

PAS DE LIBERTÉ POUR LES ENNEMIS DE LA LIBERTÉ?

Groupements liberticides et droit

*Sous la direction de
Hugues Dumont, Patrick Mandoux, Alain Strowel
et
François Tulkens*

*Actes du colloque du 14 février 2000
organisé à la Maison des parlementaires par
le Centre de Droit de la Culture des Facultés universitaires Saint-Louis,
la Conférence du Jeune Barreau de Bruxelles
et la Faculté de droit de l'Université Libre de Bruxelles.*

BRUYLANT
BRUXELLES

2 0 0 0

LA LUTTE CONTRE LES ACTIVITÉS LIBERTICIDES SUR INTERNET

PAR

ALAIN STROWEL (*)

PROFESSEUR AUX FACULTÉS UNIVERSITAIRES SAINT-LOUIS
ET À L'UNIVERSITÉ DE LIÈGE, AVOCAT

« Il nous faut donc réclamer, au nom de la tolérance, le droit de ne pas tolérer l'intolérant ».

K. POPPER

(The Open Society and Its Enemies, 1963)

L'actualité, notamment autrichienne, nous rappelle le paradoxe démocratique, c'est-à-dire le risque que fait peser sur nos démocraties le système démocratique d'élection au suffrage universel.

Un autre danger, moins visible parce qu'il n'est pas le fait de partis ou autres groupements extrémistes, ayant plus ou moins pignon sur rue, ne doit pas passer inaperçu : il résulte de l'action d'individus parfois isolés qui distillent leur discours haineux (1) sur l'Internet, contribuant ainsi à faire naître en ligne une communauté de l'intolérance.

(*) Je tiens à remercier Mme S. VERSTRAETE (magistrat au parquet de Bruxelles), MM. Manuel ABRAMOWICZ (Centre pour l'égalité des chances), Olivier BOGAERT (Computer Crime Unit - Bruxelles), Erwin FRANCIS (magistrat au parquet de Bruxelles), Pierre-Yves LAMBERT (policier à Bruxelles), Cédric LAURANT (Center for Democracy and Technology - Washington) pour les informations qu'ils m'ont transmises.

(1) Dans la suite, je considère comme interchangeables les termes de discours (ou contenu) haineux (terme traduisant directement la formule « hate speech » utilisée dans la littérature anglo-saxonne) et de discours (ou contenu) liberticide (ce terme ayant été précisé et analysé ailleurs dans le présent volume : voir la contribution de Mme LENOBLE-PINSON).

INTRODUCTION

§ 1. – *Évaluation de la présence
de matériaux haineux en ligne*

L'ampleur du phénomène est encore difficile à circonscrire.

Selon un rapport de l'Office allemand de la protection de la Constitution datant de 1999, plus de 1.400 sites web d'extrême droite auraient été recensés; plus alarmant, cet organisme aurait constaté en un an une augmentation de l'ordre de 35 % du nombre de ces sites (2). Au-delà de chiffres encore très imprécis, certains événements survenus sur la Toile font réfléchir : dans le cadre d'un vote en ligne organisé par le journal *Time* qui demandait aux gens d'élire l'homme du centenaire, Hitler est longtemps resté à la troisième place dans ce hit-parade, apparemment suite à la mobilisation en ligne de groupements néonazis (3).

Depuis le début de 2000, les affaires relatives à la présence de contenu haineux en ligne se sont en tout cas multipliées, qu'elles aboutissent à des décisions judiciaires (4), donnent lieu à des prises de position de diverses autorités (5) ou déclenchent simplement un débat public (6).

§ 2. – *Prise de position du Conseil de l'Europe
et objet de la présente contribution*

Le 25 janvier 2000, l'Assemblée du Conseil de l'Europe a adressé cinq recommandations au Comité des Ministres, dont celle « *de traiter en priorité le problème de la lutte contre la diffusion sur l'Internet*

(2) Voir *La Libre Belgique*, 26/7/99 (une cellule de la police allemande aurait même identifié des appels aux meurtres à l'encontre d'opposants antifascistes avec prime à la clef).

(3) Voir <<http://www.pathfinder.com/time/timel00/poc/century.html>>

(4) Voir par ex. ci-après les affaires *Elbers, Licra et UEJF c. Yahoo!* et *UEJF c. Multimania*.

(5) Ainsi, par exemple, la police suisse a proposé que les fournisseurs d'accès en ligne soient obligés de bloquer l'accès à des sites illicites, notamment à contenu raciste, après notification par les autorités (voir <http://www.wired.com/news/politics/0,1283,36345,00.html>, daté du 15 mai 2000).

