur la voie d'une régulation juridique et éthique d'un domaine jusqu'alors abandonné, pour le meilleur comme pour le pire, aux seules règles du marché.

La convention, adoptée formellement par les Ministres des Affaires étrangères le 8 novembre 2001, a été ouverte à la signature des Etats le 23 novembre 2001 à Budapest. La Lituanie a ratifié la Convention sur la cybercriminalité le 18 mars 2004. Cette ratification, qui était la cinquième, a entraîné l'entrée en vigueur de la convention le 1er juillet 2004.

Un Protocole additionnel à la Convention sur la cybercriminalité, demandant aux Etats de considérer comme criminelle la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques, a été adopté le 7 novembre 2002 par le Comité des Ministres. Ses deux objectifs majeurs sont d'harmoniser le droit pénal et d'améliorer la coopération internationale afin de mieux lutter contre le racisme et la xénophobie sur l'Internet. Ce protocole a été ouvert à la signature à la session d'hiver de l'Assemblée parlementaire du Conseil de l'Europe de janvier 2003 et a été immédiatement signé par la France.

I. LA CYBERCRIMINALITÉ : DÉFINITION ET DIFFICULTÉS DE RÉPRESSION

A. DÉFINITION

La cybercriminalité, c'est-à-dire les infractions pénales commises sur le réseau Internet se décline en trois modes différents :

- Les infractions relatives au **contenu** se définissent comme la diffusion intentionnelle par Internet de textes ou d'images illégaux. Les deux infractions principales concernent la diffusion de matériels, d'insultes à caractère raciste, xénophobe ou négationniste, et la pédopornographie.

- L'atteinte à la **propriété intellectuelle** illustrée notamment par la mise en ligne de fichiers musicaux gratuits sans l'accord des auteurs, interprètes ou producteurs.

- Les infractions liées aux **technologies de l'information et de la communication.** Les infractions informatiques sont des atteintes délibérées aux réseaux et bases de données, ou la diffusion de virus ainsi que les trafics relatifs aux mots de passe ou code d'accès. Il peut s'agir également de fraudes aux cartes bancaires et de recueil illégal de données bancaires qui permettent d'accomplir des escroqueries en ligne, ou bien d'interception de correspondances privées utilisant un support informatique.

B. DIFFICULTÉS DE RÉPRESSION DE LA CYBERCRIMINALITÉ

Au cours des dernières années, le développement très rapide de l'Internet a été générateur d'abus et a facilité la commission d'infractions pénales de toutes sortes. Par exemple, **la cybercriminalité menace en France quelques 25 millions d'internautes (particuliers mais aussi entreprises et services publics)**.

La toile, monde sans frontières, est devenu un lieu de prédilection pour le crime organisé. Ainsi, en 2003 en France, 464 faits de pédopornographie et 156 faits de haine raciale ont été constatés, en plus des 12 000 faits de fraude ou d'escroquerie, notamment par utilisation d'informations contenues dans les cartes bancaires.

Certes, un récent rapport remis au ministre de l'Intérieur par le ministre de l'Economie, dans le cadre d'une mission qui lui avait été confiée en juillet 2004, fait état d'une baisse globale de la cybercriminalité, le nombre de délits étant passé de 65.221 à 59.964 (soit – 8,77 %). Toutefois, l'Office

central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) reconnaît que ses statistiques ne sont pas exhaustives et ne tiennent évidemment pas compte du « chiffre noir » des infractions commises mais non signalées par les victimes.

Sur les 59.964 faits enregistrés en 2004 par l'Office, les plus nombreux (49.914, soit 83,24 % de l'ensemble), concernent la falsification et l'usage de cartes de crédits, en diminution de 0,45 % par rapport à 2003.

Viennent ensuite 8.470 escroqueries par utilisation de numéro de cartes bancaires (14,13% de l'ensemble), en diminution de 30,65 %.

Dans l'ordre décroissant, les autres infractions concernent:

- La diffusion d'images de pédopornographie sur internet: 576, soit une augmentation de 24,14%.

