AAARGH

LA BATAILLE POUR LE CONTRÔLE D'INTERNET
LA TENTATIVE D'ÉTOUFFER LE SITE DE L'AAARGH

Mise en ligne : septembre 2005

PARMI LES DROITS DE L'HOMME, IL Y A CELUI DE SAVOIR À QUELLE SAUCE ILS VEULENT NOUS MANGER.

L'ÉTAT DU DROIT EUROPÉEN EN MATIÈRE DE CONTRÔLE IDÉOLOGIQUE DE L'INTERNET (ÉTÉ 2005)

Conférence de l'OSCE sur la relation entre la propagande raciste, xénophobe et antisémite sur internet et les crimes inspirés par la haine (16-17 juin 2004)

Eléments de politique française - réponse au questionnaire de l'OSCE
Dernière mise à jour : 15/06/04

Eléments de politique française eu égard au lien entre la propagande raciste, xénophobe et antisémite sur Internet et les crimes inspirés par la haine réponse au questionnaire de l'OSCE

I Contexte et cadre juridique

1. Nombre d'ordinateurs et d'internautes en France

Une enquête de l'Institut Médiamétrie réalisée en décembre 2003 a permis d'évaluer :
- La part des ménages français possédant à cette date un équipement informatique à 42,7% et une connexion Internet à 27,7% ;
- Le nombre de Français âgés de 11 ans et plus s'étant connecté à Internet au cours du mois précédant l'enquête à 21,9 millions (soit 42,9% de la population de cette tranche d'âge.

Ainsi, entre décembre 2002 et décembre 2003, la population internaute aurait-elle progressé de 17% et le marché français du haut débit de l'ordre de 60%, 15% des foyers étant dorénavant équipés d'un accès Internet haut débit (3,6 millions d'abonnement haut débit), notamment via les technologies DSL (Digital Suscriber Line).

2. Structure de l'industrie de l'Internet, notamment associations

Il existe de nombreux syndicats et associations professionnels regroupant les différents acteurs industriels de l'Internet. A titre d'exemple, on peut citer :
- l'Association des fournisseurs d'accès et de services Internet (AFA, www.afa-france.com) ;
- l'Association française des opérateurs de réseaux multiservices (AFORM, www.aform.asso.fr)
- le Club informatique des grandes entreprises françaises (CIGREF, www.cigref.fr) ;
- le Groupement français de l'industrie de l'information (GFII, www.gfii.asso.fr) ;
- la Chambre syndicale des SSII et des éditeurs de logiciels (SYNTEC, www.syntec-informatique.fr) ;
- l'Association pour le commerce et les services en ligne (ACSEL, www.acsel.asso.fr) ;
- l'Association des villes pour le câble et le multimédia (AVICAM, www.avicam.org) ;
- etc.

3. Cadre constitutionnel et légal sur la propagande raciste, xénophobe ou antisémite, ainsi qu'eu égard aux infractions motivées par la haine (définition des infractions et statistiques y comprises)

Dispositions d'ordre général sur les crimes et délits à caractère raciste, xénophobe ou antisémite

Le préambule de la Constitution de 1946 proclame les droits inaliénables et sacrés de tout être humain, sans distinction de race, de religion, ni de croyance. Ces principes font partie intégrante de la Constitution de 1958.

La France a signé (1966) et ratifié (1971) la Convention des Nations Unies sur l'élimination de toutes les formes de discrimination raciale.

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, interdit l'inscription dans un fichier de "l'origine raciale" des personnes concernées, sauf accord exprès de ces personnes ou pour des motifs d'intérêt public. Ces dispositions sont reprises dans le code pénal (article 226-19).

La loi n° 90-615 du 13 juillet 1990 tend à réprimer tout acte raciste, antisémite ou xénophobe.

La loi n° 2001-1066 du 16 novembre 2001 relative à la lutte contre les discriminations a élargi le champ de la lutte contre les discriminations à toutes situations discriminatoires, en intégrant dans l'article 225-1 du code pénal relatif à la discrimination les notions "d'orientation sexuelle, d'âge, d'apparence physique, de patronyme ; les domaines professionnels susceptibles de faire l'objet de poursuites pénales pour discriminations en ajoutant à l'article 225-2 du code pénal les "demandes de stage ou les périodes de formation professionnelle" ; pris la mesure des phénomènes discriminatoires en les prohibant sous toutes leurs formes, etc.

La loi n° 2003-88 du 3 février 2003 visant à aggraver les peines punissant les infractions à caractère raciste, antisémite ou xénophobe fait du mobile raciste de certains crimes ou délits une circonstance aggravante conduisant à un alourdissement des peines encourues (article 132-76 du code pénal).

La loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité traduit la fermeté et la sévérité dont la France entend faire preuve à l'égard des infractions motivées par les mobiles racistes, xénophobes ou antisémites. Elle a notamment pour objet d'élargir la liste des infractions pour lesquelles la circonstance aggravante à raison de l'appartenance ou de la non-appartenance, vraie ou supposée, de la victime à une ethnie, une nation, une race ou une religion déterminée, ou à raison de l'orientation sexuelle vraie ou supposée de la victime, peut être retenue. Il s'agit de l'ensemble des menaces de crime ou de délit ou de mort (article 222-18-1 du code pénal), le vol (article 331-4 du code pénal) et l'extorsion (article 311-2 du code pénal).