(6) Ainsi, le Parti vert du Canada a accusé Amazon.com et Barnesandnoble.com de vendre en ligne des ouvrages racistes et antisémites tels que « Le protocole des Sages de Sion » (voir <http://news.cnet/news/0-1007-200-1692486.html>, daté du 13 avril 2000). De même, le Centre Simon Wiesenthal avait reproché en août 1999 à ces mêmes libraires en ligne d'offrir à la vente en Allemagne l'ouvrage « Mein Kampf », à la suite de quoi ces sociétés avaient exclu de leur catalogue cet ouvrage (voir encore *infra*, pour un cas similaire en Belgique, impliquant la société proxis.be).

de documents racistes, émanant de l'extrême droite comme de l'extrême gauche, en élaborant un instrument légal international » (7).

Il semble en revanche que nos autorités judiciaires ne soient pas encore pleinement conscientes des risques que ces nouveaux développements comportent, ce qui explique qu'à notre connaissance, aucune priorité n'ait encore été donnée à la lutte contre cette forme d'infractions en ligne (8).

En 1993, le Comité des Ministres du Conseil de l'Europe a créé la Commission européenne contre le racisme et l'intolérance (ECRI), groupe d'experts indépendants chargé d'examiner les législations, politiques et autres dispositifs des États membres visant à lutter contre le racisme. L'un des groupes de travail étudie la question de la diffusion de matériel raciste sur Internet. Un rapport devrait être achevé avant fin 2000. Ce groupe *« est chargé notamment de dresser la liste des sites antiracistes existant sur le Web, d'examiner les législations nationales – si elles existent – établissant la responsabilité pénale des créateurs de sites racistes, et, enfin, d'indiquer les jurisprudences pertinentes en la matière. Ce groupe de travail doit également rechercher les instruments non législatifs de lutte contre le racisme »* (9).

Le groupe de travail mis en place n'est apparemment pas chargé d'étudier les questions liées à la *responsabilité d'autres acteurs de l'Internet* (les intermédiaires, encore appelés les ISP, pour Internet Service Providers) ni les questions qu'offrent *d'autres services Internet que le Web*, par exemple les groupes de discussion.

Notre propos sera donc *a priori* plus large, car les problèmes de responsabilité de ces intermédiaires, ainsi que les difficultés inhérentes à ces autres services seront envisagés.

Commençons par rappeler succinctement ce que sont et comment fonctionnent ces services Internet.

(7) Conseil de l'Europe, Recommandation n° 1438 (2000) de l'Assemblée parlementaire suite au rapport de la Commission des questions politiques (rapp. M. Henning Gjellerod), *Menace des partis et mouvements extrémistes pour la démocratie en Europe*, 25 janvier 2000, § 16.

(8) En Belgique, les policiers chargés de la « traque en ligne » (Computer Crime Unit par ex.) et certains magistrats qui ont eu à traiter ce genre d'affaires semblent personnellement préoccupés par ces développements et disposés à faire davantage, même si aucune priorité n'a été officiellement accordée à ce volet de la politique criminelle.

(9) Conseil de l'Europe, Rapport de la Commission des questions politiques (rapp. M. Henning Gjellerod), *Menace des partis et mouvements extrémistes pour la démocratie en Europe*, Doc. 8607, 3 janvier 2000, § 95.

§ 3. – Les principaux services de l'Internet

Les services accessibles sur l'Internet sont variés, ils vont de l'utilisation d'outils offrant une forme d'interactivité (par ex. le courrier électronique, encore désigné comme courriel) à la simple consultation ou transfert de documents (F.T.P., Gopher, World Wide Web, etc.). On se limitera à présenter rapidement les deux services principaux que sont le web et les espaces de discussion (les babilleurs, Usenet), d'autant que les décisions rendues pour diffusion de matériaux haineux (voir *infra*) concernent précisément ces formes de services.

1. Le Web

Parmi les applications d'Internet, la « toile d'araignée mondiale » (le « World Wide Web » ou « www ») est bien connu. Ce service permet tout d'abord la consultation en ligne d'informations très diverses (textes, images, sons, etc.). Il permet de même la création aisée de sites. Le site conçu et alimenté par un fournisseur de contenu sera stocké sur un serveur géré par un tiers, le fournisseur d'hébergement. Un site se compose habituellement d'une « home-page » (la première page, la page d'accueil) et d'autres pages, appelées des « pages web ». Il se peut que le contenu de pages subséquentes soit partiellement fourni par des tiers (comme dans le cas de sites de ventes aux enchères permettant à tout vendeur de faire une offre en ligne; voir *infra*, la décision française relative aux enchères sur Yahoo!).