- L'incitation à haine raciale, antisémitisme, diffamation, négationnisme sur internet: 333, soit une augmentation de 113,46%

- L'atteinte aux systèmes (piratages): 285, soit + 12,00 %.

- La contrefaçon de logiciels: 268, en hausse de 91,43 %.

- La diffusion de programmes informatiques permettant de fabriquer de fausses cartes bancaires: 64, en baisse de 91%.

- Les infractions liées à la violation de la confidentialité: 54, en hausse de 45,95%.

Il est essentiel de protéger nos concitoyens ainsi que les entreprises et les services publics contre des atteintes dont le coût est potentiellement exorbitant.

Il est important de souligner que cette **criminalité est transnationale et se développe par définition en dehors de toute considération de frontière et que sa répression se heurte au principe de territorialité de la loi pénale**.

II. LES MOYENS DE LUTTE CONTRE LA CYBERCRIMINALITÉ

A. EN FRANCE

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a été créé par décret en mai 2000 et est rattaché à la Direction de la police judiciaire. Il a une compétence nationale et travaille en collaboration avec la Brigade d'enquête sur les fraudes aux technologies de l'information, qui dépend de la Préfecture de police de Paris, avec la DST, les douanes et la Gendarmerie.

Il a pour fonction de participer à des enquêtes judiciaires et de coordonner l'action des services répressifs compétents dans le domaine des infractions informatiques.

Ses effectifs se composent de 32 policiers et 3 gendarmes et vont doubler d'ici 2008. De plus, les enquêteurs de la Police judiciaire et ceux de la Gendarmerie qui sont spécialisés en criminalité informatique lui apportent leur soutien.

Des améliorations sont envisagées dans deux domaines : le doublement des effectifs d'enquêteurs et l'harmonisation des méthodes et matériels auxquels ont recours la police et la gendarmerie.

B. EN EUROPE

L'Office européen de police (Europol), créé en juillet 1995, coordonne, soutient et rationalise les activités des services enquêteurs des Etats de l'Union européenne. Il facilite les échanges d'informations et a notamment mis en place un fichier d'analyse relatif à la pédophilie sur Internet.

Le système d'information Schengen favorise également les échanges de renseignements relatifs aux personnes et véhicules grâce à des bases de données.

Eurojust est une unité de coopération destinée à améliorer la lutte contre toutes les formes de criminalité. C'est un organisme intégré dans le traité de l'Union européenne par le Conseil européen de Nice (décembre 2000) qui permet d'améliorer la coopération entre les autorités judiciaires des Etats membres et a notamment la possibilité, grâce au mandat d'arrêt européen, d'obtenir rapidement l'extradition de criminels recherchés par un Etat membre de l'Union.

C. AU NIVEAU INTERNATIONAL

Interpol, créé en 1946 lors de la conférence de Bruxelles, ne dispose pas de pouvoirs supranationaux pour des missions opérationnelles mais coordonne les polices des Etats membres qui fournissent ou demandent des informations et des services.

Afin d'aider les enquêteurs qui mènent des investigations sur les infractions liées aux nouvelles technologies d'information et de communication, Interpol a mis en œuvre un réseau de points de contacts dans les services de police des pays membres qui fonctionne en permanence.

III. LA CONVENTION SUR LA CYBERCRIMINALITÉ

Le développement rapide de l'Internet a engendré des abus et a facilité la commission d'infractions pénales. Mais la répression de telles infractions se heurte au principe de territorialité de la loi pénale. C'est pourquoi, au-delà des moyens évoqués précédemment, une approche internationale concertée s'imposait.

Dès 1997, le Conseil de l'Europe a créé un comité d'experts, dit comité PECY[1], chargé d'élaborer un projet de convention destinée à lutter contre les auteurs des infractions pénales commises dans l'univers des réseaux. Ce comité regroupait des experts représentant les Etats membres du Conseil de l'Europe ainsi que les Etats observateurs, notamment les Etats-Unis, le Canada et le Japon. Il a rédigé un projet de convention qui a été ouvert à la signature des Etats lors d'une conférence organisée à Budapest le 23 novembre 2001. Près de quarante pays, dont la France, ont signé cette première convention pénale à vocation universelle destinée à lutter contre les cyber-délinquants qui, désormais, ne bénéficient plus de l'impunité.

