



Présente :

**Une Europe unie face à la réglementation de l'Internet ?
– Etat des lieux –**

Institut de Berlin-Brandebourg pour la coopération franco-allemande en Europe

Par

– Lionel Thoumyre –

Juriste et chargé de mission au [Forum des droits sur l'Internet](#)
Directeur éditorial de la revue [Juriscom.net](#)

Date de mise en ligne : 23 octobre 2003

Institut de Berlin-Brandebourg pour la coopération franco-allemande en Europe

Une Europe unie face à la réglementation de l'Internet ? – Etat des lieux –

26 septembre 2003

– Lionel Thoumyre –

Juriste et chargé de mission au [Forum des droits sur l'Internet](#)

Directeur éditorial de la revue [Juriscom.net](#)

Introduction

Dresser l'état des lieux de la réglementation de l'Internet est un projet ambitieux. Non seulement parce que nous en sommes à plus de sept années d'effort de réglementation mais aussi parce que la matière juridique et politique dont il s'agit est éminemment transversale ; elle concerne un nombre de domaines impressionnant : le droit de la communication au sens le plus large du terme, la protection de l'enfance, la protection des consommateurs, la liberté d'expression, le droit fiscal, le droit international, le droit des sociétés, de nombreuses branches du droit pénal et du droit civil (droit de la preuve, droit de la responsabilité) etc...

Il s'agit donc d'effectuer une synthèse générale de ce qui a été fait et d'en proposer une analyse critique.

Mais procédons avant cela à l'état des lieux de l'Internet lui-même. Comme toute innovation technologique, l'Internet côtoie le merveilleux autant que le monstrueux. Son caractère décentralisé et transnational en font un outil de communication puissant, utile mais capable de défier toute velléité de contrôle et, par conséquent, d'attirer d'indésirables activités.

1) Un outil de communication puissant et utile

L'Internet engloutit quotidiennement des milliards de données numériques qu'il rend simultanément disponibles aux quatre coins de la planète. Gratuits ou payants, la quasi-totalité des biens dématérialisés sont concentrés sur le Net. Moyennant un peu de patience et de dextérité, on peut y retrouver l'information la plus pointue, le logiciel le plus rare, les enregistrements de concerts les plus inédits, ou les références des dernières nouveautés littéraires que l'on peut commander à distance... Il suffit pour cela de remonter le long des fils de la toile, d'investir les *newsgroups* ou les réseaux *Peer-to-peer*.

Un tel outil de communication a bien-sûr fait naître de nouveaux espoirs : ceux d'un monde meilleur, parce que plus libre ; d'une société plus civilisée, parce que mieux informée ; et de nations plus riches parce qu'elles voyaient l'émergence d'une nouvelle économie.

La frénésie des premiers temps a néanmoins cédé la place à plus de sagesse. L'Internet n'en est pas moins devenu un outil indispensable pour la plupart des secteurs d'activités et de nombreux foyers.

Au premier semestre 2003, 60% des foyers américains sont connectés, 44% en Allemagne (selon les chiffres de l'Office fédéral des statistiques), soit près d'un foyer sur deux, 40% au Royaume-Uni. La France, malheureusement, accuse encore un certain retard avec seulement 26,8% des foyers connectés.

Par ailleurs, les chiffres du commerce électronique sont plutôt encourageants, même si la progression du chiffre d'affaire des principales entreprises de e-commerce tend à se stabiliser.

En France, le commerce électronique B to C a généré 2,4 milliard d'€ pour l'année 2002 contre 61 millions en 1998. La progression du chiffre d'affaire ralentit cependant depuis l'année 2001 : +243% en 2000, +111% en 2001, +64,8% en 2002 (source : Benchmark et Fevad)

2) Un réseau difficile à contrôler

Tout surfeur averti se rend bien vite compte que les contenus et activités contraires à l'ordre public et aux bonnes mœurs ou préjudiciables prolifèrent toujours sur le réseau : contenus violents, xénophobes, révisionnistes, pédo-pornographiques, arnaques financières, jeux de hasard interdits... Avec la complicité des journalistes, la présence de ces informations a largement concouru à diaboliser l'Internet.