Chaque site a une adresse IP à laquelle correspond un code URL (ou Uniform Resource Locator) prenant la forme d'une suite de noms de domaines (dont les noms de domaine de premier niveau géographique, tels « .be » (pour Belgique); ces noms de domaine peuvent être réservés par des personnes étrangères; voir *infra*, pour le problème du droit applicable lié la réservation par un groupement liberticide d'une adresse contenant un nom de domaine géographique « exotique »).

Le web peut également être caractérisé comme une interface qui permet de rendre l'information stockée sur le site accessible à n'importe quel usager d'Internet (on parle parfois d'internaute). La caractéristique principale de cette interface est d'utiliser la technique des liens « hypertexte ». Insérés par l'auteur (sous forme d'un

mot souligné ou encadré par exemple), ces signes relais, une fois activés par l'utilisateur, peuvent « transporter » ce dernier vers une autre portion du site hébergé sur le même serveur, voire vers un site logé sur un autre serveur (éventuellement situé à l'étranger). En réalité, c'est un logiciel de navigation (appelé en anglais le « browser », tel que Explorer de Microsoft) qui permet d'accéder à d'autres pages Web. La création de liens hypertextes vers des sites illicites peut déclencher la responsabilité de celui qui crée le lien (voir *infra*). Afin de pallier l'incroyable dispersion de l'information présente sur le Web, des instruments (annuaires, comme Yahoo!, et moteurs de recherche) ont été développés. Ceux qui offrent ces outils de localisation de l'information peuvent aussi voir leur responsabilité mise en cause (voir *infra*).

2. Les espaces de discussion

Cette notion regroupe divers services et instruments.

Un babilleur ou Bulletin Board Systems (BBS) peut être défini comme « une banque de données gérée par un opérateur (System Operator ou Sysop) consultable via le réseau téléphonique et dont la nature et l'importance varient : BBS accessible par une personne à la fois ou par plusieurs simultanément, accès libre ou moyennant mot de passe et/ou paiement, contenu d'ordre général ou centré sur un thème précis... » (10). On a comparé les babillards à des valves d'affichage d'établissements scolaires. L'opérateur de ce service est bien entendu responsable des contenus qu'il place lui-même, mais la question est de savoir s'il encourt une condamnation lorsqu'un participant poste des contenus illicites dans cette banque de données. En outre, la plupart des BBS sont dotés d'un forum de discussion, lieu de débat virtuel. Ces forums peuvent être modérés ou libres (11). L'opérateur qui se réserve le droit de contrôler les contenus en tirera sans doute un argument commercial, mais, en contrepartie, il supportera probablement une responsabilité plus lourde (voir l'affaire *Stratton Oakmont Inc. v. Prodigy Services Co.*) (12). Si l'opérateur préfère ne pas intervenir dans le forum, il se trouve dans

(10) E. WERY, « Internet hors-la-loi ? Description et introduction à la responsabilité des acteurs du réseau », *J.T.*, 1997, p. 418 (qui cite E-law 3.01 : Computer information systems law and system operator liability in 1995 à l'adresse : <<http://www.leefrog.com/E-law>>).

(11) Nous suivons ici les développements éclairants d'E. WERY, *op. cit.*, p. 418.

(12) *Stratton Oakmont Inc. v. Prodigy Services Co.*, 1995 WL 323710, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995), *The Computer Law Association Bull.*, 1995, vol. 10, n° 4, pp. 18-19.

la même situation que le fournisseur d'accès Internet qui stocke sur son disque dur les fichiers du réseau Usenet (13).

Le réseau Usenet comprend des forums de discussion, sous le vocable de « news » ou de « newsgroups ». Par opposition aux babillards, auxquels ils s'apparentent par ailleurs, les newsgroups sont complètement publics, ils ne sont soumis à aucune procédure d'abonnement et ils véhiculent une quantité beaucoup plus importante d'informations (14). A la différence du système des babillards, « il n'y pas un serveur central de News, mais bien plusieurs milliers d'ordinateurs qui maintiennent chacun une copie des news et utilisent un processus très élaboré pour s'échanger les contributions respectives. Ces serveurs se synchronisent » régulièrement (15).