Il est à signaler que le gouvernement français a présenté un important programme d'actions, dans le cadre du comité interministériel à l'intégration du 10 avril 2003, comprenant 55 mesures, dont la création d'une Autorité administrative indépendante. Cette dernière sera chargée de lutter contre l'ensemble des phénomènes discriminatoires à caractère raciste et xénophobe et devrait voir le jour prochainement.

Dispositions relatives à la liberté d'expression

La Déclaration des droits de l'homme et du citoyen du 26 août 1989 - texte à valeur constitutionnelle - garantit le droit à la liberté d'expression en son article 11 : " la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme :

tout citoyen peut donc parler écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ".

La Convention européenne des droits de l'homme consacre également le droit à la liberté d'expression en son article 10. Les seules limites à la liberté d'expression procèdent de la nécessité de protection de l'intérêt général (sécurité nationale, intégrité du territoire, sécurité publique, ordre public, protection de la santé ou de la morale).

Dispositions spécifiques aux propos de nature raciste, xénophobe ou antisémite

La loi du 29 juillet 1881 sur la liberté de la presse (modifiée par la loi n° 72-546 du 1er juillet 1972 relative à la lutte contre le racisme) pénalise les écrits et les propos tenus à raison de " l'origine ou de l'appartenance ou de la non-appartenance à une ethnie, une nation, une race ou une religion déterminée ".

En outre, la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, dans le but de rendre plus effective l'application de la loi du 29 juillet 1881 sur la liberté de la presse aux infractions commises au moyen de l'Internet notamment, prévoit que les provocations à la haine raciale, la contestation de crime contre l'humanité, la diffamation et l'injure à caractère racial, sont soumises à une règle de prescription particulière.

En effet, le délai de prescription des crimes d'une telle nature passe de trois mois à un an, quel qu'en soit le support, Internet y compris (Cf. jurisprudence de la cour de cassation). Le point de départ du délai de prescription court à partir du jour de la commission de l'infraction.

Dispositions spécifiques à l'Internet

La France a signé, le 23 novembre 2001, la Convention sur la Cybercriminalité, issue d'une décision du Conseil de l'Europe qu'elle a contribué à promouvoir. Cette convention est complétée par un protocole additionnel, signé le 28 janvier 2003 par le France, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

Ces deux instruments sont en cours de ratification : le ministre des affaires étrangères a présenté, mercredi 28 janvier 2004 en Conseil des ministres un projet de loi autorisant l'approbation du protocole additionnel à la Convention européenne sur la cybercriminalité.

La directive européenne 2000/31/CE sur le " commerce électronique " a fixé des orientations générales qui tendent à opérer une nette distinction entre le contenu des informations circulant sur le réseau et la responsabilité des prestataires techniques intervenant de façon intermédiaire entre l'émetteur et le destinataire du contenu . A ce titre, elle énonce que :

- les prestataires techniques ne doivent pas être soumis à une obligation générale de surveillance des informations qu'ils transmettent ou qu'ils stockent , ni à une obligation générale de recherche active de faits ou d'activités illicites ;
- le principe directeur est que les prestataires ne sont pas responsables des contenus transmis ou hébergés et que leur responsabilité ne peut être envisagée que dans des cas limitativement énumérés (cas dans lesquels ils ont effectivement connaissance du contenu illicite et pour lesquels ils n'ont pas agi promptement afin de faire cesser l' accès à ces contenus).

La loi pour la confiance dans l' économie numérique adoptée par le parlement le 27 avril 2004 transpose fidèlement les dispositions de la directive européenne précitée (cette loi est sujette à un recours pendant auprès du Conseil Constitutionnel) .

La nouvelle loi ne modifie pas le principe constant du droit de la communication selon lequel c'est avant tout l'auteur de la communication qui porte la responsabilité.

En ce qui concerne la responsabilité des prestataires techniques, la loi reprend ainsi les principes énoncés par la directive :

s'agissant des fournisseurs d' accès, leur responsabilité - civile ou pénale- ne peut être mise en cause à raison des contenus auxquels ils fournissent l' accès que dans des cas limitativement énumérés (cas dans lesquels le fournisseur d' accès a lui-même été à l'origine de la demande de transmission litigieuse, a sélectionné le destinataire de la transmission, a sélectionné ou modifié le contenu faisant l'objet de la transmission).

S'agissant des hébergeurs, la loi reproduit le principe de la directive : les hébergeurs ne sauront être tenus civilement ou pénalement responsables des contenus qu'ils hébergent s'ils n' avaient pas effectivement connaissance de ces contenus illicites, ou si, dès qu'ils en ont eu connaissance, ils ont agi promptement afin de rendre l' accès à ces contenus impossible .

(Avant l' adoption de cette loi, les règles de droit antérieures permettaient déjà également de mettre en cause, sous certaines conditions, la responsabilité d'un prestataire hébergeur (Affaire Yahoo - novembre 2000) .

La loi française reprend également fidèlement le principe selon lequel les prestataires ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou qu'ils stockent.

Toutefois, le législateur français a souhaité précisé qu'en matière de lutte contre les contenus les plus attentatoires à la dignité humaine (pédophilie, apologie des crimes contre l'humanité et incitation à la haine raciale), les prestataires techniques pouvaient utilement apporter leur contribution : reprenant en cela les propositions spontanées faites par les professionnels du secteur, la nouvelle loi française édicte ainsi à l' égard tout à la fois des fournisseurs d'accès et des hébergeurs trois obligations particulières :

- obligation de mettre en place un dispositif de signalement facilement accessible à tout internaute ;
- obligation d'informer promptement les autorités publiques compétentes de toutes activités illicites qui leur seraient signalées ;
- obligation de rendre publics les moyens consacrés à la lutte contre ces activités illicites .

