

Département Thématique C
Droits des Citoyens et Affaires Constitutionnelles



**RENFORCEMENT DE LA SECURITE
ET DES LIBERTES FONDAMENTALES SUR INTERNET
ET POLITIQUE DE L'UE EN MATIERE DE LUTTE
CONTRE LA CYBERCRIMINALITE**

LIBERTES CIVILES, JUSTICE ET AFFAIRES INTERIEURES



PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

**Direction Générale Politiques Internes de l'Union
Département Thématique C
Droits des Citoyens et Affaires Constitutionnelles**

RENFORCEMENT DE LA SECURITE ET DES LIBERTES FONDAMENTALES SUR INTERNET ET POLITIQUE DE L'UE EN MATIERE DE LUTTE CONTRE LA CYBERCRIMINALITE

ETUDE

Résumé:

La présente étude examine les aspects liés aux droits de homme sur Internet et étudie en détail les règles de droit pénal du Conseil de l'Europe et de l'UE pertinentes en la matière. Il passe également en revue d'autres aspects liés à cybercriminalité, tels que les droits relatifs à la protection des données, le programme Safer Internet de l'UE, la pédopornographie, les attaques menées contre les systèmes d'information, le terrorisme, le racisme et la xénophobie.

L'étude conclut que l'UE devrait fixer les priorités suivantes en la matière:

- a) l'adoption d'une Charte des droits de l'Internet non contraignante - un projet est présenté en Annexe;
- b) l'élaboration d'un droit pénal matériel et de procédure de l'UE relatif à la cybercriminalité;
- c) la définition d'une action opérationnelle de l'UE concernant la cybercriminalité

Cette étude a été demandée par la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (**LIBE**).

Le présent document est publié dans les langues suivantes: EN, FR.

Auteur: **Steve Peers (Université d'Essex)**

Sous la coordination du Département de Justice et Affaires Intérieures du Centre for European Policy Studies (CEPS).

Manuscrit achevé en **janvier 2009**

Pour obtenir des copies, veuillez vous adresser à :

M. Alessandro DAVOLI
Administrateur Département Thématique C
Tel: 32 2 2832207
Fax: 32 2 2832365
E-mail: alessandro.davoli@europarl.europa.eu

Informations sur les **publications de la DG IPOL**:

<http://www.europarl.europa.eu/activities/committees/studies.do?language=EN>

<http://www.ipolnet.ep.parl.union.eu/ipolnet/cms/pid/438>

Bruxelles, Parlement européen

Les opinions exprimées sont celles de l'auteur et ne reflètent pas nécessairement la position officielle du Parlement européen.

TABLE DES MATIERES

I. INTRODUCTION.....	4
II. PROTECTION DES DROITS DE L'HOMME SUR INTERNET	4
III. CYBERCRIMINALITE.....	5
1. Mesures adoptées par le Conseil de l'Europe	5
1.1 Convention sur la cybercriminalité	5
1.2 Protocole à la convention sur la cybercriminalité.....	7
1.3 Convention pour la prévention du terrorisme	8
1.4 Convention pour la protection des enfants contre l'exploitation et les abus sexuels	10
2. Mesures adoptées par la CE et par l'UE	13
2.1 Droit matériel – Mesures du troisième pilier	13
2.1.1. <i>Attaques menées contre les systèmes d'information</i>	13
2.1.2. <i>Exploitation sexuelle des enfants et pédopornographie</i>	15
2.1.3 <i>Terrorisme</i>	20
2.1.4. <i>Racisme et xénophobie</i>	23
2.2 Droit de la CE – Mesures du premier pilier	26
2.2.1 <i>Droits de propriété intellectuelle</i>	26
2.2.2 <i>Autres mesures</i>	26
2.3 Droit de procédure	27
2.4 Autres mesures de la CE et de l'UE	27
IV. CONCLUSIONS	29
ANNEXE: Charte des droits de l'Internet	30

I. INTRODUCTION

L'UE et le Conseil de l'Europe ont déjà adopté un certain nombre de mesures de différents types concernant directement ou indirectement la question de la cybercriminalité et la protection des droits de l'homme dans le cadre d'Internet. La présente étude examine ces mesures en détail. Cependant, vu l'évolution d'Internet ces dernières années, le présent document suggère également d'autres mesures que l'UE pourrait envisager de prendre dans ce domaine.

II. PROTECTION DES DROITS DE L'HOMME SUR INTERNET

De toute évidence, l'activité sur Internet est généralement régie par les mêmes mesures de protection des droits de l'homme dérivant, dans leur sphère d'application respective, des lois et constitutions nationales, des traités internationaux sur les droits de l'homme (en particulier la Convention européenne des droits de l'homme), des principes généraux du droit communautaire ainsi que de la Charte des droits fondamentaux de l'UE.

Les droits de l'homme les plus fréquemment invoqués dans le contexte d'Internet sont le droit au respect de la vie privée et à la protection des données personnelles, ainsi que la liberté d'expression. Au nombre des autres droits particulièrement concernés par Internet, citons le droit de non-discrimination (en termes d'accès à Internet et en termes de protection contre, par exemple, les expressions d'incitation à la haine raciale et à la violence), le droit de propriété (particulièrement la propriété intellectuelle), la protection de la dignité humaine (concernant, par exemple, la mise en ligne de courriels ou de contenus abusifs sur les sites de socialisation) et les droits de l'enfant, à la fois contre les risques d'abus sur Internet et de leur droit à avoir accès à Internet dans le cadre de leur éducation et de l'expression sociale et culturelle.

La rédaction et la promotion d'une 'Charte des droits de l'Internet' pourraient résumer ces droits et les soumettre à l'attention des utilisateurs d'Internet, des acteurs de l'industrie, du secteur public (organismes de régulation, officiers de police, enseignants, etc.), des ONG pertinentes et des médias. La Charte des droits pourrait, dans un premier temps, être rédigée par le Parlement européen, puis être ouverte à la signature et/ou au soutien des acteurs de l'industrie, des ONG, des Etats membres, d'autres institutions de l'UE, des organes médias et autres. Cette charte pourrait être avalisée et promue sur les sites web de sociétés, d'ONG, d'institutions de l'UE et d'organes nationaux du secteur public.

Nous ne suggérons pas de dresser une liste de nouveaux droits ou de créer un instrument légalement contraignant, mais plutôt, d'établir une 'vitrine' des droits pertinents, afin d'informer le public sur l'application des principes des droits de l'homme sur Internet.

Une proposition de Charte des droits de l'Internet est reprise en annexe, à titre d'exemple. Les droits stipulés dans la Charte des droits ont été directement extraits des dispositions les plus pertinentes de la Charte des droits fondamentaux de l'UE, à l'exception du dernier article, l'Article 14, qui est une nouvelle disposition portant sur le contenu et l'interprétation des droits (paragraphe 1), basée sur les dispositions générales des articles 51-54 de la Charte et confirmant l'existence d'autres droits (paragraphe 2). La formulation de la disposition concernant la protection des

consommateurs a également été revue pour faire expressément référence à Internet (Article 13).

Le projet de Charte pourrait être amendé, le cas échéant, pour faire référence plus en détail au contexte d'Internet, par exemple pour les règles relatives à la confidentialité des communications, à l'interdiction des 'spams' et à la protection des enfants.

III. CYBERCRIMINALITE

1. Mesures adoptées par le Conseil de l'Europe

1.1 Convention sur la cybercriminalité

La principale mesure adoptée par le Conseil de l'Europe relative à la question de la cybercriminalité est, de toute évidence, la Convention sur la cybercriminalité du Conseil de l'Europe (ETS 185), ouverte à la signature en 2001 et entrée en vigueur le 1^{er} juillet 2004. Au 14 janvier 2009, la Convention a été ratifiée par 23 états au total, y compris 15 Etats membres de l'UE et un état non membre du Conseil de l'Europe (les USA). Elle a en outre été signée par 23 autres états, y compris les 12 Etats membres restants (Autriche, Belgique, Allemagne, Grèce, République tchèque, Irlande, Luxembourg, Malte, Pologne, Portugal, Suède et Royaume-Uni), ainsi que par trois états non membres du Conseil de l'Europe (Canada, Japon et Afrique du Sud).

Après les définitions des termes clés à l'Article 1, la Convention stipule plusieurs catégories d'infractions matérielles que les parties doivent établir. Premièrement, la Convention expose six infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques: l'accès illégal; l'interception illégale; l'atteinte à l'intégrité des données; l'atteinte à l'intégrité du système et l'abus de dispositifs (Articles 2 à 6). Les Etats peuvent limiter (mais pas exclure complètement) leurs obligations d'ériger ces actes en infractions pénales, sauf pour l'atteinte à l'intégrité du système. Ensuite, la Convention stipule deux infractions contre les systèmes informatiques, mais non spécifiques au monde en ligne: la falsification informatique et la fraude informatique (Articles 7 et 8). En ce qui concerne la falsification, les parties peuvent exiger une intention malhonnête.

Troisièmement, la Convention formule une infraction se rapportant au contenu, concernant la pornographie infantine. Cette infraction se réfère à la production, l'offre ou la mise à disposition, la diffusion ou la transmission, le fait de se procurer ou de procurer à autrui, ou la possession de pornographie infantine, via un système informatique (Article 9(1)). La pornographie infantine est définie comme un mineur 'se livrant à un comportement sexuellement explicite' (cette notion n'est pas plus amplement définie dans la Convention elle-même), ou une personne qui paraît être un mineur se livrant à ce type de comportement, ou 'des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite' (Article 9(2)). Un 'mineur' désigne toute personne âgée de moins de 18 ans. Un état peut toutefois fixer une limite d'âge inférieure, de 16 ou 17 ans (Article 9(3)). Un état peut choisir de ne pas ériger en infraction pénale la possession ou le fait de se procurer ou de procurer à autrui de la pornographie infantine, ou d'exclure la responsabilité si les images ne concernent pas des enfants réels (Article 9(4)).

Enfin, la Convention impose l'obligation d'ériger en infraction pénale certaines atteintes à la propriété intellectuelle ou aux droits connexes, 'lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique' (Article 10), même si les états peuvent se réserver le droit de ne pas

imposer de responsabilité pénale pour ces actes s'ils ont mis en place un autre système de recours efficace contre ces infractions (Article 10(3)).

Les états sont également tenus d'ériger en infraction pénale les infractions auxiliaires d'aide et de complicité en vue de la perpétration des infractions pénales principales stipulées (Article 11(1)), ainsi que les tentatives visant à commettre la plupart de ces infractions (Article 11(2)), même si les parties peuvent se réserver le droit de ne pas appliquer, en tout ou en partie, de responsabilité pénale pour les tentatives (Article 11(3)).

Les parties sont tenues d'étendre leur compétence non seulement à leur territoire, mais aussi aux navires battant leur pavillon, aux aéronefs immatriculés sur leur territoire ainsi qu'à leurs 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 état (Article 22(1)). Toutefois, des réserves sont admises concernant l'extension de compétence au-delà du territoire (Article 22(2)). La Convention stipule l'obligation d'extrader ou poursuivre ses propres ressortissants (Article 22(3)), et de se concerter quand plusieurs parties revendiquent une compétence (Article 22(5)), 'afin de déterminer la mieux à même d'exercer les poursuites'.