Un autre type d'activité, souvent illégale, l'a cependant réhabilité aux yeux du public : il s'agit de l'échange d'œuvre musicales et cinématographiques sur les réseaux Peer-to-peer.

Le téléchargement de musique a représenté, en France, 26% des opérations les plus pratiquées sur l'Internet avant l'été et l'échange de fichier 21% (source : Ipsos). 1 à 3 millions de français ont déjà téléchargé de la musique sur les réseaux P2P.

Comment expliquer l'importance, et le succès, de ces activités sur l'Internet ? Cinq causes probables peuvent être proposées :

1.- en premier lieu, l'Internet est le **miroir de l'existant** : les honnêtes gens, les bien-pensants, les courtois, les excessifs, les contrefacteurs, les violents, les racistes ... tout un chacun a accès au réseau ;

2.- en second lieu, une **culture subversive** s'est très tôt développée sur l'Internet : il s'agit de la culture cyberpunk, celle des hackers qui alimentent les sites « warez » en logiciels piratés, en codes « crackés », en fichiers musicaux MP3 et images pornographiques. Certains défendent une cause libertaire ou collectiviste, d'autres ne font que profiter ;

3.- en troisième lieu, l'**anonymat relatif** dont jouissent les utilisateurs du réseau favorise le sentiment d'impunité et l'« extériorisation » des fantasmes ainsi que des frustrations ;

4.- en quatrième lieu, il s'agit de la première fois, dans l'histoire des médias, que **l'utilisateur peut jouer un rôle aussi important**. Cela le rend davantage maître de la technique, autonome et indépendant, ce qui exalte son sentiment de liberté ;

5.- enfin, les **technologies numériques et l'architecture actuelle** du réseau permettent de cloner à l'infini n'importe quelle information accessible sur le réseau, de l'héberger sur plusieurs serveurs situés dans différents pays. Ainsi est-il difficile, voire impossible, d'obtenir la suppression d'une information lorsqu'elle a été mise en ligne.

Prenons l'exemple de l' « **affaire Gubler** », qui remonte aux années 1995 et 1996, et à partir de laquelle la réflexion juridique s'est véritablement amorcée en Europe. Le Docteur Claude Gubler, médecin de François Mitterrand, avait écrit un ouvrage intitulé « Le grand secret » au sein duquel il révélait en détail l'état de santé préoccupant de l'ancien Président de la République, avant que celui-ci ne décède. Une décision de justice intervint rapidement après la publication de ce livre pour l'interdire à la vente au motif que celui-ci portait atteinte au secret médicale et à la vie privée du défunt. Mais, au nom de la liberté d'expression, un cybercaféier en a tout de suite scanné les pages et les a diffusées sur l'Internet. Le matériel du commerçant fut rapidement saisi. Le contenu avait cependant déjà fait le tour du monde et a été reproduit sur de nombreux serveurs. Aujourd'hui encore, c'est-à-dire sept ans plus tard, on retrouve facilement cet ouvrage à l'aide d'un moteur de recherche : ici sur un site luxembourgeois, là sur un site basque, ou encore en version anglaise sur un site américain ...

Plus récemment, on constate que de nombreux auteurs d'activités considérées comme illicites dans la majorité des pays s'établissent dans le ou les seuls pays où ces activités sont tolérées. Tel est le cas de Kazaa, distributeur d'un logiciel de P2P, installé au Vanuatu, un archipel du Pacifique Sud et, surtout, un paradis fiscal renommé pour les sociétés "off shore". De même plusieurs sociétés de Casinos en ligne se sont établies sur l'île d'Antigua, telle la société Cassava, sans parler de certains révisionnistes qui prennent asile en Amérique du Nord pour bénéficier de la protection du 1^{er} Amendement de la Constitution des Etats-Unis.