En ce qui concerne plus particulièrement les fournisseurs d' accès, la loi dispose aussi que ceux-ci doivent informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services et doivent également leur proposer au moins un de ces moyens (ex : systèmes de contrôle parental)

Par ailleurs, la loi prévoit que les prestataires techniques doivent répondre à toute ordonnance de l' autorité judiciaire leur enjoignant de prendre les mesures nécessaires à la cessation des dommages qui seraient occasionnés par certains contenus mis en ligne .

Enfin, la loi " Internet " précise dans un sens favorable à la victime le mode de calcul du délai de prescription des délits de presse commis sur le réseau : le délai de recours ne court qu'à partir de la date à laquelle a cessé la mise à disposition du public du contenu illicite .

4. Quels facteurs pourraient limiter l'action des gouvernements, ONG, groupes industriels pour traiter de la propagande raciste, xénophobe et antisémite sur l'Internet ?

Les facteurs limitatifs sont liés à la nature de l'Internet qui requiert une coopération internationale de tous les acteurs pour être efficace, tout en préservant le cadre de la liberté d'expression et d'information.

5. Organisations s'occupant de la propagande raciste sur l'Internet :

MRAP, LICRA, J'accuse, SOS racisme, Centre Simon Wiesenthal, GELD *, CNCDH.

6. Associations de lutte contre l'antisémitisme:

B'naï B'rith Europe, B'naï B'rith France, Centre européen juif d'information, Centre Simon Wiesenthal Europe, Congrès Juif européen, CRIF (Conseil Représentatif des Institutions juives), Fondation pour la mémoire de la Shoah, Observatoire du Monde juif, Union des Etudiants juifs de France. [***A l'exception du MRAP, toutes ces organisations sont juives et sionistes, c'est-à-dire adhérentes à l'idéologie raciste juive définie depuis 110 ans par le mouvement sioniste. Il fut un temps où l'ONU avait inscrit ce fait, récusé ensuite sous pression américaine, et solennelement réitéré à la Conférence de Durban, sous la pression massive du Tiers-Monde***.]

II Le lien possible entre propagande raciste, xénophobe et antisémite sur l'Internet et les crimes inspirés par la haine

1. Organismes en charge du recueil de données

Le Ministère de la Justice (Direction des Affaires criminelles et des grâces) assure un suivi des actes antisémites recensés par les parquets français, par le biais d'Internet ou s'agissant d'atteintes classiques aux biens et aux personnes. Il édite aussi des guides méthodologiques sur le traitement des infractions à caractère raciste et le traitement de le cybercriminalité en général (en cours d'actualisation). [***Il est curieux de constater que le Ministère de la déesse aux yeux bandés ignore absolument tous les actes sionistes (agressions, journaux, manifestations de solidarité avec l'armée qui massacre en Palestine, etc.) qui sont, pour la communauté internationale, dans son écrasante majorité, des actes racistes.***]

Pour 2002, les principaux actes racistes et antisémites sur l'Internet ont été recensés par le Parquet de Paris.

Ces éléments sont fournis chaque année à la CNCDH dans le cadre de son rapport annuel, ainsi qu'au CERD ou à l'EUMC (observatoire européen des phénomènes racistes ou xénophobes).

Les difficultés rencontrées sont liées à l'extranéité, jusqu'au début 2004, la courte prescription, la complexité de rassembler les preuves et de confirmer l'identité réelle des auteurs.

2. Statistiques de la CNCDH

Le rapport 2003 de la CNCDH (Commission consultative des droits de l'homme) dresse un bilan des actes à caractère raciste, xénophobe et antisémite, ainsi que des actions judiciaires liées à de tels actes. Le nombre global des actes de cette nature (tant violences que menaces) a baissé de 37,7% en 2003 (817 en 2003, contre 1313 en 2002) ; toutefois ce chiffre demeure-t-il élevé si l'on le compare à celui prévalant dans les années 1990. Les statistiques du ministère de l'Intérieur relèvent 229 actes de violence en 2003 contre 381 en 2002, et 32 personnes blessées en conséquence en 2003. Le rapport opère une distinction entre les actes racistes et xénophobes, y compris anti-islam, et les actes antisémites et note un développement préoccupant du phénomène à l'école. On dénombrait 195 violences antisémites en 2002 et 125 en 2003, 737 menaces en 2002 contre 463 en 2003, le total des violences et menaces antisémites s'élevant ainsi à 932 en 2002 et 588 en 2003. Si l'année 2003 marque globalement une tendance à la baisse, le dernier trimestre 2003 enregistre une recrudescence de ce type d'actes, 1/3 des violences ayant été enregistrées d'octobre à décembre. Aussi cette hausse a-t-elle justifié, après l'incendie d'une école juive à Gagny, l'annonce, le 15 novembre 2003, par le Président de la République, de la création d'un Comité interministériel de lutte contre le racisme et l'antisémitisme (CIRA).(voir plus bas).