Les Etats membres de l'UE ayant ratifié la Convention ont formulé des réserves dans ce domaine concernant: la définition de la pornographie infantile (Danemark, France, Hongrie); les règles concernant l'accès illégal (Finlande, Lituanie, Slovaquie); l'atteinte à l'intégrité du système (Slovaquie); la pénalisation des tentatives (Finlande); et les règles de compétence (France, Lettonie).

La Convention stipule des règles spécifiques concernant le droit procédural (Articles 14-21). Ces règles sont soumises aux 'conditions et sauvegardes' générales prévues par le droit interne des états, qui doit assurer une protection adéquate des droits de l'homme et intégrer le principe de la proportionnalité (Article 15(1)). Lorsque cela est approprié, 'eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question' (Article 15(2)). En outre, les parties sont tenues d'examiner l'effet des règles de procédure sur 'les droits, responsabilités et intérêts légitimes des tiers'. Cette obligation s'applique toutefois 'dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice' (Article 15(3)).

Les obligations détaillées concernant le droit procédural sont les suivantes: la conservation rapide de données informatiques stockées; la conservation et divulgation rapides de données relatives au trafic; les injonctions de produire relatives à des données informatiques; la perquisition et saisie de données informatiques stockées; la collecte en temps réel des données relatives au trafic; et l'interception de données relatives au contenu. Toutefois, des réserves sont autorisées concernant les deux derniers points quand il n'est techniquement pas possible de collecter de telles données (Articles 20(2) et 21(2)), et l'obligation d'intercepter des données relatives au contenu ne s'applique qu'à 'un éventail d'infractions graves à définir en droit interne'. De même, les parties peuvent se réserver le droit de n'appliquer l'obligation de collecter des données relatives au trafic qu'à des catégories d'infractions spécifiées, pour autant que l'éventail de ces infractions ne soit pas plus réduit que celui des infractions pour lesquelles l'état collecte des données relatives au contenu (Article

14(3)(a)). Les parties peuvent également se réserver le droit de ne pas appliquer les obligations découlant de ces articles si leur législation nationale ne permet pas la prise de telles mesures contre des systèmes informatiques privés (Article 14(3)(b)).

Les Etats membres de l'UE qui ont ratifié la Convention ont formulé des réserves dans ce domaine en vue de limiter la collecte de données relatives au trafic à certaines infractions (Bulgarie, Danemark, Finlande) et concernant les systèmes informatiques privés (Finlande). La France a fait une déclaration spécifiant quand l'obligation de collecter des données relatives au contenu peut s'appliquer en droit français.

Le chapitre sur la coopération internationale (Articles 23-35) stipule des règles générales relatives à l'extradition et à l'entraide, ainsi que des dispositions spécifiques sur les demandes de conservation de données informatiques stockées, la divulgation rapide de données conservées relatives au trafic, l'accès aux données informatiques stockées, la collecte en temps réel de données relatives au trafic ou l'interception de données relatives au contenu. Les parties doivent également établir un réseau '24/7' assurant une assistance pour les investigations et les poursuites.

La Convention contient une autorisation générale accordée aux parties d'appliquer des règles particulières entre elles, sans référence spécifique à la CE ou à l'UE (Article 39(2)):

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

1.2 Protocole à la Convention sur la cybercriminalité

Le Protocole (ETS 189) a été ouvert à la signature en 2003 et est entré en vigueur le 1^{er} mars 2006. Il a été ratifié par 21 états et signé par 13 états en date du 14 janvier 2009. Il a été ratifié par 6 Etats membres de l'UE (Chypre, Danemark, France, Lettonie, Lituanie et Slovaquie) et signé par 13 Etats membres (Autriche, Belgique, Estonie, Finlande, Allemagne, Grèce, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie et Suède). Huit Etats membres n'ont pas signé le Protocole (Bulgarie, République tchèque, Hongrie, Irlande, Italie, Slovaquie, Espagne et Royaume-Uni).

Le Protocole concerne exclusivement la question du droit pénal matériel relative au 'matériel raciste et xénophobe' (comme défini à l'Article 2(1) du Protocole, et plus amplement expliqué ci-dessous). Il demande aux parties de veiller à ce que quatre actes spécifiques soient érigés en infraction pénale dans leur droit interne: la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques (Article 3); la menace, par le biais d'un système informatique, de commettre une infraction pénale grave envers un groupe qui se caractérise par sa race, et autres ou par sa religion (Article 4); l'insulte, par le biais d'un système informatique, d'une personne ou d'un groupe en raison de sa race, et autres ou de sa religion ou autres (Article 5); et la négation, minimisation grossière, approbation ou justification du

génocide ou des crimes contre l'humanité, tels que définis dans le Protocole, par le biais d'un système informatique (Article 6). Les parties doivent également ériger en infraction pénale le fait d'aider à perpétrer l'une de ces infractions ou d'en être complice (Article 7).

Toutefois, les parties sont habilitées à adopter des réserves sur plusieurs de ces articles, qui seront passés en revue plus loin.

1.3 Convention pour la prévention du terrorisme

Cette Convention (ETS 196, 2005) a été ratifiée par 15 états et signées par 28 autres états en date du 14 janvier 2009. Parmi les Etats membres de l'UE, 7 l'ont ratifiée (Bulgarie, Danemark, Finlande, France, Pologne, Roumanie et Slovaquie) et 19 l'ont signée (tous les autres Etats membres à l'exception de la République tchèque). La Convention est ouverte à la signature par la CE, mais la Communauté ne l'a pas encore signée. La Convention du Conseil de l'Europe pour la prévention du terrorisme est entrée en vigueur en juin 2007.

La Convention requiert des états qu'ils érigent en infraction pénale trois types d'actes pouvant être commis hors ligne et en ligne, mais qui, dans la pratique, sont souvent commis en ligne. Ces trois infractions sont : la 'provocation publique à commettre une infraction terroriste', telle que définie à l'Article 5; le 'recrutement pour le terrorisme', tel que défini à l'Article 6; et l' 'entraînement pour le terrorisme', tel que défini à l'Article 7. L'Article 8 de la Convention spécifie que pour que l'un de ces actes constitue une infraction, 'il n'est pas nécessaire que l'infraction terroriste soit effectivement commise'.

Les états doivent également ériger en infraction pénale la participation en tant que complice à l'une de ces infractions, l'organisation de la commission d'une infraction et le fait de donner l'ordre à d'autres personnes de la commettre, la contribution à la commission de ces infractions par un groupe de personnes et toute tentative (Article 9), même si l'obligation d'ériger en infraction pénale les tentatives ne s'applique pas à l'infraction de 'provocation publique'. Les sanctions pénales sont subordonnées aux obligations en matière de droits de l'homme ainsi qu'au principe de proportionnalité et 'devraient exclure toute forme d'arbitraire, de traitement discriminatoire ou raciste'. (Article 12). L' 'infraction terroriste' est définie par référence aux dix conventions internationales énumérées dans l'Annexe de la Convention (Article 1(2)).

Les parties sont tenues d'étendre leur compétence à leur territoire, aux navires battant leur pavillon et aux aéronefs immatriculés sur leur territoire, ainsi qu'aux actes commis par leurs ressortissants (Article 14(1)). Les états *peuvent* également établir leur compétence dans un certain nombre d'autres cas (Article 14(2)). La convention stipule une obligation de concertation quand plus d'une partie revendique une compétence (Article 14(5)), 'afin de déterminer celle qui est la mieux à même d'exercer les poursuites'. Elle prévoit en outre une disposition 'extrader ou poursuivre' forte (Article 18). La 'clause d'exception politique' traditionnellement applicable à la coopération pénale internationale doit être abolie pour les infractions définies dans la Convention, même si les parties sont habilitées à formuler une réserve pour continuer à l'appliquer (Article 20). Il n'y a aucune obligation d'extrader ou d'accorder l'entraide 'si la Partie requise a des raisons sérieuses de croire que la demande d'extradition motivée par une infraction [énumérée dans la Convention]... ou d'entraide judiciaire eu égard à de telles infractions a été présentée aux fins de

poursuivre ou de punir une personne pour des considérations de race, de religion, de nationalité, d'origine ethnique ou d'opinions politiques, ou que la situation de cette personne risque d'être aggravée pour l'une ou l'autre de ces raisons' (Article 21(1)). De même, il n'y a aucune obligation d'extrader si la personne faisant l'objet de la demande d'extradition risque d'être exposée à la torture ou à des traitements inhumains ou dégradants (Article 21(2)), ou risque d'être exposée à la peine de mort ou à la peine privative de liberté à perpétuité, si l'état requis n'impose pas l'emprisonnement à perpétuité comme sanction (Article 21(3)).

Enfin, l'UE a insisté sur l'inclusion d'une clause de 'déconnexion' (Article 26(3)):

Les Parties qui sont membres de l'Union européenne appliquent, dans leurs relations mutuelles, les règles de la Communauté et de l'Union européenne dans la mesure où il existe des règles de la Communauté ou de l'Union européenne régissant le sujet particulier concerné et applicable au cas d'espèce, sans préjudice de l'objet et du but de la présente Convention et sans préjudice de son entière application à l'égard des autres Parties.

Le rapport explicatif fait référence (paragraphe 272) à une déclaration formulée par la Communauté européenne et les Etats Membres lors de l'adoption de la Convention:

En demandant l'inclusion de la 'clause de déconnexion', la Communauté européenne/Union européenne et ses Etats membres réaffirment que leur objectif est de prendre en compte la structure institutionnelle de l'Union lorsqu'elles adhèrent à des Conventions internationales, en particulier en cas de transfert de pouvoirs souverains des Etats membres à la Communauté.

Cette clause n'a pas pour objectif de réduire les droits ou d'accroître les obligations des Parties non membres de l'Union européenne vis-à-vis de la Communauté européenne/Union européenne et de ses Etats membres, dans la mesure où ces dernières sont également Parties à la présente Convention.

La clause de déconnexion est nécessaire pour les dispositions de la Convention qui relèvent de la compétence de la Communauté/Union, afin de souligner que les Etats membres ne peuvent invoquer et appliquer, directement entre eux (ou entre eux et la Communauté/Union), les droits et obligations découlant de la Convention. Ceci ne porte pas préjudice à l'application complète de la Convention entre la Communauté européenne/Union européenne et ses Etats membres, d'une part, et les autres Parties à la Convention, d'autre part ; la Communauté et les Etats membres de l'Union européenne seront liés par la Convention et l'appliqueront comme toute autre Partie à la Convention, le cas échéant, par le biais de la législation de la Communauté/Union. Ils garantiront dès lors le plein respect des dispositions de la Convention vis-à-vis des Parties non membres de l'Union européenne.