La convention sur la cybercriminalité vise d'abord à harmoniser les législations nationales en matière d'incrimination et de sanctions pénales pour une liste de comportements soumis à répression. Doivent, entre autres, être réprimés l'accès illégal à un système informatique ou la diffusion de matériel pédophile par le biais d'un système informatique.

En second lieu, elle tend à compléter l'arsenal juridique des Etats en matière procédurale, afin d'améliorer la capacité des services de police à mener en temps réel leurs investigations et à rassembler des preuves sur le territoire national avant qu'elles ne disparaissent.

Enfin, elle adapte les règles classiques des conventions du Conseil de l'Europe en matière d'extradition et d'entraide répressive.

La convention sur la cybercriminalité, entrée en vigueur le 1er juillet 2004, constitue un texte pionnier de caractère universel, parfois novateur **dans un secteur où la liberté absolue d'expression était la règle initiale** et qui permet la mise en place d'un régime rapide et efficace de coopération internationale.

Pour permettre aux Etats de faire connaître leurs demandes et afin d'y répondre avec célérité, la convention a prévu, en plus des voies de communication traditionnelles, un réseau de points de contact disponibles 24 heures sur 24 et 7 jours sur 7. En France, ce service est géré par l'office central

---

(1) Comité d'expert sur la criminalité dans le cyber-espace.

de lutte contre la criminalité liée aux technologies de l'information et de la communication.

La convention du Conseil de L'Europe sur la cybercriminalité constitue le premier texte de droit international visant à garantir la sécurité des réseaux et de ses utilisateurs. Le G 8 s'étant saisi de cette question, les Etats-Unis, le Japon, le Canada et l'Afrique du Sud ont également signé la convention le 23 novembre 2001 aux côtés de 34 des 46 membres du Conseil de l'Europe, ce qui porte à 38 le nombre d'Etats signataires.

Toutefois, sur les 38 Etats signataires, 30 n'ont à ce jour pas déposé leurs instruments de ratification. Il importe donc que la France soit en mesure de le faire rapidement.

IV. LE PROTOCOLE ADDITIONNEL À LA CONVENTION SUR LA CYBERCRIMINALITÉ

Lors des rencontres et discussions préalables à cette convention dite « de Budapest », le comité d'experts n'avait pas adopté les propositions des délégations allemande et française concernant l'**incrimination des comportements racistes et xénophobes sur internet** en raison de l'opposition de diverses délégations, qui invoquaient le principe de la liberté d'expression (Canada, Etats-Unis et Japon notamment)

Aussi le Conseil de l'Europe suggéra-t-il dès 2001 l'élaboration d'un protocole additionnel spécifique. La France a eu un rôle moteur dans son élaboration.

Ce protocole, adopté le 7 novembre 2002 par le Conseil de l'Europe et ouvert à la signature à Strasbourg, le 28 janvier 2003, à l'occasion de la première session 2003 de l'Assemblée parlementaire du Conseil de l'Europe, est un complément essentiel à la convention de Budapest.

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 souhait d'un monde sans haine ni discrimination raciale ne s'est que partiellement concrétisé.

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.

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. Il convient, à cet égard, de se rapporter au rapport de M. Thierry Breton précité : sur les 59.964 faits enregistrés en 2004 pour l'OCLTIC en France, l'incitation à la haine raciale, l'antisémitisme, la diffamation et le négationnisme sont en augmentation de plus de 113 % par rapport à 2003.

Pour pouvoir mener des enquêtes et poursuivre les personnes coupables de ces délits, la coopération internationale est essentielle. La convention sur la cybercriminalité a été élaborée pour permettre une entraide concernant les crimes informatiques au sens large du terme, conçue de manière souple et moderne. **Le 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.