III Les moyens de faire face à la propagande raciste, xénophobe et antisémite sur l'Internet, les crimes de haine et leurs interactions possibles

1. Traitement judiciaire

Eu égard aux procédures judiciaires liées à des infractions à caractère raciste, antisémite ou discriminatoire, les chiffres sont les suivants :
- 162 condamnations ont été prononcées en 2002 (154 en 2001) , dont 103 pour injures publiques en raison de la race, la religion ou l'origine (109 en 2001). Il faut relever une augmentation sensible des cas de condamnation pour cause de discrimination dans l'offre d'un bien ou d'un service (24 en 2002 contre 7 en 2001).
- 108 procédures liées à des infractions à caractère antisémite ont été transmises par les parquets généraux en 2003 - contre 120 en 2002.
- une dizaine d'actes anti-musulmans ont été recensés en 2003, notamment l'incendie de la mosquée de Nancy.Exemples de dossiers liées à la propagande raciste et antisémite ; condamnation dans le cadre de l'affaire " amisraeli.org " ; en cours l'affaire " SOS-racaille " ; cas de relaxes et de non lieu.

2. Action du gouvernement français en matière de lutte contre les crimes de nature raciste, xénophobe et antisémite, et au regard de la propagande de même nature sur Internet

Le Président de la République a annoncé, en novembre 2003, la création d' un Comité interministériel de lutte contre le racisme et l'antisémitisme (CIRA). Ce Comité s'est réuni le 9 décembre 2003, le 27 janvier , le 18 mars ainsi que le 3 mai 2004. Plusieurs mesures ont été annoncées :
- Police, sécurité : mise en place d'un fonds doté de 15 millions d'euros pour contribuer au renforcement de la sécurité de sites susceptibles d'être la cible de violences : synagogues, écoles, lieux associatifs ; nouveau logiciel de signalement des incidents à caractère antisémite.
- Développement de la prise de conscience à l'école :
- Distribution d'un livret républicain, journée consacrée à la mémoire de la Shoah, le 27 janvier, jour anniversaire de la libération du camp d'Auschwitz, voyages d'études sur les lois de mémoire.
- Mise en place d'un système de veille qui repère les discours antisémites et racistes dans les médias en liaison avec le Conseil supérieur de l'audio-visuel. L'AFA (association française des

fournisseurs d'accès et de services notamment) coopère avec le CRIF et les autorités françaises compétentes en matière de veille sur l'Internet).
- A l'initative de M. Lellouche, député, une loi du 3 février 2003 visant à aggraver les peines punissant les infractions à caractère raciste, antisémite ou xénophobe avait été votée à l'unanimité par le Parlement français.
- La liste des infractions, dont les peines sont susceptibles d'être aggravées suivant les dispositions de la loi du 3 février 2003, a été complétée par la loi du 9 mars 2004,
- Le Président de la République a également demandé au Médiateur de la République de mettre en place une Haute autorité pour lutter contre les discriminations. Celle-ci devrait être instituée au 2ème trimestre 2005. Elle vise à renforcer le dispositif existant (CODAC : Commissions départementales d'Accès à la citoyenneté créées en janvier 1999 pour aider les jeunes issus de l'immigration à trouver un emploi et à s'insérer dans la société) et s'intègre dans la politique menée par l'Union en la matière.
- Recueil de données (voir II).

3. Coopération actuelle entre les différents acteurs, gouvernements, ONG, associations religieuses et bonnes pratiques : Gouvernance de l'Internet - le Forum des droits sur l'Internet

Fondé en 2001 avec le soutien des pouvoirs publics, le Forum est investi de trois grandes missions : la concertation entre les acteurs, l'information et la sensibilisation du public et la coopération internationale.

3.1 La concertation

Structure permanente de dialogue, le Forum organise l'échange et la concertation entre les utilisateurs, les acteurs économiques et les instances publiques sur les questions de droit et de société liées aux réseaux.

Cette activité est préparatoire à la prise de décision des autorités publiques ou privées et éclaire les fondements de celle-ci.

Sur la base des débats qu'il a organisé et des conclusions des groupes de travail, le Forum peut formuler des recommandations qui s'adressent aussi bien aux acteurs privés, en les appelant à une action d'autorégulation, qu'aux acteurs publics de la régulation pour un aménagement du droit existant. Cette mission de recommandation est exercée de sa propre initiative ou sur saisine du gouvernement, du Parlement ou des autorités administratives indépendantes (CSA, ART, CNIL...).

Le Forum peut aussi favoriser l'échange d'expériences entre acteurs de secteurs professionnels différents. Dans ce cas, il n'émet pas de recommandations mais peut suggérer des bonnes pratiques ou usages.

Dans tous les cas, et sans être investi d'aucun pouvoir réglementaire, le Forum est un intermédiaire impartial et constructif entre acteurs publics et privés permettant une réflexion collective.

3.2 L'information et la sensibilisation du public

Le premier acteur de civilité étant l'internaute, le Forum mène auprès de celui-ci de nombreuses actions pédagogiques, et recueille son avis et ses propositions sur les règles et les usages de l'Internet.

Plate-forme d'information et instrument du dialogue, le site du Forum (http://www.foruminternet.org/) est ainsi devenu un lieu de référence sur les droits et les devoirs de l'internaute. Des actualités pertinentes y sont régulièrement diffusées, des questions-réponses et des aides pratiques répondront de manière concrète à la plupart de ses interrogations. Une base de connaissance réunira les sources principales du droit français, des usages et des normes internationales applicables aux réseaux. Le site comporte aussi un espace de réflexion ouvert aux internautes pour que chacun puisse participer activement aux débats en cours.

Un site web grand public et d'autres actions spécifiques, décrites plus bas (IV Mesures visant à éduquer les usagers et assurer une meilleure prise de conscience du public) font du Forum des droits sur l'Internet un acteur central de la sensibilisation du public aux droits et aux usages de la toile.