*

* *

Dans l'optique un peu militante, mais surtout très pragmatique que suggère le titre de ma contribution, je voudrais successivement passer en revue les moyens judiciaires (section 1), un exemple d'autoréglementation (section 2) et des mesures extrajuridiques, disons citoyennes (section 3), qu'il est possible et recommandable de mettre en œuvre afin de lutter contre la diffusion de propos liberticides sur Internet. Les exemples cités sont empruntés à divers ordres juridiques obéissant à des règles parfois très différentes; certains seront sans doute déroutés par cette démarche qui s'embarasse peu de la complexité des règles nationales; elle nous paraît difficile à éviter compte tenu de ce que le phénomène Internet méconnaît les frontières (entre autres juridiques).

(13) E. WERY, *op. cit.*, p. 418.

(14) *Ibidem*, p. 420.

(15) O. HANCE, « Business et droit d'Internet », *Best Of Publishing*, 1996, p. 43. Dans l'affaire *Demon* (*Laurence Godfrey v. Demon Internet*, 26 mars 1999, Queen's Bench Division of the High Court of Justice, § 8 (disponible à l'adresse : <<http://www.courtservice.gov.uk/godfrey2.html>>), un juge anglais, Mr. Justice Morland, a défini comme suit le service Usenet : dans ce système de publication en ligne, « un article (connu sous le nom de 'message' ['posting']) est soumis par son auteur au serveur de news Usenet situé auprès de son ISP local (l'ISP originaire) qui dissémine le message à travers Internet. En fin de compte, le message est distribué et stocké sur les serveurs news de chaque (ou de presque chaque) ISP dans le monde qui offre un service Usenet à ses clients. Les internautes du monde entier peuvent lire et 'télécharger' ['download'] le message en se connectant au serveur de news de leur ISP local ».

SECTION I^{re}. — LA LUTTE PAR DES MOYENS JUDICIAIRES

C'est tout d'abord la responsabilité des fournisseurs de contenus haineux sur Internet qui peut être mise en cause.

Le *fournisseur de contenu* peut être défini comme celui qui met à la disposition d'autrui des informations, que celles-ci soient constituées de textes, d'images, de fichiers musicaux ou de marqueurs (metatags) inscrits dans le code source (en langage html) d'un site web. Ce fournisseur de contenu est donc par exemple l'émetteur d'un courrier électronique, le responsable (webmaster) d'un site web, le participant à un babillard ou à un newsgroup. Il est clair que sa responsabilité directe peut être engagée si le contenu qu'il fournit est illicite ou dommageable (voir *infra*, point A).

Mais la communication sur Internet fait intervenir d'autres intermédiaires — on parle de *fournisseurs d'infrastructure, d'accès ou de services* — dont la responsabilité peut être indirectement mise en cause. On reviendra (voir *infra*, point B) sur les problèmes de complicité éventuelle de ces intermédiaires à des violations réalisées par les fournisseurs de contenu haineux.

§ 1. — La responsabilité des fournisseurs de contenu

A. Les précédents

S'agissant des contenus haineux mis en ligne, des décisions ont déjà été rendues pour des forums de discussion et des sites web (16).

1. Groupes de discussion

Affaire Elbers (Belgique)

La première affaire relative à l'article 150 révisé de la Constitution belge (17) concerne la diffusion de propos racistes à travers des groupes de discussion en ligne. M. Elbers était poursuivi sur pied de l'article 1^{er} de la loi du 30 juillet 1981 tendant à réprimer certains

(16) Les services donnant lieu à des communications privées ne peuvent que difficilement donner lieu à des poursuites, vu les conditions de publicité requises par exemple pour les atteintes à l'honneur des personnes. Voir O. VANDEMEULENBROEKE, « Le droit pénal et la procédure pénale confrontés à Internet (Les apprentis surfeurs) », in *Internet sous le regard du droit ?*, Bruxelles, éd. du Jeune Barreau, pp. 220 et s.

(17) Voir à ce sujet d'autres contributions dans le présent volume, dont celle d'A. SCHAUS.

actes inspirés par le racisme ou la xénophobie pour avoir incité à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard d'un groupe ou d'une communauté (et tout particulièrement la communauté marocaine). Un arrêt du 27 juin 2000 de la Cour d'appel de Bruxelles a confirmé sur le plan pénal le jugement rendu par le tribunal de première instance le 22 décembre 1999 (condamnation à six mois de prison avec sursis et une amende de 100.000 BEF), mais en n'accordant toutefois sur le plan civil que 1 franc symbolique de dommages-intérêts à la partie civile, le Centre pour l'égalité des chances (au motif que le premier juge ne pouvait tenir compte de l'acharnement haineux voué par le prévenu au directeur du Centre, ce fait étant étranger à ceux faisant l'objet de la prévention).