Ces acteurs « honnis » de l'Internet ne sont certes **pas à l'abri d'une condamnation** par l'un ou l'autre des pays connectés. Plusieurs affaires ont d'ores et déjà démontré que les autorités ou les juridictions nationales des pays européens n'hésitaient pas à faire **application de leur droit local** pour condamner des sociétés ou des individus situés à l'étranger et, parfois, à obtenir gain de cause. Tel a été le cas dans **l'affaire Yahoo!**, en France en 2000, et avant celle-ci, dans **l'affaire Compuserve** en Allemagne en 1997.

Mais se pose alors le problème de **l'effectivité du droit**, c'est-à-dire de l'application non plus du droit national, mais des sentences nationales à l'étranger (**l'exequatur**). La question légitime que tout le monde se pose alors est : comment chacun de nos pays peuvent-ils, en Europe, faire respecter ses valeurs et son droit local face aux activités illicites qui persistent sur l'Internet ?

En répondant à cette question, on remarquera que les pays européens s'essoufferaient à vouloir imposer leur droit national sur le réseau (I) et qu'il s'agit bien plutôt d'unir nos forces autour de modes de régulation adaptés au réseau (II).

I. Quand le local se heurte au global

Chacun des pays européens a dû entreprendre une démarche positive et « personnelle » pour lutter contre les contenus illicites. Alertées ou saisies par des associations civiles, les autorités de police et les autorités judiciaires de plusieurs états membres ont tout d'abord agi individuellement contre le « fléau internet ». Deux exemples s'imposent, ceux de l'affaire Compuserve Allemagne et de l'affaire Yahoo!

L'affaire Compuserve Allemagne tout d'abord. Il s'agissait de la première grande affaire européenne ayant eu à résoudre un problème conséquent, celui des newsgroups du réseau Usenet. Usenet est en quelque sorte l'ancêtre du P2P : il n'y a aucun serveur central. Tous les groupes de discussion proliférant sur Usenet sont automatiquement « relayés » sur l'ensemble des serveurs des fournisseurs d'accès.

Or, parmi ces newsgroups accessibles en Allemagne, un certain nombre était consacré à la **pédopornographie ou à la zoophilie**. Etant donné leur nombre et le fait qu'il était impossible d'appréhender facilement leurs auteurs et leurs participants, les autorités se

sont naturellement tournées vers l'un des fournisseurs d'accès les plus importants afin de rendre ces contenus inaccessibles sur le territoire allemand. C'est ainsi que les autorités nationales parvinrent à obliger Compuserve US à **bloquer l'accès** à toute la hiérarchie des newsgroups en « alt.bin » où se situait le nœud du problème.

Il n'est pas inutile de préciser que ce blocage s'est répercuté sur tous les points d'accès gérés par Compuserve à travers le monde, **supprimant du même coup l'accès à des contenus licites**. Par ailleurs, Monsieur Felix Somm, l'ancien directeur de Compuserve Allemagne, a été condamné le 28 mai 1998 à deux ans de prison avec sursis et à 100 000 DM d'amende pour avoir permis l'accès à ces newsgroups. Depuis, la justice a relaxé Monsieur Felix Somm sur demande du procureur.