Les sites du Forum des droits sur l'Internet sont visités chaque mois par plus de 100.000 internautes.

3.3 La coopération internationale

Compte tenu de la dimension internationale de la plupart des questions juridiques posées par le monde en réseau, il est essentiel de favoriser le rapprochement des positions

internationales, à commencer par l'Europe. Pour cela, de nouvelles formes de dialogue sont nécessaires, plus souples et plus informelles. Pour réaliser cet objectif, Le Forum participe de façon active aux diverses initiatives européennes et internationales.

Le Forum des droits sur l'Internet a mis en place un réseau européen de co-régulation de l'Internet (EICN) de structures publiques ou privées de sept pays différents (Grande-Bretagne, Italie, Belgique, Autriche, Suède, Hongrie, France) partageant ses valeurs, désirant travailler ensemble sur les questions de régulation et promouvoir la méthode de la co-régulation. Plus d'informations sur le réseau européen de co-régulation sont disponibles à l'adresse : http://www.internet-coregulation.org /

3.4 Les relations avec l'Administration

Un Observateur siégeant avec voix consultative au conseil d'orientation permet d'assurer les relations du Forum avec l'Administration. Le directeur de la Direction du Développement des Médias (DDM), rattachée au Premier ministre, a été désigné pour occuper ce poste. Des représentants des administrations sont également invités à participer aux groupes de travail (art. 23 des statuts).

Les relations avec les autorités administratives indépendantes (AAI)

Le Forum tient les AAI périodiquement informées de l'avancement de ses travaux. Chaque AAI intéressée (CSA, ART, CNIL, Conseil de la Concurrence.) désigne un de ses membres comme correspondant permanent de l'association. Ces correspondants peuvent être invités à participer au conseil d'orientation. Par ailleurs, des représentants des AAI interviennent dans les groupes de travail (art. 24 des statuts).

4. Coopération intergouvernementale :

- L'Union européenne a, par décision 276/1999CE du 25 janvier 1999, mis en place un plan d'action pluriannuel visant à promouvoir une utilisation plus sûre d'Internet (Safer Internet et Safer Internet Plus) notamment à travers la lutte contre les contenus illicites et préjudiciables diffusés sur les réseaux mondiaux. Sont ainsi encouragés l'auto-réglementation de l'industrie d'Internet et le développement de dispositifs de filtrage.
- Dans le cadre du G8, le groupe de Lyon " High Tech ", qui traite de la criminalité organisée sur les réseaux de télécommunications , a encouragé l'OSCE dans son initiative de lutte contre le racisme et l'antisémitisme sur l'Internet lors de sa réunion à Paris le 19 novembre 2003.

5. Contribution des acteurs privés (société civile, industriels et associations) français :

5.1 AFA

L'Association Française des Fournisseurs d'accès et de services Internet adhère aux axes définis par la Commission européenne pour un Internet plus sûr : signalement, sensibilisation, logiciels de filtrage pour l'utilisateur final.

S'agissant de la recherche des auteurs de crimes ou de délits, les données conservées par les fournisseurs d'accès et transmises le cas échéant sur réquisition judiciaire sont essentielles.

L'AFA, constitue le point de contact français En effet, depuis 1998, l'AFA anime le site d'assistance http://www.pointdecontact.net ouvert à tous les internautes, qui permet de signaler les contenus de pornographie enfantine ou d'incitation à la haine raciale (222 des 4 700 signalements reçus et traités par l'AFA entre novembre 2002 et octobre 2003 concernaient l'incitation à la haine raciale) , et donne des informations détaillées sur les textes applicables en la matière. Ce site apporte également aux citoyens tous les renseignements utiles au signalement d'autres contenus potentiellement illégaux, et notamment les adresses appropriées des autorités publiques et des membres de l'AFA. Il informe enfin sur les logiciels de filtrage disponibles en langue française.

5.2 MRAP

Le MRAP (mouvement contre le racisme et pour l'amitié entre les peuples) a, à titre d'exemple relevé et suivi 59 cas d'injures et d'écrits racistes publiés sur Internet en 2002, 51 cas en 2003 et 26 au premier trimestre 2004. 37% ont été classés sans suite, 7% d'entre eux concernaient des sites hébergés à l'étranger. Le MRAPreçoit en moyenne 300 signalements par an.. Le MRAP estime que s'échangent quotidiennement des centaines de messages racistes. Ne pouvant en diriger vers les services compétents qu'environ un cinquième, il se propose de créer une cellule de suivi des contenus.

6. Existe-t-il des organisations ou réseaux, comme Inhope et Inach, qui recherchent et font de la veille sur la propagande raciste et l'incitation à la violence sur l'Internet ?

L'association française des fournisseurs d'accès et de services ou AFA participe au réseau INHOPE. (voir plus haut)

Le MRAP s'appuie sur le réseau des ONG européennes INACH compétent dans le domaine de la connaissance des sites et des modes de diffusion des propos appelant à la haine raciale. Il souhaite créer une cellule de veille des contenus racistes sur l'Internet pour prendre la mesure du discours illicite francophone, établir des liens avec les ONG espagnoles en ce domaine et s'interconnecter avec le réseau INACH (Internationale network against cyberhate). Il souhaiterait faciliter les signalements auprès des institutions et des intermédiaires techniques et recenser les bonnes pratiques existantes.