Le rapport poursuit en affirmant : 'En tant qu'instrument établi à l'occasion de la conclusion d'un traité au sens de l'article 31, paragraphe 2, (b) de la Convention de Vienne sur le droit des traités, cette déclaration fait partie du "contexte" de la présente Convention.' Il indique également (en son paragraphe 273) que la CE 'serait en mesure de fournir, aux seules fins de transparence, l'information nécessaire concernant la répartition des compétences entre la Communauté et ses Etats membres dans les domaines couverts par la présente Convention, dans la mesure où cela n'implique pas d'obligations supplémentaires pour la Communauté.' Il convient

toutefois de noter que la CE n'a pas signé la Convention, et que la Commission n'a pas proposé qu'elle le fasse.

Lorsqu'il a ratifié la Convention, le Danemark s'est réservé le droit de ne pas abolir la clause d'exception politique concernant la 'provocation publique à commettre une infraction terroriste', y compris pour les infractions auxiliaires. La Hongrie a publié une déclaration interprétant l'Article 5 de la Convention concernant la définition de la 'provocation publique'.

1.4 Convention pour la protection des enfants contre l'exploitation et les abus sexuels

Cette Convention (ETS 201, 2007) a été signée par 20 Etats membres de l'UE et 13 états non membres, mais n'est pas encore entrée en vigueur. La Convention est également ouverte à la signature et à la conclusion par la CE, mais celle-ci ne l'a pas signée. Elle contient plusieurs dispositions relatives à la cybercriminalité. Premièrement, les Etats membres sont tenus d'ériger en infraction pénale les infractions de 'pornographie infantile' telle que définie à l'Article 20(2) de la Convention. Ces infractions impliquent, intentionnellement et 'sans droit', la production, l'offre ou la mise à disposition, la diffusion ou la transmission, le fait de se procurer ou de procurer à autrui, ou la possession de pornographie infantile, ou 'le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie infantile' (Article 20(1); les autres infractions pouvant être commises en ligne ou hors ligne). Les parties peuvent choisir de ne pas appliquer la dernière infraction (Article 20(4)), ou de ne pas ériger en infraction pénale la production et la possession de pornographie infantile lorsque les images ne concernent pas un enfant réel, ou impliquent des enfants ayant atteint l'âge de la majorité sexuelle, lorsque ces images sont produites et détenues par ceux-ci pour leur usage privé (Article 20(3)).

Comparé aux dispositions pertinentes de la Convention sur la cybercriminalité, cet Article n'est pas uniquement limité aux systèmes informatiques. L'infraction consistant à avoir accès à ce matériel est également nouvelle par rapport à cette convention. Aux termes de la Convention sur les enfants, un 'enfant' désigne une personne âgée de moins de 18 ans (Article 3(a)), tandis que la Convention sur la cybercriminalité permet d'abaisser cet âge à 16 ou 17 ans pour la pornographie infantile (Article 9(3) de la Convention sur la cybercriminalité). La Convention des enfants contient une définition plus précise de la pornographie infantile, qui ne se réfère pas expressément aux personnes qui *paraissent* être mineures. En ce qui concerne les réserves, la Convention des enfants permet une réserve générale concernant la nouvelle infraction de l'accès en ligne, mais, pour le reste, la possibilité de réserve est plus limitée : la convention sur la cybercriminalité autorise des réserves générales concernant les infractions consistant à procurer à autrui ou se procurer ou à posséder du matériel, ou le matériel n'impliquant pas des enfants réels, alors que la Convention des enfants n'autorise les réserves que pour la production ou la possession et seulement dans les cas impliquant soit du matériel ne concernant pas un enfant réel, ou produit par des mineurs ayant dépassé l'âge de la majorité sexuelle pour leur usage privé. Dès lors, les états qui ratifient la Convention des enfants ne peuvent plus s'abstenir d'ériger en infraction pénale le fait de procurer à autrui ou de se procurer de

la pornographie enfantine, et ne peuvent s'abstenir d'ériger la possession en infraction criminelle que dans des cas très spécifiques.

La Convention établit également des infractions pénales concernant les abus sexuels commis sur les enfants (Article 18), la prostitution enfantine (Article 19), la participation d'enfants à des spectacles pornographiques (Article 21) et la corruption d'enfants (Article 22), mais ces infractions ne peuvent de toute évidence qu'être commises hors ligne (il convient de noter que le rapport explicatif de la Convention indique que l'Article 21 'vise essentiellement les spectacles, organisés en direct, présentant des enfants se livrant à un comportement sexuellement explicite': paragraphe 147).

Enfin, la Convention inclut également une infraction de 'solicitation'. Les états doivent ériger en infraction pénale 'le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant n'ayant pas atteint l'âge' de la majorité sexuelle, dans le but d'avoir une activité sexuelle ou de produire de la pornographie enfantine, 'lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre' (Article 23). Aucune réserve ne peut être formulée concernant cet Article.

Les états doivent également ériger en infraction pénale l'aide et la complicité ainsi que la tentative de commettre de telles infractions. Cependant, des réserves sont admises concernant l'obligation d'ériger en infraction pénale les tentatives visant à commettre les infractions de sollicitation et de corruption, certains aspects de l'infraction de 'participation' et la plupart des infractions de pornographie enfantine (Article 24).

Il convient de noter que selon le rapport explicatif de la Convention, 'les négociateurs n'ont pas estimé opportun d'introduire dans la Convention de dispositions relatives à la connaissance ou à l'ignorance, par l'auteur présumé de l'infraction, de l'âge de la victime. Cette question relève donc de la législation et de la jurisprudence de chaque Partie' (paragraphe 115). Le rapport stipule en outre que 'les négociateurs reconnaissent que, dans certaines circonstances, lorsque des mineurs commettent des infractions (par exemple, lorsqu'ils produisent de la pornographie enfantine entre eux et pour leur usage privé mais qu'ils la diffusent par la suite ou la mettent en accès sur Internet), il pourrait y avoir des réponses plus appropriées que les poursuites pénales, et que celles-ci ne devraient être appliquées qu'en dernier ressort' (paragraphe 116). Quoi qu'il en soit, la Convention requiert des états qu'ils érigent en infraction pénale cette circulation plus vaste dans ce type de cas.

En ce qui concerne certains aspects spécifiques du droit matériel, le rapport explicatif indique que dans la Convention, l'infraction de 'pornographie enfantine' 'n'est pas limitée à la pornographie enfantine pratiquée au moyen d'un système informatique. Toutefois, avec l'utilisation croissante d'Internet, ce dernier est devenu l'instrument principal d'échange de ce type de contenus. On s'accorde largement à reconnaître que ce matériel et les pratiques en ligne qui lui sont associées contribuent à soutenir, à encourager ou à faciliter les infractions sexuelles commises à l'encontre d'enfants' (paragraphe 134). Le rapport clarifie par ailleurs le fait que 'la 'mise à disposition' vise à inclure, par exemple, la mise en ligne de pornographie enfantine devant être utilisée par autrui en créant des sites pédopornographiques. Ce paragraphe entend également s'appliquer à la création ou à la compilation d'hyperliens vers des sites de pornographie enfantine' (paragraphe 136). En outre, le terme 'transmettre' couvre 'le fait d'envoyer à autrui des supports pédopornographiques par un système informatique' (paragraphe 137). L'expression 'se procurer ou procurer à autrui' inclut

le ‘téléchargement de données informatiques’ (paragraphe 138). La possession inclut le matériel ‘stocké dans un système informatique’ (paragraphe 139). Le rapport donne également une description détaillée de l’infraction d’accès en ligne (paragraphe 140):

Il vise à permettre les poursuites à l'encontre de ceux qui regardent des images d'enfants sur des sites de pornographie infantile mais qui, ne les téléchargeant pas, se mettent à l'abri de l'infraction consistant à procurer ou à posséder ces images dans certains systèmes juridiques. Pour être punissable, la personne doit avoir eu l'intention d'entrer sur un site proposant de la pornographie infantile tout en sachant que de telles images s'y trouvent. Ainsi, ne doivent pas être incriminées les personnes qui entrent par inadvertance dans des sites proposant de la pornographie infantile. Le caractère intentionnel de l’infraction pourra notamment être déduit de son caractère répété ou du fait que les faits ont été commis par un service moyennant paiement.

Le rapport explique également le terme ‘sans droit’ et la définition de ‘pornographie’, ainsi que la possibilité de réserves.

Les parties sont tenues d’étendre leur compétence à leur territoire, aux navires battant leur pavillon et aux aéronefs immatriculés sur leur territoire, mais aussi d’appliquer une vaste forme du principe de la ‘personnalité active’, étant donné qu’elles sont obligées d’étendre leur compétence à leurs ressortissants et aux personnes ayant leur résidence habituelle sur leur territoire qui commettent les infractions établies dans la Convention, quel que soit le lieu où l’infraction est commise (Article 25(1)). Toutefois, des réserves sont admises concernant l’extension de cette compétence aux résidents habituels (Article 25(3)). Les parties doivent également ‘s’efforcer’ de prendre des mesures pour garantir une vaste forme de compétence de ‘personnalité passive’ à l’égard à la fois de leurs ressortissants et des personnes ayant leur résidence habituelle sur leur territoire (Article 25(2)). Les parties sont tenues de renoncer au principe de ‘double incrimination’ concernant la production de pornographie infantile (Article 25(4)) et les aspects de la participation à des spectacles pornographiques, et doivent renoncer à la condition du dépôt d’une plainte de la victime concernant les infractions commises, ou d’une dénonciation de l’Etat du lieu où les faits ont été commis, avant que la compétence basée sur la personnalité active puisse être établie (Article 25(6)). La Convention stipule une obligation de consultation quand plus d’une partie revendiquent leur compétence (Article 25(8)), ‘afin de déterminer la mieux à même d’exercer les poursuites’. Elle établit par ailleurs une règle ‘extrader ou poursuivre’ que les états doivent appliquer à leurs ressortissants (Article 25(7)).

La Convention fixe également des règles concernant la responsabilité des personnes morales, la reconnaissance des condamnations antérieures et les circonstances aggravantes, ainsi qu’un certain nombre de règles relatives aux enquêtes et au droit procédural. En particulier, elle stipule des règles détaillées concernant la protection des victimes, la mise en œuvre des poursuites, la prescription, les auditions d’enfants et les procédures judiciaires impliquant des enfants. Les états doivent enregistrer les données relatives à l’identité ainsi qu’au profil génétique (ADN) des personnes condamnées pour les infractions établies conformément à la Convention, et mettre ces informations à la disposition des autorités d’une autre partie.

Enfin, la Convention prévoit une clause de ‘déconnexion’ générale à l’égard des Etats membres de la CE/UE (Article 43(3)):

Les Parties qui sont membres de l’Union européenne appliquent, dans leurs relations mutuelles, les règles de la Communauté et de l’Union européenne dans la mesure où il existe des règles de la Communauté ou de l’Union européenne régissant le sujet particulier concerné et applicables au cas d’espèce, sans préjudice de l’objet et du but de la présente Convention et sans préjudice de son entière application à l’égard des autres Parties.