De son côté, la justice française a également eu des démêlés avec une société américaine (**Yahoo! inc.**) qui proposait un service de ventes aux enchères sur lequel était vendu des objets nazis, en contravention avec notre Code pénal. Suite une action judiciaire intentée par des associations militant contre le racisme, une ordonnance de référé du 22 mai (jugement d'urgence) du Tribunal de grande instance de Paris a estimé que « *en permettant la visualisation en France de ces objets et la participation éventuelle d'un internaute installé en France à une telle exposition-vente, YAHOO! Inc. commet une **faute sur le territoire français**, faute dont le caractère non intentionnel est avéré mais qui est à l'origine d'un dommage [pour les associations demanderesse] ...* ». Le tribunal a également ordonné à l'entreprise américaine « *de prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de ventes aux enchères d'objets nazis et de tout autre site ou service qui constituent une apologie du nazisme ou une contestation des crimes nazis.* »

On peut en conclure que, par la force des choses, France et Allemagne se sont retrouvés **unis contre la perméabilité naturelle du réseau vis-à-vis des contenus illicites en provenance d'autres territoires, notamment américains**. Cette perméabilité est due non seulement à l'architecture de l'Internet mais aussi au premier amendement de la constitution américaine garantissant largement la liberté de parole.

La France et l'Allemagne ont donc eu une expérience commune qui a dévoilé au grand jour **quatre séries de difficultés**, qui persistent jusqu'à aujourd'hui, alors même que tous les Etats du monde se trouvent confrontés au phénomène du peer-to-peer :

1.- Première difficulté : le filtrage d'un service situé à l'étranger peut avoir des **répercussions au-delà des frontières** de l'Etat l'ayant demandé. La question est donc la suivante : un seul Etat est-il fondé à faire la loi sur l'Internet, par essence international ?

2.- Seconde difficulté : le filtrage d'un service situé à l'étranger peut avoir une portée supérieure à celle qui est désirée, c'est-à-dire aboutir à **bloquer l'accès à des contenus considérés comme licites** sur le territoire de l'Etat ayant demandé le filtrage. La question est alors : quid de la liberté d'expression ? Quid des dommages collatéraux ?

3.- Troisième difficulté : comment la loi d'un Etat peut-elle être appliquée sur le sol d'un autre Etat ? Et comment le **jugement d'un Etat peut-il être exécuté sur le sol d'un autre Etat** ? Sur ce point, une réponse a déjà été donnée par la justice américaine qui a dû se prononcer sur l'affaire Yahoo!. Elle est on ne peut plus claire : « *Bien que la France ait le droit souverain de contrôler le type d'expression autorisée sur son territoire, cette cour ne pourrait appliquer une ordonnance étrangère qui viole la Constitution des Etats-Unis en empêchant la pratique d'une expression protégée à l'intérieur de nos frontières* » (Cour de District de San José, 7 novembre 2001).

4.- Dernière difficulté : si la technique nous permet un jour d'effectuer un filtrage à la fois efficace et suffisamment sélectif pour ne pas occasionner de **dommages collatéraux**, à qui le **financement** du filtrage devra-t-il incomber ? L'Etat demandant le filtrage ? L'Etat sur le sol duquel l'activité illicite est exercé ? L'Etat où est situé le fournisseur du service concerné ? Le demandeur de l'action en justice ? Le fournisseur du service lui-même ?

On pourrait ajouter une dernière question à celles-ci : souhaitons-nous promouvoir le cloisonnement des frontières physiques sur le réseau des réseaux ou **assumerons-nous différemment les conséquences de la mondialisation de l'information ?**

Ces questions sont posées depuis l'année 1996, depuis la fameuse affaire Gubler. Elles résonnent encore à travers des **affaires plus récentes** et dans certaines transpositions de la directive commerce électronique du 8 juin 2000.

Citons entre autres :

- l'affaire « **J'accuse** » jugée en France le 30 octobre 2001 au cours de laquelle le juge a estimé qu'il ne pouvait contraindre les fournisseurs d'accès à filtrer des sites révisionnistes basés sur le territoire américain ;
- le **filtrage ordonné par le gouvernement local de Düsseldorf** en février 2002 imposant à 80 fournisseurs d'accès à l'Internet de bloquer l'accès à divers sites. Cette décision n'est pas passée inaperçu : le Chaos Computer Club (CCC) et des associations protectrices des droits de l'homme et de la liberté d'expression ont invité les internautes à descendre manifester dans les rues de Düsseldorf ;
- le **projet de loi français sur l'Economie numérique** (LCEN) : un article de ce projet prévoit que le juge peut ordonner des mesures de filtrage. Il s'agit de l'article 43-12 qui est actuellement âprement discuté.