IV Mesures visant à éduquer les usagers et assurer une meilleure prise de conscience du public

1. Efforts pour informer les jeunes et les éducateurs

Le Forum des droits sur l'Internet a lancé en mars 2002 le site DroitDuNet.fr (http://www.droitdunet.fr), qui place le droit et les usages de l'Internet à la portée de tous les utilisateurs du réseau. Plus d'une centaine de fiches pratiques décrivent les règles et les bonnes pratiques applicables à la plupart des usages du réseau. Le Forum édite également des guides pratiques à destination des internautes sur des thématiques spécifiques (téléprocédures, protection des mineurs…) et participe à certaines actions de sensibilisation et de formation, notamment auprès des enseignants.

Le Conseil consultatif de l'Internet, structure de concertation associant des utilisateurs de l'Internet, des représentants des acteurs économiques et associatifs et des élus du parlements a été créé le 8 décembre 2003 (décret N. 2003-1167) pour renforcer la co-régulation de l'Internet. Le Forum des droits sur l'Internet en assure le secrétariat.

2. Programmes spécifiques

Le ministère de Education nationale, de l'Enseignement supérieur et de la Recherche a développé une démarche de sensibilisation et de responsabilisation des enseignants, des élèves et des parents eu égard aux valeurs républicaines de civilité, de respect et de justice (examens informatiques pour les enseignants et les élèves). Il encourage les établissements scolaires à l'usage d'une charte générale d'utilisation des réseaux :

(http://www.educnet.education.fr/chargt/charteproj.pdf)

L'Université de Sciences sociales de Toulouse 1 a été pionnière en matière de recueil du nom des sites (liste noire) considérés comme inappropriés pour les mineurs (http://www.educnet.education.fr/aiedu/listenoire.htm). Une liste noire spécifique aux sites racistes et antisémites est en cours d'élaboration, dans le cadre du projet européen Safer Internet Action Plan/PRINCIP (PRINCIP est un système de détection automatique des pages web racistes, antisémites, xénophobes et négationistes en allemand, anglais et français ; les partenaires du projet sont l'institut national des langues et civilisations orientales, l'Université Pierre et Marie Curie, de Paris , Dublin, City University d'Irlande et Otto-von Guericke Magdeburg Universität, en Allemagne). Ces listes noires permettent de créer, dans l'Éducation nationale un Internet où tout est autorisé sauf la consultation de quelques sites.

Afin de suivre le projet de protection des mineurs, les chefs d'établissement sont appelés, à compter de mars 2004, à renseigner régulièrement un formulaire signalant les difficultés éventuelles rencontrées.

3. Initiatives de l'industrie à cet égard

L'association française des fournisseurs d'accès considère l'information et la pédagogie comme des éléments centraux dans la lutte contre les contenus illégaux et notamment l'incitation à la haine raciale. Cette volonté d'informer les internautes sur la loi applicable et la façon dont ils peuvent réagir face aux contenus illicites (pornographie infantile ou racisme) a présidé à la création du point de contact de l'AFA en 1998.

L'AFA propose son travail de synthèse et d'explication sur les sites http://www.pointdecontact.net/haine.htm et http://www.pointdecontact.net/protection de l'enfance.html, relayés sur son portail : http://www.afa-france.com

V. Mesures prises par l'industrie de l'Internet

1. Code professionnel d'éthique ou de bonnes pratiques mis en place et principaux aspects de ces codes

En concertation avec le gouvernement l'Association des fournisseurs d'accès et de services Internet a publié le 29 mars [2004] une charte par laquelle les hébergeurs prennent l'engagement de lutter contre les contenus pédo-pornographiques et racistes ou antisémites sur l'Internet .
S'appuyant sur le point de contact créé en 1998 et permettant le signalement par les internautes des contenus illicites dans les domaines précités, la charte prévoit :
- une communication renforcée sur les moyens mis à disposition du public pour les aider à signaler ces contenus ;
- Un engagement de chaque hébergeur à rendre le signalement de ces contenus plus aisé sur ses services en ligne ;
- Pour tout professionnel qui aurait pris connaissance de tels contenus l'engagement de les signaler sans délai aux services de police.
Ces mesures viennent s'ajouter à celles prises depuis plusieurs années en matière de coopération avec les pouvoirs publics :
- formation des officiers de police judiciaire et des magistrats ;
- participation à des groupes de travail communs police- industrie ;
- action pour la protection de l'enfance.

2. Hotlines mises en place par l'industrie.

cf. plus haut, hotline de l'AFA et réseau européen Inhope

Source :
http://www.diplomatie.gouv.fr/actu/article.asp?ART=42736

PROPOSITION VISANT À ABOLIR UNE FOIS POUR TOUTES LES LOIS QUI PROTÈGENT ENCORE UN PEU LA LIBERTÉ D'EXPRESSION

Projet de loi relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques présenté le 28 janvier 2004 au Conseil des ministres [français]

Le ministre des affaires étrangères a présenté en conseil des ministres le mercredi 28 janvier 2004 un projet de loi sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.
Le projet de loi autorise **l'approbation d'un protocole additionnel** à la convention européenne sur la cybercriminalité adoptée à Budapest le 23 novembre 2001. Il vise à harmoniser le droit pénal français et européen dans le domaine d'actes de nature raciste et xénophobe sur des sites Internet, des listes de discussion ou des forums publics.

Seraient ainsi incriminés :
* la diffusion de matériel raciste et xénophobe,
* des insultes et menaces motivées par des considérations racistes et xénophobes,
* **l'expression publique de propos négationnistes ou révisionnistes** ou la justification publique de faits de génocide ou de crime contre l'humanité.