C'est pourquoi l'Assemblée parlementaire du Conseil de l'Europe a confié au Comité européen pour les problèmes criminels (CPDC), 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, ouvert à la signature et à la ratification des Parties contractantes à la Convention, pour traiter en particulier des questions suivantes :

- 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 ;

- 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.

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.

Un premier chapitre définit l'expression «matériel raciste et xénophobe» de la façon suivante : « *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. » Dans un deuxième chapitre, le protocole énumère un certain nombre de comportements à caractère xénophobe, susceptibles de causer un trouble à l'ordre social et qui, partant, doivent être incriminés. Ainsi, les Etats signataires s'engagent à ériger en infractions pénales non seulement « la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste ou xénophobe » mais encore l'insulte raciste proférée par le biais d'un système informatique. Bien plus, le discours négationniste diffusé par ce biais ainsi que l'approbation ou la justification des actes constitutifs de génocide ou de crimes contre l'humanité doivent pareillement être incriminés. C'est une première dans un traité international.

Enfin, le chapitre III détermine l'articulation du protocole avec la convention sur la cybercriminalité, dont sont applicables les dispositions concernant la procédure pénale -conservation rapide de données informatiques stockées, collecte en temps réel de données relatives au trafic ou au contenu- et la coopération internationale.

Ainsi que le précise le Conseil de l'Europe, plusieurs pays incriminent déjà certains actes liés au contenu raciste ou xénophobe. Cependant, la diffusion de tels matériels à travers les réseaux informatiques pose davantage de difficultés aux autorités chargées de l'application de la loi. Il est donc indispensable de mettre en place une approche coordonnée pour pouvoir répondre de manière efficace à l'échelle nationale et internationale, sur la base d'éléments communs qui devront être inclus dans un Protocole additionnel à la Convention sur la cybercriminalité.

Ce Protocole aura pour conséquence d'élargir le champ d'application de la Convention, y compris ses dispositions en matière de droit matériel, de procédure pénale et de coopération internationale, de sorte à couvrir également les infractions de propagande raciste ou xénophobe. Ainsi, outre l'harmonisation des éléments de droit matériel de tels comportements, le Protocole rendra plus facile l'utilisation par les Parties des moyens et voies de coopération internationale établis, dans ce domaine, dans la Convention-mère.

Au total, ce Protocole, actuellement signé par 23 Etats, reprend des formules très souples, susceptibles de préserver les spécificités de chaque ordre juridique national tout en élargissant la portée de la convention mère sur la cybercriminalité à des comportements contre lesquels la France se fait un point d'honneur de lutter.

Toutefois, 23 Etats ont signé le protocole mais seules l'Albanie et la Slovénie ont procédé à sa ratification. Il est à noter que plusieurs membres de l'Union européenne n'ont pas signé le protocole, dont le Royaume-Uni. Pour entrer en vigueur, il doit avoir été ratifié par cinq Etats. Une approbation rapide de ce protocole par la France s'impose

d'autant plus que notre pays est à l'origine du texte ; elle constituerait en outre un signal pour obtenir un plus grand nombre de signatures.

V. LE VOTE JOINT DE LA CONVENTION ET DU PROTOCOLE

Alors que l'Assemblée nationale avait été saisie de la convention de base, le Gouvernement a déposé le projet autorisant l'approbation de son protocole additionnel au Sénat. Pour des raisons de cohérence et de lisibilité du travail parlementaire, et aussi pour accélérer la procédure d'approbation, la commission des affaires étrangères de l'Assemblée nationale a adopté deux amendements tendant à joindre l'examen de la convention et du protocole additionnel.

Certes, dans notre pays, les pouvoirs publics ont déjà intégré dans le droit national l'essentiel des stipulations de la convention et de son protocole additionnel.

On citera pour mémolire les lois suivantes : la loi pour la sécurité quotidienne du 15 novembre 2001 ; la loi d'orientation et de programmation pour la sécurité intérieure du 18 mars 2003 ; la loi pour la confiance dans l'économie numérique du 21 juin 2004 ; la loi portant adaptation de la justice aux évolutions de la criminalité du 9 mars 2004.