Cette clause est identique à la clause de déconnexion de la Convention sur la prévention du terrorisme. La Communauté et ses Etats membres ont fait la même déclaration que pour cette autre Convention (voir paragraphe 279 du rapport explicatif de la présente Convention) et le rapport de la présente Convention mentionne similairement que la Commission serait en mesure de fournir une clarification des compétences (voir paragraphe 280 du rapport explicatif). A nouveau, comme susmentionné, la CE n’a pas signé la Convention et la Commission n’a pas proposé que la Communauté la signe.

2. Mesures adoptées par la CE et l’UE

2.1 Droit matériel – Mesures du troisième pilier

2.1.1. Attaques visant les systèmes d’information

La première mesure du droit matériel de l’UE digne d’être mentionnée est la Décision-cadre relative aux attaques visant les systèmes d’information (JO 2005 L 69/67). La décision-cadre requiert des Etats qu’ils établissent trois infractions pénales : l’accès illicite, l’atteinte à l’intégrité d’un système et l’atteinte à l’intégrité des données. Ces trois infractions sont plus vastes que la Convention sur la cybercriminalité étant donné que la Convention ne s’applique qu’aux ‘systèmes informatiques’, définis comme étant ‘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’ (Article 1(a) de la Convention). Par contre, la Décision-cadre s’applique aux systèmes *d’information*, définis comme étant ‘tout dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, conformément à un programme, un traitement automatisé de données *informatiques*, ainsi que *les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance*’ (Article 1(a) de la Décision-cadre; les mots en italique diffèrent de ceux utilisés dans la Convention). La définition de ‘données informatiques’ est, toutefois, identique dans les deux mesures (Article 1(b) de la Décision-cadre et de la Convention).

Pour les trois infractions spécifiques, l’infraction d’‘accès illégal’ est décrite de manière identique, hormis la différence de portée des termes ‘systèmes informatiques’ et ‘systèmes d’information’ (Article 2(1) de la Décision-cadre; Article 2 de la Convention). Implicitement, la Décision-cadre n’exige pas l’érection en infraction pénale des cas ‘mineurs’ et permet expressément aux Etats membres de n’ériger en infraction pénale que les ‘infractions à une mesure de sécurité’ (Article 2(2)).

Ensuite, l'infraction d'atteinte à l'intégrité d'un système' est décrite de manière largement identique (Article 3 de la Décision-cadre; Article 5 de la Convention), à nouveau hormis la différence de portée. Cependant, la Décision-cadre fait référence à l'*interruption*, en plus du fait de provoquer une perturbation grave d'un système informatique. Elle fait également référence au fait de 'rendre inaccessibles' des données informatiques. A nouveau, il s'agit là d'une liberté implicite laissée aux Etats membres de ne pas ériger en infraction pénale les cas mineurs.

Troisièmement, l'infraction d'atteinte à l'intégrité des données' est identique, à nouveau hormis la différence de portée, et, à nouveau, avec l'addition du fait de 'rendre inaccessibles' des données informatiques comme spécifié dans la Décision-cadre (Article 4 de la Décision-cadre; Article 4 de la Convention). Alors que la Décision-cadre permet implicitement aux Etats membres de ne pas ériger en infraction pénale les cas mineurs, la Convention permet expressément aux parties de ne pas ériger en infraction pénale les cas sauf s'ils entraînent des 'dommages sérieux' (Article 4(2) de la Convention).

La Décision-cadre n'aborde pas les infractions étroitement corrélées d'interception illégale de données (Article 3 de la Convention) et d'abus de dispositifs (Article 6 de la Convention). De même, elle n'aborde pas les 'infractions informatiques' de falsification informatique et fraude informatique (Articles 7 et 8 de la Convention). Les deux mesures exigent des états qu'ils imposent une responsabilité pour les aides et complicités et tentatives, mais avec la possibilité de ne pas ériger en infraction pénale les tentatives d'accès illicite à des données (Article 5 de la Décision-cadre; Article 11 de la Convention).

En ce qui concerne la compétence, la Décision-cadre exige des Etats membres qu'ils établissent leur compétence pour les infractions qui ont été commises en tout ou en partie sur leur territoire, ou par l'un de leurs ressortissants (sans qualification), ou au profit d'une personne morale dont le siège est situé sur leur territoire (Article 10(1)). Toutefois, les Etats membres peuvent décider de renoncer à leur compétence, sauf pour la compétence territoriale (Article 10(5)). La Décision-cadre spécifie expressément que la compétence territoriale s'applique quand:

- (a) l'auteur de l'infraction l'a commise alors qu'il était physiquement présent sur son territoire, même si l'infraction ne vise pas un système d'information situé sur son territoire, ou
- (b) l'infraction vise un système d'information situé sur son territoire, même si l'auteur de l'infraction n'était pas physiquement présent sur ce territoire (Article 10(2)).

Par opposition, la Convention sur la cybercriminalité requiert des parties qu'elles établissent leur compétence à l'égard des infractions commises sur leur territoire, à bord de navires battant leur pavillon et à bord d'aéronefs immatriculés sur leur territoire, ainsi qu'aux actes commis par leurs ressortissants sous certaines conditions (Article 22 de la Convention). Cependant, les parties peuvent formuler des réserves à l'ensemble de ces obligations, à l'exception de la compétence territoriale. La position est donc très similaire dans les deux mesures, hormis pour la clarification de la compétence territoriale aux termes de la Décision-cadre.

La proposition de la Commission (COM (2002) 173) indique clairement que la Décision-cadre n'a pas abordé des questions relevant du droit communautaire, en particulier 'l'accès aux données à caractère personnel et à leur divulgation, à la

confidentialité des communications, à la sécurité du traitement des données à caractère personnel, aux signatures électroniques ou les violations des droits de propriété intellectuelle et elle n'affecte pas la directive 98/84/CE concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel'. Il n'y a aucune obligation en matière pénale à l'égard de ces mesures, mais une proposition relative à la propriété intellectuelle sera discutée plus loin.

La Commission a affirmé qu'à la lumière de la jurisprudence de la Cour de justice sur la portée des pouvoirs de la CE en matière de droit pénal, la Décision-cadre aurait dû être remplacée en tout ou en partie par un acte législatif de la Communauté (COM (2005) 583). Cependant, la Commission n'a encore présenté aucune proposition à cet effet. Elle a annoncé son intention de proposer des amendements à la Décision-cadre en 2009 concernant 'en particulier les 'botnets' et d'autres instruments utilisés pour lancer des attaques criminelles à grande échelle' (voir le programme de travail de la Commission pour 2009, COM (2008) 712).

2.1.2. Exploitation sexuelle des enfants et pédopornographie

L'UE a abordé le sujet des délits à caractère sexuel impliquant des enfants dans la Décision-cadre relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie (JO 2004 L 13/44). Cette mesure, postérieure à la Convention sur la cybercriminalité mais antérieure à la Convention du Conseil de l'Europe sur la protection des enfants, exige des Etats membres de l'UE qu'ils érigent en infraction pénale la pédopornographie (Article 3) et la prostitution infantine (Article 2). Cette dernière infraction ne peut être commise qu'hors ligne. Comme pour l'infraction de pédopornographie, les Etats membres sont obligés de punir la production, la distribution, la diffusion ou la transmission, le fait d'offrir ou de rendre disponible et l'acquisition ou la détention de pédopornographie (Article 3(1)). L'obligation s'applique indépendamment d'une éventuelle connexion à un système informatique. La Décision-cadre définit un 'enfant' comme étant toute personne âgée de moins de dix-huit ans (Article 1(a)) et stipule également une définition de 'pédopornographie' (Article 1(b)), qui s'applique aussi au matériel impliquant des adultes qui paraissent être des enfants (Article 1(a)(ii)), et aux 'images réalistes d'un enfant qui n'existe pas' (Article 1(a)(iii)).

Les Etats membres peuvent exclure de la responsabilité tous les cas où la personne réelle impliquée dans le matériel était en fait un adulte (Article 3(2)(a)). Ils peuvent également exclure de la responsabilité tous les cas de production ou de distribution, de diffusion ou de transmission, quand le matériel a été produit par des personnes ayant atteint la majorité sexuelle pour leur usage privé, à condition que 'même lorsque l'existence d'un consentement a été établi, il ne sera pas reconnu comme valable, si, par exemple, l'auteur de l'infraction a profité de son âge plus avancé, de sa maturité, de sa position, de son statut, de son expérience ou de l'état de dépendance dans lequel se trouvait la victime à son égard pour obtenir ce consentement' (Article 3(2)(b)). Enfin, ils peuvent exclure de la responsabilité tous les cas impliquant du matériel relatif à des enfants qui n'existent pas lorsque 'il est établi que le matériel pornographique est produit et détenu par le producteur uniquement pour son usage privé' dans la mesure où aucun matériel pédopornographique ou matériel concernant des adultes paraissant être des enfants n'a été utilisé aux fins de la production, et à condition qu'il n'y ait aucun risque de diffusion du matériel (Article 3(2)(c)).

Les Etats membres sont tenus d'ériger en infraction pénale l'instigation, l'aide et la complicité pour l'ensemble de ces infractions (Article 4(1)), ainsi que les tentatives de commettre ces infractions, à l'exception des tentatives de posséder, d'offrir ou de rendre disponible de la pédopornographie (Article 4(2)). Les Etats membres doivent stipuler la possibilité d'imposer une sanction d'au moins un à trois ans d'emprisonnement pour les infractions décrites dans la Décision-cadre, et une peine d'au moins cinq à dix ans en cas de circonstances 'aggravantes' (Article 5). Toutefois, ils peuvent imposer des sanctions non pénales en cas de pédopornographie 'virtuelle' (Article 5(4)).

Les Etats membres doivent établir leur compétence lorsque l'infraction a été commise, en tout ou en partie, sur leur territoire, lorsque l'auteur de l'infraction est l'un de leurs ressortissants ou lorsque l'infraction a été commise pour le compte d'une personne morale établie sur leur territoire (Article 8(1)), bien qu'un Etat membre puisse décider de ne pas appliquer les deux dernières obligations (Article 8(2)). Chaque État membre doit aussi veiller 'à ce que sa compétence couvre les cas dans lesquels une infraction ... a été commise au moyen d'un système informatique auquel l'accès a été obtenu à partir de son territoire, que ce système informatique se trouve ou non sur ce dernier' (Article 8(5)). Les Etats membres doivent en outre autoriser les poursuites pour au moins les infractions les plus graves après que la victime a atteint l'âge de la majorité (Article 8(6)).

Par rapport à la Convention sur la cybercriminalité, la Décision-cadre s'applique à tous les enfants de moins de 18 ans, sans possibilité d'abaisser la limite d'âge (cfr. Article 9(3) de la Convention). De même, la Décision-cadre n'est pas limitée à l'activité en ligne. La Décision-cadre concerne également la 'diffusion' (non mentionnée dans la Convention), le 'fait d'offrir' et l' 'acquisition' de pédopornographie et pas uniquement l' 'offre' et 'le fait de se procurer ou de procurer à autrui' ce type de matériel. La définition de 'pédopornographie' donnée dans la Décision-cadre suit celle de la Convention (Article 9(2)), avec quelques mots additionnels dans la première mesure pour définir plus amplement la notion de 'comportement sexuellement explicite'. La Décision-cadre ne permet pas de renoncer à ériger en infraction pénale le fait de se procurer (c'est-à-dire l'acquisition) ou de posséder de la pédopornographie (cf Article 9(4) de la Convention), et la possibilité de renoncer à ériger en infraction pénale le matériel relatif à des enfants 'virtuels' est limitée à un cas particulier. Par contre, la possibilité de renoncer à ériger en infraction le matériel relatif à des adultes paraissant être des enfants est intégralement retenue et il existe une ultérieure possibilité de renoncer à ériger en infraction pénale ce qui touche au matériel produit par des enfants ayant atteint l'âge de la maturité sexuelle pour leur usage privé.