Le Protocole prévoit de **faciliter l'extradition au sein de l'espace européen** et l'entraide judiciaire pour la répression de ces agissements.

ARTESI
http://www.artesi.artesi-idf.com/public/article.tpl?id=6483 .

Voici donc un projet radical qui vise à faire de nous des hors-la-loi en Europe, avec chasse à courre garantie et geôle globale à la clé. Une Europe comme Orwell l'avait rêvée dans ses pires cauchemars. Pour en savoir plus, il faut donc se reporter d'abord à la Convention européenne de Budapest, qui pourrait ne pas être dans toutes les mémoires, et à son sulfureux Protocole additionnel, dont il faut comprendre pourquoi il a été rajouté plus tard à ce petit monument d'ignominie et de mépris du Droit :

Convention sur la cybercriminalité

Budapest, 23.XI.2001

Protocole

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 cyber-espace, 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 États et l'industrie privée dans la lutte contre la cybercriminalité et le besoin de protéger les intérêts légitimes liés au 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, l'intégrité et la disponibilité des systèmes informatiques, des réseaux et des données ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit de 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 de la protection des données personnelles, telle que la confère, par exemple, 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 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 procédures pénales portant sur des infractions pénales en relation avec des systèmes et 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 cyber-espace, et notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant la Recommandation N°(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, la Recommandation N° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, la Recommandation N° R(87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, la Recommandation 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 la Recommandation 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 la Recommandation 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 à leur 21e Conférence (Prague, juin 1997) qui recommande au Comité des Ministres de soutenir les activités menées par le Comité européen pour les problèmes criminels (CDPC) concernant la cybercriminalité afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution N°3, adoptée lors de la 23e Conférence des Ministres européens de la Justice (Londres, juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions adaptées permettant au plus grand nombre d'Etats d'être parties à la Convention et 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 Deuxième Sommet (Strasbourg, 10 - 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 – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention, l'expression:

a. «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. «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. «fournisseur de service» désigne :

i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

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 du 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 et 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 – 5 ci-dessus ;

ii. d'un mot de passe, d'un code d'accès ou des 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 – 5 ; et

b. la possession d'un élément visé aux paragraphes (a) (1) ou (2) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 – 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 interpréter 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'a pas pour but de commettre une infraction établie conformément à l'Article 2 à 5 de la présente Convention, comme en cas d'essais autorisés 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)(2).

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 en droit interne 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 par:

a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques,

b. 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, la «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 (d) et 1 (e) et 2 (b) et 2 (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 définie par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971, 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 celle-ci a souscrites en application de la Convention internationale sur la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion faite à Rome (Convention de Rome), de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations, exécutions et 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 9(1)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 faire en sorte 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, sur les bases suivantes:

a. un pouvoir de représentation de la personne morale;

b. une autorité pour prendre des décisions au nom de la personne morale;

c. une autorité pour exercer un contrôle au sein de la personne morale.

2. Outre les cas déjà prévus au paragraphe 1, chaque Partie adopte les mesures nécessaires pour s'assurer qu'une personne morale puisse 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 visées au paragraphe 1 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 faire en sorte que les infractions pénales établies en application des articles 2 - 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 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 :

a. aux infractions pénales établies conformément aux articles 2-11 de la présente Convention ;

b. à toutes 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 qui

i. est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii. n'emploi[e] pas les réseaux publics de télécommunications 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 du pouvoir ou de la procédure 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 protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

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

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

Article 17 – Conservation et divulgation rapides de données relatives au trafic

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

a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication; et

b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service 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 la possession où sous le contrôle de cette personne, et 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, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte 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 service ;

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 service.

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 un d'un 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 ; et

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 à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. 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 relativement à un éventail d'infractions graves à définir en droit interne, à :

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

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire , ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis 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 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 et15.

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 – 11 de la présente Convention, lorsque l'infraction est commise:

a. sur son territoire ;

b. à bord d'un navire battant pavillon de cette Partie ;

c. à bord d'un aéronef immatriculé dans cette Partie ;

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 conditions spécifiques, les règles de compétence définies aux paragraphes 1b – 1d 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 décider quelle est celle qui est 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 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 les unes avec les autres, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1. a. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, c'est la peine minimum prévue par ce traité ou cet arrangement qui 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 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 le cryptage si nécessaire), 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, en relation avec 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 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 ne soient utilisées que sous 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 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 restent confidentiels, 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 de tels 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 que 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 à la condition :

a. que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou

b. 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 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 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

qu'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

a. si la Partie requise estime que le fait d'accéder de 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 pour garantir la disponibilité future des données, 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 60 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. Lorsqu'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 service 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, et 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 évoqués 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 évoqués 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 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 24 heures sur 24, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et 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 ; et

c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2. a. Le point de contact d'une Partie pourra 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 auprès du 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 et 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 sur lesquels 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 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 concernant les 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 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 État fédéral peut se réserver le droit d'honorer les obligations aux termes du 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 États 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 œuvre 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 aux Article 4, paragraphe 2, Article 6, paragraphe 3, Article 9, paragraphe 4, Article 10, paragraphe 3, Article 11, paragraphe 3, Article 14, paragraphe 3, Article 22, paragraphe 2, 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. 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 États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État 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 Comité européen pour les problèmes criminels (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 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 Comité européen pour les problèmes criminels, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord commun 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 Comité européen pour les problèmes criminels (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 Comité européen pour les problèmes criminels (CDPC) procèdera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les aménagement 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 États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État 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 des Articles 40 et 41 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, et 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.

http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

LE PROTOCOLE ADDITIONNEL, GUILLOTINE DE L'AVENIR

Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'acte de nature raciste et xénophobe commis par le biais de systèmes informatiques

Strasbourg, 30.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.