Mais il est essentiel de ratifier rapidement et donc conjointement cette convention et son protocole additionnel car le récent rapport (mars 2005) de la Commission nationale consultative des Droits de l'Homme est très alarmant :

En 2004, le nombre d'actes racistes et antisémites a atteint des niveaux « exceptionnels et inquiétants », passant de 833 à 1565, soit une progression de 87,8 % par rapport à l'année précédente, selon ce rapport. Il relève 970 faits antisémites en 2004, contre 601 en 2003, soit une hausse de 50 % et 595 actes racistes en 2004, contre 232 en 2003, soit une augmentation de plus de 100 %. La multiplication des profanations de lieux de culte et de cimetières juifs et musulmans (65 en 2004 contre 44 en 2003) et la forte recrudescence des violences et menaces en milieu scolaire ont marqué l'année. La Commission nationale consultative des Droits de l'Homme estime qu'en dépit d'une législation française complète, le « rendement » de la répression « a été faible » en 2004, puisque, sur 387 affaires recensées par la Chancellerie, 319 n'ont pas fait l'objet de poursuites pénales.

Le recours aux réseaux informatiques ne doit en aucun cas faciliter la diffusion du racisme et de la xénophobie.

CONCLUSION

L'adoption de la convention de Budapest sur la cybercriminalité et du protocole additionnel sur la diffusion de propos et de matériels raciste et xénophobe par le biais de systèmes informatiques est d'une importance capitale et la France peut jouer un rôle exemplaire en les ratifiant, tout particulièrement en ce qui concerne le protocole qui n'est pas encore applicable puisque seuls deux pays l'ont ratifié.

C'est pourquoi, votre commission des affaires étrangères, de la défense et des forces armées vous invite à adopter ce projet de loi issu de la rédaction proposée par l'Assemblée nationale.

EXAMEN EN COMMISSION

La commission a examiné le présent rapport lors de sa réunion du mercredi 4 mai 2005.

A la suite de l'exposé du rapporteur, **M. André Rouvière** a exprimé ses craintes relatives au développement de la cybercriminalité qui est difficilement mesurable et à la difficulté d'une répression efficace.

M. Robert Del Picchia, rapporteur, a rappelé qu'une directive européenne permettait de fermer des sites illégaux et que les grands distributeurs présents sur internet mettaient en place des filtres. Toutefois, les sites à dimension mondiale ne peuvent être facilement contrôlés.

Mme Gisèle Gautier a souligné le caractère d'urgence de la présentation au Sénat de ce projet de loi et l'importance du débat qu'il permettrait.

PROJET DE LOI

Article premier

Est autorisée l'approbation de la convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, et dont le texte est annexé à la présente loi. [1]

Article 2

Est autorisée l'approbation du protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003.

[1] *Voir le document annexé au projet de loi n° 905*

ANNEXE I -

CONVENTION SUR LA CYBERCRIMINALITÉ
STCE NO. : 185

Traité ouvert à la signature des Etats membres et des Etats non membres qui ont participé à son élaboration et à l'adhésion des autres Etats non membres

Ouverture à la signature

Lieu : Budapest
Date : 23/11/2001

Entrée en vigueur

Conditions : 5 Ratifications incluant au moins 3 Etats membres du Conseil de l'Europe
Date : 1/7/2004

Situation au 15/4/2005

Etats membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	23/11/2001	20/6/2002	1/7/2004							
Allemagne	23/11/2001									
Andorre										
Arménie	23/11/2001									
Autriche	23/11/2001									
Azerbaïdjan										
Belgique	23/11/2001									
Bosnie-Herzégovine	9/2/2005									
Bulgarie	23/11/2001	7/4/2005	1/8/2005		X	X				
Chypre	23/11/2001	19/1/2005	1/5/2005							
Croatie	23/11/2001	17/10/2002	1/7/2004							
Danemark	22/4/2003									
Espagne	23/11/2001 r									
Estonie	23/11/2001	12/5/2003	1/7/2004				X			
Finlande	23/11/2001									
France	23/11/2001									
Géorgie										
Grèce	23/11/2001									
Hongrie	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Irlande	28/2/2002									
Islande	30/11/2001									
Italie	23/11/2001									
Lettonie	5/5/2004									
l'ex-République yougoslave de Macédoine	23/11/2001	15/9/2004	1/1/2005				X			
Liechtenstein										