Les réponses aux problématiques énoncées ci-dessus ne sont donc pas aisées à trouver. Gageons qu'elles le resteront dans le cadre d'une régulation traditionnelle. Cette situation nous incite à réfléchir à d'autres modes d'action.

II. Vers une régulation à l'image de l'Internet

A réseau international, solutions internationales. Ces solutions sont triples, il s'agit :

- de poursuivre l'harmonisation des législations communautaires ;
- d'adopter des conventions internationales sur des sujets de haute importance ;
- d'élaborer un réseau multi-acteurs de régulation à l'image de l'Internet.

A. L'harmonisation des législations communautaires

1. Etat des lieux

La course à l'harmonisation des législations européennes pour accompagner l'avènement de la société de l'information a débuté sur le thème de la **protection des données personnelles**. La Directive dite « protection des données à caractère personnel » du 24 octobre 1995 a notamment posé le principe suivant lequel un « traitement de données à caractère personnel » doit « être fondé sur le consentement de la personne concernée ».

Son œuvre sera poursuivie par la directive « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications » du 15 décembre 1997 et celle du 12 juillet 2002 intitulée « vie privée et communications électroniques » qui aborde le cas des communications électroniques non sollicitées pour lesquelles il est exigé que l'expéditeur ait obtenu le consentement préalable du destinataire avant de les lui envoyer. Cette même directive aborde également la question des « cookies » ou « témoins de connexion ». Leur utilisation est autorisée lorsque ces dispositifs sont destinés à des fins légitimes, c'est-à-

dire pour faciliter la fourniture d'un service de la société de l'information, et que les utilisateurs se voient donner des informations claires et précises sur leur finalité.

Le second thème qui a occupé le législateur européen ces dernières années est celui du **commerce électronique**. Est tout d'abord apparue la directive du 20 mai 1997 sur la « protection des consommateurs en matière de contrats à distance » dont l'objet couvre les contrats effectués dans le cadre de la vente à distance traditionnelle mais concerne également le commerce électronique « B to C ». Ce texte détermine les informations dont le consommateur doit bénéficier avant de conclure tout contrat à distance et fixe les modalités précises suivant lesquelles un contrat peut être passé entre un consommateur et un professionnel éloignés. La directive « commerce électronique » du 8 juin 2000 complète et affine certaines dispositions de celle du 20 mai 1997 pour les adapter à la société de l'information. Elle s'intéresse ainsi aux communications électroniques et aux contrats conclus par voie électronique. Elle aborde également l'épineux problème de la responsabilité pour les messages illicites et préjudiciables, découlant de l'exercice des activités techniques : le transport d'information, le caching et la fourniture d'hébergement. Enfin, la directive sur les « signatures électroniques » du 13 décembre 1999 a été adoptée pour favoriser l'utilisation et la reconnaissance juridique des signatures électroniques dans la Communauté européenne, élément indispensable, nous dit-on, pour que fleurisse le commerce électronique.

L'ensemble de ces directives contribuent à la sécurisation des échanges sur l'Internet pour l'ensemble des acteurs du réseau des réseaux.

D'autres directives visent à protéger les intérêts de certains acteurs : **les créateurs, les producteurs et les distributeurs d'informations**. C'est ainsi que la directive dite « accès conditionnel » du 20 novembre 1998 se destine à lutter contre les dispositifs illicites permettant un accès non autorisé à un service protégé et que la directive du 22 mai 2001 dite « droit d'auteur et droits voisins dans la société de l'information » aménage une protection juridique des mesures techniques de protection des œuvres numériques.