2 Une Partie peut:

a soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule;

b soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

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

1 Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.

2 Une Partie peut:

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

b soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Article 7 – Aide et complicité

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

Chapitre III – Relations entre la Convention et ce Protocole

Article 8 – Relations entre la Convention et ce Protocole

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

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

Chapitre IV – Dispositions finales

Article 9 – Expression du consentement à être lié

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

a la signature sans réserve de ratification, d'acceptation ou d'approbation; ou

b la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.

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

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

Article 10 – Entrée en vigueur

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

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

Article 11 – Adhésion

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

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

Article 12 – Réserves et déclarations

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

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

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

Article 13 – Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 12 ci-dessus retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception d'une notification de retrait par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

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

Article 14 – Application territoriale

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

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

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

Article 15 – Dénonciation

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

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

Article 16 – Notification

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

a toute signature;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

c toute date d'entrée en vigueur du présent Protocole conformément à ses articles 9, 10 et 11;

d tout autre acte, notification ou communication ayant trait au présent Protocole.

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

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

Conseil de l'Europe

http://conventions.coe.int/Treaty/FR/Treaties/Html/189.htm

Voir les signatures et les ratifications :
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=1&DF=&CL=FRE

A la date du 23 septembre 2005, il y avait quatre ratifications adhésions enregistrées (Albanie, Danemark, Chypre et Slovénie. Les poids lourds ont signé mais se sont bien gardés de ratifier.) Si un cinquième Etat ratifie, ce protocole additionnel deviendra applicable dans les pays qui l'auront ratifié.

On voit bien que l'article 6 2 b a pour fonction de laisser possible l'adhésion d'Etats qui protègent plus ou moins la liberté d'expression, comme les Etats-Unis avec leur Premier Amendement.

Signalons la création récente d'une nouvelle officine de propagande et de contrôle de l'internet, sous les espèce d'un « Observatoire pour la Prévention de la Haine sur Internet » :

Lancement de l'Observatoire (OPHI)

mardi 3 mai 2005.

L'Observatoire pour la prévention de la haine sur Internet a été créé en 2005. Outil organisationnel de la lutte contre les contenus incitant à la haine, il utilisera les données collectées dans sa base de données à l'établissement de son rapport annuel, parallèlement à ses propres observations.

L'accumulation des données et travaux de l'OPHI sur plusieurs années permettra par la suite d'établir des études évolutives et des études transversales de la haine sur Internet, dans un but de prévention, d'autorégulation du web et de renforcement des moyens de lutte contre ce phénomène.
http://www.observatoire-haine.net/article.php3?id_article=13

Ce vocabulaire est très révélateur. Le terme de « haine » qui relève d'un vocabulaire assez désuet du registre des passions a été confisqué aux Etats-Unis, pour renouveler le concept fatigué, éculé, épuisé, d'«antisémitisme», un terme dont l'absurdité constitutive se révèle au premier examen. Les spécialistes américains de l'exercice de l'hégémonie juive sur les expressions politiques publiques (ADL et assimilés) se présentent comme des victimes (imaginaires) d'une haine (vague et encore plus imaginaire), ce qui permet de déguiser leur volonté de domination sous le vocable plus acceptable de «défense», de défenser « contre la haine ». On a donc vu fleurir aux Etats-Unis toutes sortes d'organisations fantômes et de sites dévoués à la « lutte contre la Haine » ou la « cyberhaine ». Depuis six ou sept ans, le terme perfuse dans toute l'Europe et en particulier dans le milieu sioniste français et on voit apparaître ainsi des initiatives « contre la HAINE ». Il faut les replacer dans le cadre de l'intervention en Europe, de plus en plus incisives, des puissantes et richissimes organisation judéo-sionistes américaines, celles qui forment le « lobby », une fédération qui a pignon sur rue à Washington, et qui est légale. Ce lobby téléguide des groupes comme le centre Wiesenthal (le diable ait son âme) qui ont le savoir faire médiatique. Ils recrutent en France quelques excités du bulbe qui rêvent de jouer les Fouquier-Tinvelle, comme les Marc Knobel, Jean-Yves Camus, et d'autres zozos, logés dans de somptueux bureaux du quartier des Champs Elysée, les seuls que peuvent décemment fréquenter leur riches mécènes.

En fait de haine, on peut remarquer celle que les militants sionistes éprouvent à l'égard de leurs adversaires politiques. On ne compte plus les agressions physiques, les dégradations, les coups et blessures infligés en toute impunité par les haineux sionistes. De leur haine à eux, ils ne parlent évidemment jamais.

En collant l'étiquette de « haine » ou « haineux » à tout ce qui déplaît à l'establishment sioniste, ces flics d'opérette espèrent faire taire les critiques qui s'élèvent contre l'inqualifiable occupation de la Palestine par les soudards judéo-israéliens. Ce sont ces critiques, cette voix qui monte qui empêchent les sionistes de remplir leur programme qui aboutit au génocide des populations palestiniennes. L'enjeu est donc crucial et il importe de comprendre que

L'usage du mot « haine » décèle une manipulation sioniste

http://litek.ws/aaargh
http://aaargh.com.mx
http://vho.org/aaargh

mailto : aaarghinternational@hotmail.com