Luxembourg	28/1/2003									
Malte	17/1/2002									
Moldova	23/11/2001									
Monaco										
Norvège	23/11/2001									
Pays-Bas	23/11/2001									
Pologne	23/11/2001									
Portugal	23/11/2001									
République tchèque	9/2/2005									
Roumanie	23/11/2001	12/5/2004	1/9/2004				X			
Royaume-Uni	23/11/2001									
Russie										
Saint-Marin										
Serbie-Monténégro	7/4/2005									
Slovaquie	4/2/2005									
Slovénie	24/7/2002	8/9/2004	1/1/2005							
Suède	23/11/2001									
Suisse	23/11/2001									
Turquie										
Ukraine	23/11/2001									

Etats non membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Afrique du Sud	23/11/2001									
Canada	23/11/2001									
Etats-Unis	23/11/2001									
Japon	23/11/2001									

Nombre total de signatures non suivies de ratifications :	32
Nombre total de ratifications/adhésions :	10

Renvois :a.: Adhésion - s.: Signature sans réserve de ratification - su.: Succession - r.: signature "ad referendum". R.: Réserves - D.: Déclarations - A.: Autorités - T.: Application territoriale - C.: Communication - O.: Objection.

Source : Bureau des Traités sur http://conventions.coe.int

ANNEXE II -

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
STCE NO. : 189

Traité ouvert à la signature des Etats qui ont signé le Traité STE 185

Ouverture à la signature

Lieu : Strasbourg
Date : 28/1/2003

Entrée en vigueur

Conditions : 5 Ratifications.
Date : //

Situation au 4/6/2005

Etats membres du Conseil de l'Europe

Situation au 4/6/2005 Etats membres du Conseil de l'Europe Etats	Signature	Ratification	Entrée en vigueur
Albanie	26/5/2003	26/11/2004	
Allemagne	28/1/2003		
Andorre			
Arménie	28/1/2003		
Autriche	30/1/2003		
Azerbaïdjan			
Belgique	28/1/2003		
Bosnie-Herzégovine	9/2/2005		
Bulgarie			
Chypre	19/1/2005		
Croatie	26/3/2003		
Danemark	11/2/2004		
Espagne			
Estonie	28/1/2003		
Finlande	28/1/2003		
France	28/1/2003		
Géorgie			
Grèce	28/1/2003		
Hongrie			
Irlande			
Islande	9/10/2003		
Italie			
Lettonie	5/5/2004		
l'ex-République yougoslave de Macédoine			
Liechtenstein			
Lituanie			
Luxembourg	28/1/2003		
Malte	28/1/2003		

Moldova	25/4/2003		
Monaco			
Norvège			
Pays-Bas	28/1/2003		
Pologne	21/7/2003		
Portugal	17/3/2003		
République tchèque			
Roumanie	9/10/2003		
Royaume-Uni			
Russie			
Saint-Marin			
Serbie-Monténégro			
Slovaquie			
Slovénie	26/2/2004	8/9/2004	
Suède	28/1/2003		
Suisse	9/10/2003		
Turquie			
Ukraine			
Etats non membres du Conseil de l'Europe Etats	Signature	Ratification	Entrée en vigueur
Afrique du Sud			
Canada			
Etats-Unis			
Japon			
Nombre total de signatures non suivies de ratifications :			23
Nombre total de ratifications/adhésions :			2

Renvois : a.: Adhésion - s.: Signature sans réserve de ratification - su.: Succession - r.: signature "ad referendum". R.: Réserves - D.: Déclarations - A.: Autorités - T.: Application territoriale - C.: Communication - O.: Objection.
Source : Bureau des Traités sur http://conventions.coe.int/