2. Eléments critiques

Les **problèmes** abordés par les directives sont complexes et techniques. On ressent à travers les textes que plusieurs **compromis** ont été nécessaires non seulement entre les états membres mais également entre les acteurs en présence. Ce n'est pas forcément un mal, mais cela donne parfois lieu à des textes qui sont, au final, **difficiles à transposer, interprétables** à merci voire **vide de sens**.

Ex. L'article 6-4 al 4 de la directive du 22 mai 2001 sur le droit d'auteur et les droits voisins dans la société de l'information. Cette disposition retire explicitement aux Etats membres, pour les « services à la demande » sur l'Internet, l'obligation de garantir le bénéfice de l'exception de copie privée lorsqu'une œuvre est protégée techniquement.

Les dispositions des premier et deuxième alinéas ne s'appliquent pas aux oeuvres ou autres objets protégés qui sont mis à la disposition du public à la demande selon les dispositions contractuelles convenues entre les parties de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement.

Lorsque le présent article est appliqué dans le cadre des directives 92/100/CEE et 96/9/CE, le présent paragraphe s'applique mutatis mutandis.

Outre la rédaction assez particulière de ce texte qui utilise quelque peu abusivement la technique du renvoi, la question est : qu'est-ce qu'un service à la demande ? Peut-on parler d'une prestation de service pour la distribution d'une œuvre de l'esprit ? Peut-on distinguer selon les techniques de distribution

ou de diffusion (streaming, téléchargement...) pour y répondre ?

Ces conséquences risquent de faire échouer l'harmonisation des législations européennes.

Enfin, la solution de l'harmonisation des législations des directives demeure « **eurocentrique** », c'est-à-dire qu'elles ne visent à résoudre les problèmes posés par la société de l'information qu'au sein même de l'Union qui ne concerne que 15 pays.

Du côté des **aspects positifs**, mentionnons l'expression d'une réelle volonté, que l'on retrouve dans plusieurs directives, de **promouvoir un mode de régulation alternatif**.

Par exemple, l'article 16 intitulé « Code de conduite » de la directive du 8 juin 2000 sur le commerce électronique encourage « l'élaboration, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs, de codes de conduite au niveau communautaire, destinés à contribuer à la bonne application des articles » de la directive.

L'article 17 intitulé « Règlement extrajudiciaire des litiges » de la même directive incite à lever les obstacles « à l'utilisation des mécanismes de règlement extrajudiciaire pour le règlement des différends (...), y compris par des moyens électroniques appropriés. »

B. Les conventions internationales

Le droit international permet de régler les conflits de lois ou de juridictions et organise l'entraide judiciaire en vue de la répression des infractions.

1. Etat des lieux

Outre les préoccupations liées à la protection des intérêts des auteurs et des producteurs cristallisées au sein des traités de l'OMPI de 1996 sur le droit d'auteur et les droits voisins, et auxquels fait écho la directive du 22 mai 2001, la société de l'information a suscité une autre inquiétude au niveau international liée à ce que l'on appelle aujourd'hui la « **Cybercriminalité** ».

Ainsi une Recommandation (N° R [95] 13) du Comité des Ministres a été formulée à l'attention des Etats membres du Conseil de l'Europe le 11 septembre 1995 à propos des problèmes de **procédure pénale** liés à la technologie de l'information. Les considérants de ce texte faisait part d'une préoccupation certaine quant au « *risque que les systèmes électroniques d'information et l'information électronique puissent également être utilisés pour **commettre des infractions criminelles*** ».