La Décision-cadre oblige les Etats membres à ériger en infraction pénale l'aide, la complicité et l'incitation à commettre ces infractions ainsi que la tentative visant à commettre certaines infractions liées à la pédopornographie, à l'exception de la tentative de fournir, rendre disponible, acquérir ou posséder de la pédopornographie (Article 4). Cette mesure rejoint les dispositions de la Convention sur la cybercriminalité, hormis le fait que cette dernière ne s'applique pas à l'instigation et permet aux parties de ne pas ériger en infraction pénale les tentatives liées à n'importe quel aspect de la pédopornographie (Article 11 de la Convention).

La Décision-cadre stipule une obligation générale de compétence pour les actes commis par un ressortissant, tandis que la Convention sur la cybercriminalité n'établit qu'une obligation conditionnelle. Les deux mesures autorisent néanmoins les états à ne pas appliquer ces obligations. La Convention sur la cybercriminalité requiert l'application de la compétence aux navires et aéronefs d'un Etat membre, mais cette disposition n'a certainement dans la pratique qu'une pertinence limitée et les états peuvent, par ailleurs, renoncer à appliquer ces obligations. Contrairement à la Convention sur la cybercriminalité, la Décision-cadre stipule une clause très pertinente concernant la compétence lorsque l'infraction a été commise au moyen d'un système informatique auquel l'accès a été obtenu à partir du territoire. La Décision-cadre prévoit l'application expresse de la compétence aux actes commis en partie sur le territoire.

La comparaison de la Décision-cadre à la Convention des enfants fait apparaître l'absence d'infraction de 'solicitation' dans la Décision-cadre. Comme dans le cas de la pédopornographie, la Convention des enfants et la Décision-cadre s'appliquent toutes les deux aux activités en ligne et hors ligne. Les deux dispositions présentent également la même définition du terme 'enfant' (toute personne âgée de moins de 18 ans). On note également quelques différences mineures concernant la formulation des principales infractions (ex. : la 'diffusion' est mentionnée dans la Décision-cadre mais pas dans la Convention ; la Décision-cadre fait référence au 'fait d'offrir' et à 'l'acquisition' de pédopornographie plutôt qu'à 'l'offre' et au 'fait de se procurer ou de procurer à autrui'. La principale différence réside dans le fait que la Décision-cadre ne prévoit pas l'infraction d'accès en ligne. La Convention formule la même définition étendue que la Décision-cadre pour la 'pédopornographie' mais fait généralement référence à la représentation visuelle de l'enfant ('tout matériel représentant de manière visuelle un enfant ...'), plutôt qu'aux trois catégories (enfants réels, adultes paraissant être des enfants et enfants virtuels) stipulées dans la Convention sur la cybercriminalité et dans la Décision-cadre.

Si l'on compare les réserves possibles, il apparaît que la Convention des enfants stipule la possibilité inconditionnelle de ne pas criminaliser les images d'enfants 'virtuels' pour ce qui est de la production et de la possession, tandis que la Décision-cadre est plus conditionnelle, mais permet des réserves pour toutes les infractions. Les deux mesures prévoient la possibilité de réserves pour la possession et la production de matériel par des enfants ayant atteint la maturité sexuelle pour leur propre usage, mais la mesure de l'UE comporte une possibilité d'invalider le consentement. En ce qui concerne l'exception formulée pour les images d'adultes reprise dans la Décision-cadre, il n'est pas clair si la Convention s'applique aux images d'adultes paraissant être des enfants dans tous les cas de figure.

Pour les infractions virtuelles, la Convention des enfants (Article 24) ne s'applique toujours pas à l'instigation et oblige les parties à ériger en infraction pénale l'aide et la complicité et les tentatives de sollicitation et de pédopornographie, à l'exception de la possibilité de renoncer à criminaliser les tentatives visant à commettre l'infraction de sollicitation ainsi que certaines infractions liées à la pédopornographie. Les parties doivent au moins ériger en infraction pénale les tentatives visant à commettre les infractions de production ou de distribution et de transmission de pédopornographie. La Décision-cadre stipule donc une norme plus stricte concernant les infractions 'traditionnelles' liées à la pédopornographie (à savoir, en dehors de l'accès en ligne).

En ce qui concerne la compétence, la Convention des enfants va au-delà de la Décision-cadre en obligeant les parties à assurer inconditionnellement leur compétence pour les actes commis par leurs ressortissants (Article 25), tandis que la Décision-cadre permet aux Etats membres de déroger à cette obligation. Contrairement à la Décision-cadre, la Convention s'applique également aux actes commis par des résidents, même si elle stipule une possibilité de réserve sur ce point.

Le projet de rapport au PE concernant l'implémentation de la Décision-cadre (rapport Angelilli) recommande notamment ce qui suit:

- (a) Tous les Etats membres devraient signer et ratifier la Convention des enfants du Conseil de l'Europe;
- (b) Les Etats membres devraient améliorer leur législation vu les variations de l'âge de la majorité sexuelle;
- (c) les Etats membres devrait exclure explicitement l'exigence de double incrimination en vue d'établir leur compétence;
- (d) les États membres qui n'ont pas encore entièrement mis en œuvre la décision-cadre devraient être aidés à le faire dans les meilleurs délais;
- (e) le suivi de la mise en oeuvre de la décision-cadre devrait être amélioré;
- (f) la décision-cadre devrait être révisée pour relever le niveau de protection au moins au niveau proposé par la Convention des enfants et concentrer l'attention sur les agressions liées à Internet et à d'autres technologies de communication; et inclure les dispositions suivantes:
 - création de systèmes de gestion nationaux sur les délinquants sexuels, qui incluraient une évaluation des risques ainsi que des programmes d'intervention pour prévenir ou minimiser le risque de récurrence, et les thérapies proposées aux délinquants sexuels sur la base du volontariat;
 - criminalisation de la sollicitation d'enfants à des fins sexuelles - grooming – et utilisation d'une définition de cette pratique basée sur la [Convention des enfants];
 - criminalisation de la pratique d'activités sexuelles avec un enfant (d'un âge inférieur ou supérieur à celui de la majorité sexuelle en vertu du droit national) en faisant usage de la contrainte, de la force ou de menaces, en abusant d'une position reconnue de confiance, d'autorité ou d'influence sur un enfant, y compris au sein de la famille, en abusant de la situation particulièrement vulnérable de l'enfant, notamment en raison d'un handicap physique ou mental ou d'une situation de dépendance, ou en proposant de l'argent ou toute autre forme de rémunération ou de considération en échange d'activités sexuelles avec l'enfant;
 - criminalisation du mariage forcé imposé à un enfant;
 - criminalisation du fait d'assister en connaissance de cause à des spectacles pornographiques impliquant des enfants ou d'obliger des enfants à assister à des actes ou des abus sexuels;
 - criminalisation des forums de discussion pédophiles ou des forums pédophiles sur Internet;
 - autorisation pour les organes de contrôle nationaux d'exiger des fournisseurs Internet qu'ils bloquent l'accès des sites utilisés pour commettre des infractions, ou pour faire la publicité d'infractions pouvant être commises, infractions établies conformément à la décision-cadre;
 - révision de l'article 5, paragraphe 3, de la décision-cadre dont les dispositions sont limitées pour empêcher les délinquants sexuels ayant été condamnés d'approcher des

enfants à l'occasion d'activités professionnelles ou bénévoles impliquant des contacts réguliers avec des enfants, entre autres en envisageant une obligation, pour les États membres, de veiller à ce que les candidats à certains postes impliquant un travail auprès d'enfants soient soumis à un contrôle de leur casier judiciaire, y compris l'établissement de règles ou de lignes directrices précises à l'intention des employeurs sur leurs obligations à cet égard.

– facilitation de la coopération internationale par le recours aux instruments prévus par [la Convention des enfants];

– dispense, pour certains groupes professionnels particuliers, de l'obligation de confidentialité lorsqu'une personne entre en possession d'informations sur une infraction constatée conformément à la décision-cadre ou a de sérieuses raisons de croire qu'une telle infraction pourrait avoir été commise, dans les cas où l'information provient directement de la victime d'un abus sexuel;

– obligation pour les professionnels en contact avec des enfants de faire part des situations dans lesquelles ils ont toutes les raisons de soupçonner un abus;

– amélioration de l'identification des enfants victimes d'abus sexuels grâce à la formation du personnel régulièrement en contact avec eux;

– facilitation de la participation des enfants aux procédures pénales afin d'éviter tout traumatisme, en prévoyant des dispositions spécifiques concernant la manière dont sont recueillies les preuves auprès des enfants victimes au cours d'entretiens;

– interdiction de la publicité encourageant des activités susceptibles d'inciter à l'utilisation de services pouvant conduire à commettre des infractions constatées conformément à la décision-cadre;

– criminalisation de toute démarche visant à induire, aider, inciter et tenter de commettre toutes les formes d'infractions constatées conformément à la décision-cadre;

– extension de la liste des circonstances aggravantes lors de la détermination des sanctions correspondant aux infractions constatées conformément à la décision-cadre en intégrant la liste des circonstances aggravantes établie dans la Convention [des enfants];

– classification au rang des circonstances aggravantes de l'exploitation, par le délinquant, de sa position dominante (au sein de la famille, dans le milieu de l'éducation, dans les relations professionnelles, en cas d'immigration illégale, etc.);

(g) créer une base de données européenne commune recueillant des images d'exploitation d'enfants ; et

(h) mettre en place un programme d'action qui aurait pour objectif d'offrir aux enfants identifiés comme étant victimes d'abus sexuels sur ces images une protection et un soutien appropriés;

La Commission a annoncé son intention de proposer des amendements à la Décision-cadre en 2009. Cette proposition 'devrait relever le niveau de protection des enfants garanti actuellement ... la lutte contre l'exploitation sexuelle des enfants et la pédopornographie. Il est nécessaire de tenir compte de nouveaux phénomènes en matière de criminalité et d'intégrer de nouvelles dispositions, et d'aligner ainsi la législation de l'UE sur les normes internationales les plus élevées' (voir programme de travail de la Commission pour 2009, COM (2008) 712).

2.1.3 *Terrorisme*

La Décision-cadre de l'UE préexistante en la matière, qui oblige les Etats membres à amender la définition du terrorisme dans leur droit pénal (JO 2002 L 164/3), a été amendée en novembre 2008 à la lumière de la Convention susmentionnée du Conseil de l'Europe de 2005 (JO 2008 L 330/21, les Etats membres doivent implémenter la nouvelle mesure pour le 9 décembre 2010). La Décision-cadre amendée ajoute trois nouvelles définitions d'infractions à la Décision-cadre initiale : la 'provocation publique à commettre une infraction terroriste', le 'recrutement pour le terrorisme' et l' 'entraînement pour le terrorisme' (Article 3(1) amendé de la Décision-cadre). Les Etats membres sont tenus de garantir que ces actes seront considérés comme des 'infractions liées aux activités terroristes' (Article 3(2) amendé). La Décision-cadre spécifie également que pour que ces actes soient punissables, 'il n'est pas nécessaire qu'une infraction terroriste soit effectivement commise' (nouvel Article 3(3)). Ce dernier point correspond à l'Article 8 de la Convention du Conseil de l'Europe.

En outre, la Décision-cadre de 2002 a été amendée pour spécifier l'obligation d'ériger en infraction pénale l'aide et la complicité à commettre ces infractions (Article 4(1) amendé). Toutefois, la Décision-cadre révisée n'exige pas des Etats membres qu'ils punissent l'incitation et la tentative (Article 4(2) amendé et nouvel Article 4(3)). La Décision-cadre revue spécifie uniquement que les Etats membres *peuvent* rendre punissable le fait de tenter de commettre une infraction relative à l'entraînement pour le terrorisme et au recrutement pour le terrorisme (nouvel Article 4(4)).

Par rapport à la Convention du Conseil de l'Europe, l'obligation imposée par l'UE de punir l'aide et la complicité pourrait en quelque sorte être considérée comme l'équivalent de l'obligation stipulée par le Conseil de l'Europe de punir la participation en tant que complice. Toutefois, la Décision-cadre de l'UE ne rejoint pas l'obligation prévue par le Conseil de l'Europe de punir l'organisation de la commission de ces infractions ou le fait de donner l'ordre à d'autres personnes de commettre ces infractions, la contribution à la commission d'une ou plusieurs de ces infractions par un groupe, ou la tentative de commettre deux de ces trois infractions. Ceci s'explique par le fait que les obligations imposées par l'UE concernant les groupes terroristes (Article 2 de la Décision-cadre) ne s'appliquent qu'aux 'infractions terroristes' et non aux infractions liées au terrorisme. Dans tous les cas, certaines différences sont à noter entre la conception du 'groupe terroriste' selon l'UE et selon le Conseil de l'Europe (il convient de comparer l'Article 2(1) de la Décision-cadre à l'Article 9(1)(c) de la Convention). La Convention ne définit en fait pas la notion de 'groupe terroriste' en tant que tel. Tandis que la Convention du Conseil de l'Europe fait référence à l'organisation de la commission d'une infraction spécifiée dans la Convention ou le fait de donner l'ordre à d'autres personnes de la commettre (Article 9(1)(b)), la Décision-cadre évoque le fait de 'diriger un groupe terroriste' (Article 2(2)(a)).

Par ailleurs, les mesures de l'UE et du Conseil de l'Europe se distinguent concernant les infractions 'terroristes' sous-jacentes auxquelles les nouvelles infractions sont liées. Comme susmentionné, la Convention du Conseil de l'Europe définit une 'infraction terroriste' comme l'une quelconque des infractions interdites par l'un des dix traités énumérés dans l'Annexe de la Convention (Article 1(1) de la Convention). La Décision-cadre définit pour sa part comme étant des infractions terroristes huit infractions spécifiques (ou la menace de les commettre) qui, eu égard à leur nature et leur contexte, sont commises dans un but spécifié (Article 1(1) de la Décision-cadre). Il y a certes un large degré de similitudes entre les infractions couvertes par les deux

mesures, mais le chevauchement n'est pas parfait (pour une comparaison des mesures de lutte contre le terrorisme des NU et la Décision-cadre originale, voir S. Peers, 'EU Responses to Terrorism', 52 ICLQ (2003) 227).

L'infraction clé consistant à recruter pour le terrorisme diffère également, étant donné que la Convention exige des Etats qu'ils punissent 'le fait de solliciter une autre personne pour commettre ou participer à la commission d'une infraction terroriste, ou pour se joindre à une association ou à un groupe afin de contribuer à la commission d'une ou plusieurs infractions terroristes par l'association ou le groupe' (Article 5(1)), tandis que la Décision-cadre révisée requiert des Etats membres qu'ils punissent le fait de 'solliciter une autre personne pour commettre ou participer à la commission d'une infraction terroriste comme définie dans la Décision-cadre ou la direction ou la participation à un groupe terroriste' comme défini dans la Décision-cadre (nouvel Article 3(1)(b)). L'UE n'impose pas la criminalisation de la sollicitation à participer *per se* et elle définit plus précisément mais plus largement le concept de participation à un groupe terroriste (voir Article 2(2)(b) de la Décision-cadre, qui *inter alia* fait référence aux 'activités criminelles' et pas uniquement aux 'infractions terroristes').

Les deux mesures se distinguent également au niveau de la compétence. Comme susmentionné, la Convention (Article 14(1)) exige des Etats membres qu'ils établissent leur compétence sur leur territoire et sur une notion étendue du territoire (navires battant leur pavillon et aéronefs immatriculés sur leur territoire) et par personnalité active (actes commis par des ressortissants). La Décision-cadre quant à elle requiert aussi des Etats membres qu'ils établissent leur compétence pour les actes commis par leurs 'résidents', quand 'l'infraction a été commise pour le compte d'une personne morale établie sur son territoire' et quand l'infraction a été commise contre ses institutions ou sa population, ou contre une institution de l'Union européenne ou d'un organisme créé conformément au traité instituant la Communauté européenne ou au traité sur l'Union européenne, et ayant son siège dans l'Etat membre concerné' (Article 9(1) de la Décision-cadre).

Il convient également de noter que, dans le cas de la Convention, la compétence territoriale s'appliquera au lieu où l'infraction *annexe* a été commise, qui peut différer du lieu où l'infraction *principale* est commise (voir rapport explicatif de la Convention, paragraphe 34 : '...le lieu où une telle infraction est commise n'est pas non plus pertinent pour établir que l'une quelconque des infractions ...' a été commise. Voir également les paragraphes 79, 126 et 127 du rapport). On peut dire que la même règle vaut pour la Décision-cadre. Ainsi, une 'provocation publique' en France visant à commettre un acte 'terroriste' en Irak serait couverte par ces mesures. Dans la situation inverse (une 'provocation publique' en Irak à commettre un acte 'terroriste' en France), les Etats membres devront prendre leur compétence aux termes de la Décision-cadre (étant donné que cet acte pourrait certainement être qualifié d'acte 'contre les institutions ou la population de l'Etat membre', en vertu de l'Article 9(1)(e)), mais pas nécessairement aux termes de la Convention, pour laquelle la 'personnalité passive' est purement optionnelle en matière de compétence (Article 14(2)(a) de la Convention).

En ce qui concerne les sauvegardes prévues dans les deux mesures, la Convention spécifie que les obligations des états doivent être 'réalisées en respectant les obligations relatives aux droits de l'homme lui incombant, notamment la liberté d'expression, la liberté d'association et la liberté de religion, telles qu'établies dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, dans le Pacte international relatif aux droits civils et politiques, et d'autres obligations

découlant du droit international, lorsqu'ils lui sont applicables' (Article 12(1)). Elle spécifie également que les obligations de criminalisation doivent 'en outre être subordonnées au principe de proportionnalité eu égard aux buts légitimes poursuivis et à leur nécessité dans une société démocratique, et devraient exclure toute forme d'arbitraire, de traitement discriminatoire ou raciste' (Article 12(2)).

Pour sa part, la Décision-cadre amendée déclare qu'elle 'n'a pas pour effet d'obliger les Etats membres à prendre des mesures contraires aux principes fondamentaux relatifs à la liberté d'expression, en particulier à la liberté de la presse et à la liberté d'expression dans d'autres médias, tels qu'ils résultent des traditions constitutionnelles ou des règles régissant les droits et responsabilités de la presse ou d'autres médias ainsi que les garanties de procédure en la matière, lorsque ces règles portent sur la détermination ou la limitation de la responsabilité' (Article 2). Le préambule à la mesure amendée indique également que:

(13) L'Union observe les principes reconnus par l'article 6, paragraphe 2, du traité UE et réaffirmés par la Charte des droits fondamentaux de l'Union européenne, notamment ses chapitres II et VI. Rien dans la présente décision-cadre ne peut être interprété comme visant à réduire ou à entraver des libertés ou des droits fondamentaux tels que la liberté d'expression, de réunion ou d'association, le droit au respect de la vie privée et familiale, y compris le droit au respect de la confidentialité de la correspondance.

(14) La provocation publique à commettre des infractions terroristes, le recrutement et l'entraînement pour le terrorisme sont des infractions intentionnelles. Rien dans la présente décision-cadre ne peut dès lors être interprété comme visant à réduire ou à entraver la diffusion de données à des fins scientifiques, académiques ou d'information. L'expression d'opinions radicales, polémiques ou controversées dans le cadre d'un débat public sur des questions politiquement sensibles, y compris le terrorisme, ne relève pas du champ d'application de la présente décision-cadre ni, en particulier, de la définition de la provocation publique à commettre des infractions terroristes.

(15) La mise en oeuvre de l'incrimination au titre de la présente décision-cadre devrait être proportionnelle à la nature et aux circonstances de l'infraction, eu égard aux buts légitimes poursuivis et à leur nécessité dans une société démocratique, et devrait exclure toute forme d'arbitraire ou de traitement discriminatoire,

La Décision-cadre d'origine spécifie qu'elle 'ne saurait avoir pour effet de modifier l'obligation de respecter les droits fondamentaux et les principes juridiques fondamentaux tels qu'ils sont consacrés par l'article 6 du traité sur l'Union européenne' (Article 1(2)). Le préambule de la version originale de la Décision-cadre précise que:

(10) La présente décision-cadre respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne des droits de l'homme et des libertés fondamentales, et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes du droit communautaire. L'Union observe les principes reconnus par l'article 6, paragraphe 2, du traité sur l'Union européenne et reflétés par la charte des droits fondamentaux de l'Union européenne, notamment son chapitre VI. Rien dans la présente décision-

cadre ne peut être interprété comme visant à réduire ou à entraver des droits ou libertés fondamentales telles que le droit de grève, la liberté de réunion, d'association ou d'expression, y compris le droit de fonder avec d'autres des syndicats et de s'affilier à des syndicats pour la défense de ses intérêts, et le droit de manifester qui s'y rattache.

Ces sauvegardes s'appliquent également à la mesure amendée.

2.1.4. Racisme et xénophobie

Le Protocole à la Convention sur la cybercriminalité relatif au racisme et à la xénophobie peut être comparé à la récente Décision-cadre de l'UE sur le même sujet (JO 2008 L 328/55), adoptée en novembre 2008. Le Protocole et la Décision-cadre ont chacun leur propre définition des infractions clés sous-jacentes. Pour le Protocole, '*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' (Article 2(1) du Protocole). Comme susmentionné, les parties doivent criminaliser quatre actes spécifiques: la diffusion de matériel de ce type par le biais de systèmes informatiques; la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, envers un groupe défini par la race ou autres ou par la religion; une insulte contre une personne ou un groupe pour des motifs raciaux, religieux et autres par le biais d'un système informatique; et la négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité comme défini dans le Protocole par le biais d'un système informatique. Les parties doivent également punir l'aide ou la complicité en vue de commettre de telles infractions.