Cette recommandation est à l'origine de la fameuse **Convention internationale sur la cybercriminalité** (STE n° 185), signée à Budapest le **23 novembre 2001**, qui vise à **faciliter la recherche et la preuve des infractions à travers la coopération interétatique**. Elle dispose ainsi en son article 25 que les Etats Parties « *s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.* »

La Convention s'architecture autour de trois axes de réglementation :

- **l'harmonisation des législation nationales**. Quatre catégories d'infractions sont ainsi définies : (1) les infractions liées à la **sécurité** des réseaux (accès et interceptions illégales, atteinte à l'intégrité des données, abus de dispositifs), (2) les **infractions informatiques** (faux et fraudes informatiques), (3) les infractions **se rapportant au contenu** (telles que la diffusion de pornographie infantile) et à propos desquels un

protocole additionnel sur les contenus racistes est actuellement discuté, et (4) les infractions liées aux atteintes à la **propriété intellectuelle** et aux droits connexes ;

- **l'adaptation des moyens d'enquêtes** et de poursuites au terrain du cyberspace. Il s'agit notamment de mesures visant à ordonner la conservation, la perquisition, la saisie et l'interception des données stockées dans un système informatique ;

- la mise en place d'un **système de coopération internationale** rapide et efficace : les Etats signataires peuvent agir pour le compte d'un autre pays dans la recherche de preuve électroniques.

Sont signataires de ce traité : la plupart des Etats membres du Conseil de l'Europe ainsi que le Japon, les Etats-Unis, le Canada et l'Afrique du Sud, soit 37 pays. Mais le traité n'entrera en vigueur que lorsque 5 états membres l'auront ratifiés. Actuellement, seuls trois états ont procédé à cette ratification : l'Albanie, la Croatie et l'Estonie.

2. Eléments critiques

Les conventions internationales reçoivent à peu de choses près les mêmes critiques que les directives, à l'exception du caractère eurocentrique. Elles présentent d'autres difficultés notamment en ce qui concerne le **processus d'adoption** et leur **mise en œuvre**.

La Convention sur la cybercriminalité est l'exemple d'une certaine réussite. De 1995 à 2001, il aura fallu peu de temps, compte tenu de l'ambition de ce texte, pour l'adopter. Le 11 septembre 2001 aura sans doute un peu précipité les événements. Mais quel a été le prix de cette précipitation ?

Pas moins de 27 remaniements auront été nécessaires pour emporter le consensus des Etats membres. Par ailleurs, le protocole additionnel sur la répression des textes racistes et xénophobes, qui en est à sa troisième mouture, peine toujours à être adopté. Enfin, depuis 2001 seulement trois Etats ont ratifié le traité. Or, celui-ci ne rentre en vigueur qu'à partir de la cinquième signature.

Ce traité témoigne ainsi du problème que pose les **désaccords fondamentaux** existant entre les pays signataires sur certaines valeurs et normes juridiques.

Mais **l'avantage** indéniable des conventions internationales est qu'elles présentent des solutions intéressant un **nombre important d'Etats**.

Ce mode de coopération internationale est essentiel et, sans aucun doute, indispensable pour lutter contre les activités criminelles. Il n'en reste pas moins un outil **trop lourd** pour réguler l'ensemble des activités sur l'Internet et lutter contre la **cyber-délinquance**.

C. Un réseau mondial multi-acteurs

Moins traditionnelle, plus expérimentale, une troisième source de solution est à l'étude, notamment sous l'impulsion du Forum des droits sur l'Internet.

Le Forum des droits sur l'Internet est un **organisme de co-régulation**. Il organise depuis mai 2001 la concertation, au niveau français, entre les **acteurs publics et privés** sur des sujets relatifs à la régulation de l'Internet. En deux années de fonctionnement, il a produit plus d'une **dizaine d'avis** sur des projets de loi majeurs et **de recommandations** à l'attention du législateur français ou européen, des acteurs économiques, des utilisateurs ou encore des juridictions. Ces recommandations concernent des **sujets très variés** et **techniques** tels que : les données de connexion,

les modes alternatifs de règlement des conflits, les données publiques, l'administration électronique, les communications électorales, le vote électronique, les hyperliens, les forums de discussion, les mesures techniques de protection des œuvres numériques, le filtrage des contenus illicites etc... Le Forum a en outre lancé en juin 2003 un service de médiation pour traiter les différends liés au réseau.

L'idée du Forum part du constat suivant lequel l'Internet ne peut être régulé comme les médias traditionnels au moyen d'une autorité administrative classique ayant pouvoir de sanction. Le caractère décentralisé, international, protéiforme du réseau, et la nouvelle culture de communication qui y est attaché nécessitent d'imaginer un **modèle de régulation adapté**.

Les nombreux avantages que présente le Forum des droits sur l'Internet en font un **outil de plus en plus utilisé** par les acteurs publics et privés. Sa **souplesse** de fonctionnement, sa **neutralité** garantie notamment par un financement public majoritaire, sa capacité à organiser la **concertation sur des sujets complexes** et ses **actions d'information** auprès du public permettent de réaliser progressivement, chaque jour, son objectif de co-régulation.

Mais, pour être véritablement efficace, cette action **doit s'inscrire au niveau international**. Le Forum des droits sur l'Internet participe ainsi activement à la constitution d'un réseau européen multi-acteurs de régulation. Ce **réseau doit être à l'image de l'Internet : fondé sur plusieurs actions locales, décentralisé, partageant un protocole commun (la concertation, la co-régulation...), favorisant la circulation rapide de l'information entre chacune de ses entités**.

Ce projet fédère déjà des organismes belge (l'Observatoire des droits de l'Internet), britanniques (Internet Watch Foundation - Oxford internet Institute), autrichien (Osterreichisches institui fur angewandte telekommunikation), italien (Forum per la tecnologia della informazione) et hongrois (ISTR). Nous espérons associer rapidement des organismes allemand, suisse, polonais et irlandais.

Le **principe d'un réseau multi-acteurs a été acté** aux articles 6 et 38 du projet de déclaration de principe du sommet de Genève sur la Société de l'information qui aura lieu en décembre 2003. Un **suivi de la concertation** qui aura eu lieu à travers ce réseau sur quelques thèmes choisis sera assuré lors du sommet de Tunis en décembre 2005. Ce réseau multi-acteurs pourra donner lieu à la production de conventions internationales emportant plus facilement le consensus.

Ce modèle de régulation coexiste avec un certain nombre d'initiatives européennes, qu'il ne faut pas omettre, telles que le **programme Inhope** issu du plan d'action pour un internet plus sûr (Safer Internet Action Plan) débuté en 1999. Ce programme associe les fournisseurs d'accès européens pour combattre les contenus illégaux et violents à travers un réseau de points d'accès (hotlines), pour réaliser la classification des contenus et des logiciels de filtrage ainsi que des actions de sensibilisation. Le programme **e-Safe** adopté en 2002 poursuit ce plan d'action jusqu'en 2004.

Conclusion

Encore et toujours, l'Internet provoque. Il interpelle nos institutions juridiques : le droit de la presse, le droit de la communication audiovisuel, la propriété littéraire et artistique ou le droit des télécommunications. Depuis bientôt 10 ans, l'Internet défie les autorités centralisées et désoriente les méthodes répressives traditionnelles. Ses plus fervents protecteurs (libertaires, utopistes et génies de l'informatique) considèrent chaque action répressive comme une attaque virale à laquelle ils répondent par la création de puissants « antidotes ». Les logiciels de P2P en sont un bel exemple. Le combat normatif et

répressif est essentiel pour lutter contre la haute criminalité mais inadapté voire dangereux pour remédier aux délits mineurs et aux incivilités sur le réseau.

Il s'agit de doser adroitement les productions normatives internationales, pour qu'elles ne heurtent pas les libertés fondamentales (droit à la vie privée et liberté d'expression) et, surtout, de poursuivre l'œuvre de co-régulation à travers le développement d'un réseau multi-acteurs. Ce réseau part du même postulat holistique sur lequel l'Internet est fondé : « Le tout est supérieur à la somme des parties ».