Comme indiqué plus haut, un certain nombre de réserves sont admises. En ce qui concerne la diffusion de matériel raciste ou xénophobe, les parties peuvent soit exonérer la responsabilité pénale dans la mesure où les principes établis dans son ordre juridique interne concernant la liberté d'expression l'exigent (Article 3(3)), ou, alternativement, ne pas imposer de responsabilité pénale pour le matériel qui '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' (Article 3(2); mise en évidence ajoutée). En ce qui concerne l'obligation de criminaliser les insultes racistes, une partie peut décider de ne pas appliquer du tout cette disposition (Article 5(2)(b)), ou 'exiger que l'infraction ... ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule' (Article 5(2)(a)). Enfin, pour ce qui est de la négation de génocide et autres, une partie peut soit décider de ne pas appliquer du tout cette disposition (Article 6(2)(b)), soit 'prévoir que la négation ou la minimisation grossière ... 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' (Article 6(2)(a)). Par contre, aucune réserve n'est autorisée concernant l'obligation de criminaliser les menaces racistes commises par le biais d'un système informatique.

Parmi les Etats membres qui ont ratifié le Protocole, le Danemark a invoqué les trois réserves et a ainsi annoncé qu'il peut s'abstenir en tout ou en partie d'établir les infractions stipulées aux Articles 3, 5 et 6 du Protocole, tandis que la Lituanie a invoqué la réserve autorisée à l'Article 6(2)(a). La France a émis une déclaration stipulant son interprétation de l'Article 6.

Dans le cas de la Décision-cadre, les Etats membres doivent d'abord considérer comme une infraction pénale 'l'incitation publique à la violence ou à la haine visant un groupe de personnes ou un membre d'un tel groupe, défini par référence à la race, la couleur, la religion, l'ascendance, l'origine nationale ou ethnique' (Article 1(1)(a)), ou 'la commission [d'un tel acte] par diffusion ou distribution publique d'écrits, d'images ou d'autres supports' (Article 1(1)(b)). Pour ces infractions, les Etats membres ont la possibilité de 'choisir de ne punir que le comportement qui est soit exercé d'une manière qui risque de troubler l'ordre public, soit menaçant, injurieux ou insultant' (Article 1(2)). La Décision-cadre indique également que la référence à la 'religion' dans la définition des infractions 'est censée couvrir au moins le comportement qui constitue un prétexte pour mener des actions contre un groupe de personnes ou un membre de ce groupe défini par référence à la race, la couleur, l'ascendance ou l'origine nationale ou ethnique' (Article 1(3)). Cette disposition est relativement similaire à la référence à la religion incluse dans le Protocole sur la cybercriminalité.

Contrairement au Protocole, la *préconisation* et l'*encouragement* à la violence ou la haine ne sont pas couverts par la Décision-cadre, qui ne fait par ailleurs aucune référence à la discrimination. Dès lors, la réserve possible concernant la discrimination stipulée dans le Protocole est superflue pour ce qui est de la Décision-cadre (mais voir la discussion des mesures de la CE ci-dessous). La Décision-cadre opère la distinction entre l'incitation publique d'une part et la diffusion de l'autre, tandis que le Protocole n'aborde que la diffusion. La Décision-cadre ne couvre pour sa part pas expressément les insultes ou les menaces. Cependant, dans certains cas, l'incitation publique à la haine ou à la violence reprise dans la Décision-cadre couvre également la menace ou l'insulte telles que définies par le Protocole. De toute évidence, la portée du Protocole est limitée aux activités en ligne, alors que ce n'est pas le cas de la Décision-cadre.

En ce qui concerne la 'négation de l'Holocauste' et les infractions similaires, le Protocole exige des parties qu'elles érigent en infraction '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' reconnu par les parties. Comme susmentionné, les parties peuvent, à nouveau, décider de ne pas appliquer cette disposition du tout ou exiger que l'action 'soit commise avec l'intention d'inciter à la haine, à la discrimination ou à la violence' pour des raisons de race, etc.

La Décision-cadre implique 'l'apologie, la négation ou la banalisation grossière' de l'Holocauste ou de crimes similaires, 'visant un groupe de personnes ou un membre d'un tel groupe défini par référence à la race, la couleur, la religion, l'ascendance ou l'origine nationale ou ethnique lorsque le comportement est exercé d'une manière qui risque d'inciter à la violence ou à la haine à l'égard d'un groupe de personnes ou d'un membre d'un tel groupe' (Article 1(1)(c) et (d)). La Décision-cadre autorise les Etats

membres à déclarer qu'ils ne puniront la négation ou la banalisation grossière que si ces crimes 'ont été établis par une décision définitive rendue par une juridiction nationale de cet État membre et/ou une juridiction internationale ou par une décision définitive rendue par une juridiction internationale seulement' (Article 1(4)). Comme pour les autres infractions couvertes par la Décision-cadre, les États membres peuvent 'choisir de ne punir que le comportement qui est soit exercé d'une manière qui risque de troubler l'ordre public, soit menaçant, injurieux ou insultant' (Article 1(2)).

Comparé au Protocole, la Décision-cadre ne permet pas de renoncer complètement à l'application de cette disposition. Elle s'applique aussi bien aux activités en ligne qu'hors ligne, tandis que le Protocole ne concerne que l'activité en ligne. En outre, la portée des négations est plus vaste que les simples cas dans lesquels des crimes de guerre et autres ont été établis par des cours internationales, même si les États membres ont la possibilité de limiter son application à ces seuls cas. A nouveau, la Décision-cadre ne s'applique pas à la discrimination, mais uniquement à la haine et à la violence. Elle concerne par ailleurs les mesures susceptibles de susciter une réaction, alors que le Protocole s'applique aux mesures visant à susciter une réaction. Cette différence est toutefois restreinte par la possibilité de limiter l'application de la Décision-cadre aux comportements qui menacent l'ordre public, ou qui sont insultants, etc.

Comme le Protocole, la Décision-cadre s'applique à l'aide et à la complicité en vue de commettre toutes les infractions pertinentes (Article 2(2)). Contrairement au Protocole, elle couvre également l'instigation à l'infraction de 'négation de l'Holocauste' (Article 2(1)). Les deux mesures spécifient, en des termes légèrement différents, qu'elles n'exigent pas des États qu'ils agissent contre les principes fondamentaux relatifs à la liberté d'expression, mais la mesure de l'UE ne se réfère qu'à l'exonération de la responsabilité des médias concernant toutes les infractions stipulées (Article 7(2)), alors que le Protocole évoque une exemption de la diffusion de matériel raciste et xénophobe en ce qui concerne la liberté d'expression plus généralement.

Le Protocole applique les mêmes règles de compétence que la Convention sur la cybercriminalité (Article 8(1) du Protocole), avec la possibilité pour les parties de formuler les mêmes réserves pour les règles de compétence (voir Article 12(2) du Protocole). Cela signifie que les États doivent établir leur compétence sur les actes commis sur leur territoire, à bord de navire battant leur pavillon ou d'aéronefs immatriculés sur leur territoire, et par leurs ressortissants, dans certaines conditions (Article 22 de la Convention). Toutefois, les parties peuvent formuler des réserves concernant toutes ces obligations, à l'exception de la compétence territoriale. Pour la Décision-cadre, les États membres doivent établir leur compétence lorsque l'acte a été commis en totalité ou en partie sur leur territoire, a été commis par un de leurs ressortissants (sans qualification), ou a été commis pour le compte d'une personne morale ayant son siège social sur leur territoire (Article 9(1)). Cependant, les États membres peuvent décider de ne pas appliquer toutes leurs compétences, à l'exception de la compétence territoriale (Article 9(3)). La situation est donc la même que dans le Protocole, hormis le fait que la Décision-cadre spécifie expressément que la compétence territoriale s'applique quand:

- a) son auteur commet l'acte alors qu'il est physiquement présent sur son territoire, que l'acte fasse ou non intervenir du matériel hébergé sur un système d'information situé sur son territoire; ou

b) il fait intervenir du matériel hébergé sur un système d'information situé sur son territoire, que son auteur le commette ou non alors qu'il est physiquement présent sur son territoire (Article 9(2)).

2.2 Droit de la CE – Mesures du premier pilier

Le droit communautaire n'a pas établi d'infractions pénales relatives à la cybercriminalité. A ce jour, la jurisprudence de la Cour de justice n'a clairement établi la compétence de la CE en matière de droit pénal que pour l'environnement (Cas C-176/03 et C-440/05). A l'heure actuelle, la question de savoir si la Communauté possède une compétence pénale dans un quelconque autre domaine demeure ouverte.

2.2.1 *Droits de propriété intellectuelle*

Dans le domaine spécifique des droits de propriété intellectuelle, la Commission a proposé une Directive qui établirait des obligations de droit pénal concernant 'toute atteinte intentionnelle à un droit de propriété intellectuelle dès lors que celle-ci est commise à une échelle commerciale' (Article 3, COM (2006) 168). Cette directive s'appliquerait 'à toute atteinte aux droits de propriété intellectuelle prévue par la législation communautaire et/ou la législation nationale des Etats membres' (Article 1 de la proposition). La proposition n'est actuellement pas en discussion au Conseil, même si le PE a voté son avis en première lecture.

La proposition de la Commission peut être comparée à l'obligation stipulée dans la Convention sur la cybercriminalité d'établir des infractions relatives à 'l'atteinte à la propriété intellectuelle', telle qu'établie dans le droit national et dans des conventions internationales spécifiées, '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' (Article 10(1)), et aux 'droits connexes' aux mêmes conditions (Article 10(2)). Une partie peut déroger à ces obligations dans des 'circonstances bien délimitées, 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 vertu des traités spécifiés (Article 10(3)).

2.2.2 *Autres mesures*

La question de la discrimination raciale (distincte de la violence), qui fait l'objet de la Directive 2000/43, et la protection des données, qui fait l'objet de la Directive 95/46 et, pour le secteur des télécommunications, de la Directive 2002/58 (JO 2002 L 201/37) sont d'autres domaines du droit communautaire liés à la cybercriminalité. Ces actes n'établissent pas d'obligations en droit pénal. Si la Communauté avait des pouvoirs en matière pénale dans des domaines autres que l'environnement lorsque nécessaire pour garantir l'application effective des règles qu'elle établit (par analogie aux jugements susmentionnés relatifs au droit environnemental), elle serait compétente pour fixer des punitions de droit pénal relatives à la discrimination raciale (pour les aspects parallèles à ceux du Protocole à la Convention sur la cybercriminalité) et en matière de droit de protection des données. Ces dernières obligations pourraient être rapprochées de l'infraction d'atteinte à l'intégrité des

données stipulée dans la Convention sur la cybercriminalité (Article 4 de la Convention), même s'il convient de noter que l'obligation de la Convention n'est pas limitée aux cas impliquant des données à *caractère personnel* et que la Directive ne s'applique pas uniquement aux systèmes informatiques mais aux réseaux de télécommunications plus globalement. Une disposition spécifique de la Directive sur l'e-privacy stipule la confidentialité des communications (Article 5), mais la question se pose de savoir s'il doit y avoir des obligations de droit pénal en matière de sécurité des données (Article 4) et de communications non sollicitées (Article 13(1) et (4)), au moins dans les cas les plus flagrants des 'spams'. Des obligations de droit pénal pourraient aussi être liées aux dispositions équivalentes de la Directive plus générale sur la protection des données.

Il y a également un certain degré de chevauchement entre la législation de la CE interdisant les dispositifs permettant l'accès illicite à divers services de radiodiffusion ou informatiques (Directive 98/84, JO 1998 L 320/54) et la criminalisation de l'abus de dispositifs dans la Convention sur la cybercriminalité (Article 6).

2.3 Droit de procédure

En ce qui concerne les dispositions du droit procédural stipulées dans la Convention du Conseil de l'Europe sur la cybercriminalité, la Directive de la CE sur la conservation des données (Directive 2006/24, JO 2006 L 105/54) est de toute évidence pertinente. Par rapport à l'Article 20 de la Convention, la Directive donne une définition différente de la notion de 'données relatives au trafic' (Article 2(b) de la Directive; Article 1(d) de la Convention). La Directive s'applique aussi aux données de localisation. Il n'y a cependant qu'un chevauchement limité entre les deux dispositions, si même il y en a un, étant donné que la Convention couvre uniquement l'interception 'en temps réel', tandis que la Directive porte aussi sur la conservation pour un éventuel usage ultérieur. Il y a également un certain degré de chevauchement quand la Convention s'applique à la conservation des données informatiques stockées, qui peuvent inclure les données relatives au trafic (Articles 16 et 17 de la Convention).

En ce qui concerne les mesures transfrontalières, il peut y avoir un degré de chevauchement entre les dispositions de la Convention sur la conservation rapide de données informatiques stockées (Article 29 de la Convention) et la Décision-cadre de l'UE relative à l'exécution dans l'Union européenne des décisions de gel de biens ou d'éléments de preuve (JO 2003 L 196/45).

2.4 Autres mesures de la CE et de l'UE

La Communauté a récemment adopté la version la plus récente du programme 'Safer Internet' (JO 2008 L 348/118), qui a pour but de 'protéger les enfants lors de l'utilisation de l'Internet et d'autres technologies de communication'. Citons également la Recommandation de la CE sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne (JO 2006 L 378/72). Cette dernière mesure suggère en particulier de '(a) adopter un label de qualité des fournisseurs de service qui permette à tout utilisateur de déterminer facilement si un fournisseur adhère ou non à un code de bonne conduite', et '(b) instaurer des moyens appropriés pour signaler des activités illégales et/ou suspectes sur Internet' (point 4),

et fait référence à des systèmes de filtres, à l'étiquetage des contenus et à l'indication de l'âge (point 5).

En ce qui concerne les aspects opérationnels de la cybercriminalité, notons la Recommandation du Conseil concernant les points de contact assurant un service vingt-quatre heures sur vingt-quatre pour lutter contre la criminalité liée à la haute technologie (JO 2001 C 187/5), qui implémente l'une des dispositions de la Convention sur la cybercriminalité (Article 35). La cybercriminalité relève à la fois des attributions d'Europol et d'Eurojust. Le Conseil JAI d'octobre 2008 a adopté des conclusions sur la question de la cybercriminalité, demandant aux Etats membres de mettre en place des plates-formes d'alerte 'afin de centraliser les alertes sur les infractions commises sur Internet', et a également recommandé la mise en œuvre d'une plate-forme de l'UE hébergée par Europol.

La Commission a suggéré l'organisation d'un réseau européen sur la cybercriminalité (Communication en matière de cybercriminalité, COM (2007) 267). Ce réseau serait comparable aux réseaux existants concernant d'autres infractions (cf. le réseau de lutte contre la corruption, JO 2008 L 301/38 et la décision établissant le réseau de recouvrement des avoirs, JO 2007 L 332/103).

Il convient de rappeler que les mesures établies par le droit pénal européen en matière de reconnaissance mutuelle abolissent la double incrimination concernant les 'infractions informatiques', même si diverses mesures stipulent des exceptions, et la plupart sont subordonnées à la prévision d'une peine d'au moins trois ans dans la loi de l'état émetteur. On note également diverses exceptions à l'obligation de reconnaître les décisions des autres Etats membres, en particulier l'exception de territorialité qui peut être particulièrement pertinente dans le cas de la cybercriminalité.

Les mesures adoptées pertinentes sont les suivantes:

- 1) Décision-cadre relative au mandat d'arrêt européen (JO 2002 L 190/1), Article 2;
- 2) Décision-cadre relative aux décisions de gel (JO 2003 L 196/45), Article 3;
- 3) Décision-cadre concernant les sanctions pécuniaires (JO 2005 L 76/16), Article 5; il n'y pas de peine minimum et la double incrimination est abolie pour l'atteinte aux droits de propriété intellectuelle' et pour les infractions couvertes par les obligations d'exécution du droit de la CE ou de l'UE;
- 4) Décision-cadre relative aux décisions de confiscation (JO 2006 L 328/59), Article 6;
- 5) Décision-cadre concernant la probation et autres (JO 2008 L 337/102), Article 10; Les Etats membres ont la possibilité de maintenir la double incrimination (Article 10(4));
- 6) Décision-cadre sur le transfert de prisonniers (JO 2008 L 327/27), Article 7(4); Les Etats membres ont la possibilité de maintenir la double incrimination (Article 7(4)); et
- 7) Décision-cadre relative au mandat européen d'obtention de preuves (JO 2008 L 350/72), Article 13; L'Allemagne n'abolira la double incrimination que dans la mesure où les infractions relèvent de la portée de la Décision-cadre sur les attaques contre les systèmes d'information, ou des infractions clés concernant

le fonctionnement des systèmes informatiques stipulées dans la Convention sur la cybercriminalité (Article 23(4) et déclaration).

Il convient également de rappeler que les infractions relatives à la cybercriminalité relèvent de la portée des règles Schengen *ne bis in idem* (Articles 54-58 de la Convention de Schengen). Ces règles sont particulièrement susceptibles d'être applicables à la lumière de la nature transfrontalière des infractions de cybercriminalité. En outre, la règle *ne bis in idem* constitue une exception obligatoire ou optionnelle à l'application des diverses mesures de reconnaissance mutuelle en droit pénal de l'UE.

Enfin, la présidence tchèque du Conseil prévoit de proposer très prochainement une décision-cadre sur la question de la prévention et du règlement des conflits de compétence. A nouveau, eu égard à la nature transfrontalière de nombreuses infractions de cybercriminalité, cette proposition pourrait être particulièrement pertinente dans ce domaine.

Vu les complications qui découlent d'un chevauchement des compétences dans ce domaine, l'UE pourrait envisager de définir ultérieurement de quelle manière le principe de la compétence territoriale s'applique aux infractions informatiques en particulier.

IV. CONCLUSIONS

La présente étude a suggéré que les points suivants soient inscrits parmi les priorités de l'action de l'Union européenne dans le domaine des droits fondamentaux sur Internet et de la lutte contre la cybercriminalité:

- a) l'adoption d'une Charte des droits de l'Internet non contraignante;
- b) l'alignement éventuel du droit pénal matériel de l'UE sur les dispositions des mesures pertinentes du Conseil de l'Europe, en particulier concernant les infractions liées au droit à la protection des données (spécifiquement, l'interception des données/la confidentialité de la communication, la sécurité des données et les 'spams'), la fraude et la falsification en ligne (par exemple le 'phishing'), la pédopornographie et la sollicitation en ligne d'enfants à des fins d'abus sexuel;
- c) l'adoption d'une mesure établissant un réseau opérationnel chargé des questions de cybercriminalité ; et
- d) la clarification des questions de compétence territoriale concernant les infractions de cybercriminalité.

ANNEXE

Charte des droits de l'Internet

Dans le contexte de l'Internet, les droits suivants doivent être spécifiquement respectés, observés et promus:

Article 1

Dignité humaine

La dignité humaine est inviolable. Elle doit être respectée et protégée.

Article 2

Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 3

Protection des données à caractère personnel

Toute personne a droit à la protection des données à caractère personnel la concernant.

Article 4

Liberté d'expression et d'information

1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés.

Article 5

Liberté des arts et des sciences

Les arts et la recherche scientifique sont libres. La liberté académique est respectée.

Article 6

Droit de propriété

La propriété intellectuelle est protégée.

Article 7

Non-discrimination

1. Est interdite, toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle.
2. Dans le domaine d'application des Traités et sans préjudice des dispositions particulières desdits traités, toute discrimination fondée sur la nationalité est interdite.

Article 8

Diversité culturelle, religieuse et linguistique

L'Union respecte la diversité culturelle, religieuse et linguistique.

Article 9

Egalité entre hommes et femmes

L'égalité entre les hommes et les femmes doit être assurée dans tous les domaines.

Article 10

Droits de l'enfant

1. Les enfants ont droit à la protection et aux soins nécessaires à leur bien-être. Ils peuvent exprimer leur opinion librement. Celle-ci est prise en considération pour les sujets qui les concernent, en fonction de leur âge et de leur maturité.
2. Dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale.

Article 11

Droits des personnes âgées

L'Union reconnaît et respecte le droit des personnes âgées à mener une vie digne et indépendante et à participer à la vie sociale et culturelle.

Article 12

Intégration des personnes handicapées

L'Union reconnaît et respecte le droit des personnes handicapées à bénéficier de mesures visant à assurer leur autonomie, leur intégration sociale et professionnelle et leur participation à la vie de la communauté.

Article 13

Protection des consommateurs

Un niveau élevé de protection des consommateurs est assuré concernant l'Internet.

Article 14

Dispositions générales

1. Le contenu des présents droits, y compris leur champ d'application, leur portée et leur interprétation (et, notamment, toute dérogation et limitation de ces droits), le niveau de protection assuré par ces droits et l'interdiction d'abus de ces droits, sont régis par les règles relatives à la protection des droits de l'homme garanties par les constitutions des Etats membres, par les traités internationaux sur les droits de l'homme dont la Convention européenne des droits de l'homme, les principes généraux du droit communautaire et la Charte des droits fondamentaux de l'UE ou par toute autre règle pertinente du droit national, international, communautaire et de l'Union, dans leurs champs d'application respectifs.
2. La présente Charte des droits ne porte pas préjudice aux autres droits applicables à l'Internet ou aux droits applicables dans d'autres domaines, garantis par les constitutions des Etats membres, les traités internationaux sur les droits de l'homme dont la Convention européenne des droits de l'homme, les principes généraux du droit communautaire et la Charte des droits fondamentaux de l'UE ou par toute autre règle pertinente du droit national, international, communautaire et de l'Union, dans leurs champs d'application respectifs.