Dans sa décision de décembre 1999, le tribunal correctionnel de Bruxelles reconnaissait tout d'abord que les textes postés dans les groupes de discussion (le groupe soc.culture.belgium) répondaient aux conditions de publicité requises par l'article 444 du Code pénal (18). Il en va *a fortiori* de même des textes disponibles sur un site web. La Cour d'appel confirme ce point.

Sur la question de sa compétence territoriale, le tribunal estime que « la réception des messages et la participation au Newsgroup est possible en tous points du territoire belge et *a fortiori* dans l'arrondissement judiciaire de Bruxelles » et qu'il est donc territorialement compétent (la Cour d'appel ne se prononce pas sur cet aspect). Le même raisonnement a été suivi dans les affaires Faurisson et Yahoo! tranchées en France (voir *infra*).

Enfin s'agissant de l'imputabilité des faits, le tribunal suivi par la Cour s'appuie sur l'existence d'une signature sous les messages (de la part de (« from ») Wim Elbers *wimelbers@innet.be*) et sur les présomptions résultant de ce que « une analyse des messages indique qu'aucun doute n'est possible quant au fait que c'est bien le prévenu qui en est l'auteur » et que le prévenu « n'aurait certainement pas manqué de protester devant une telle accumulation de messages signés de son nom, s'il n'en avait pas été l'auteur ». On peut supposer qu'il résultait du dossier que le prévenu avait connaissance de l'existence de ces nombreux messages. La doctrine (19) a raison de se demander pourquoi le Ministère public n'a pas, en s'adressant au

(18) Voir O. VANDEMEULEBROEKE, *op. cit.*, pp. 221 et s.

(19) Th. VERBIEST, « Racisme et Internet : première condamnation belge », *actualité* 13/1/2000 sur le site www.droit-technologie.org/.

fournisseur d'accès, requis l'identification de l'adresse TCP/IP attribuée à l'ordinateur utilisé par le prévenu de façon à rapporter une preuve plus sérieuse.

Cette possibilité d'identifier l'ordinateur qui a envoyé le message existe à condition que les données relatives aux communications soient conservées. On comprend donc l'enjeu de la disposition du projet de loi sur la criminalité informatique (20) qui prévoit l'obligation pour les fournisseurs d'accès d'identifier leurs abonnés et de retracer leurs numéros TCP/IP et, surtout, de conserver ces données.

En dépit de sa condamnation, M. Elbers continuerait à inonder le réseau de ses propos malveillants, mais cette fois sous un pseudonyme que certaines jugent transparent (« pauffin de saint morel »).

L'intervention juridique lourde du pénal révèle ses limites devant la faculté de récidive et d'anonymisation que permet l'Internet, à travers notamment le système des remailers (21).

Affaire Infonie

Une autre affaire (22) a déjà été fixée devant le tribunal correctionnel de Bruxelles (audience fixée au 31 janvier 2001 devant la 56^e chambre). Dans ce cas, c'est le modérateur d'un groupe de discussion sur Infonie qui a déposé plainte contre l'émetteur des messages après avoir vainement tenté de calmer le jeu. L'individu en cause a pu rapidement être identifié dans le cadre de l'enquête et il n'a pas nié les faits. Décision attendue pour le prochain millénaire.

2. Web

Affaire Costes (France)

Au moins trois décisions ont déjà été rendues dans cette affaire qui concernait la diffusion sur le réseau Internet par un compositeur

(20) L'article 14 du projet de loi qui vise à modifier l'article 109^{ter}, E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques prévoit que le délai de conservation des données sera déterminé par arrêté royal, mais ne pourra jamais être inférieur à un an. Il est probable que cette disposition soit encore modifiée avant l'adoption finale de la loi par la Chambre (probablement à l'automne 2000).

(21) Les remailers fonctionnent comme suit : le message est envoyé au remailer plutôt qu'à son destinataire, le remailer se charge de supprimer l'adresse de l'émetteur avant de transmettre le message à l'adresse figurant d'une manière spéciale dans le texte du message (voir *Astuces et Conseils Internet*, 19/01/00, n° 17, p. 4). Il est aussi possible de cacher son identité en ouvrant un compte messagerie sous un faux nom.

(22) Affaire BR 56.11.20340/98.

interprète de rock alternatif, Jean-Louis Costes, de trois textes intitulés « Apprenez le caniveau aux bicots », « Les races puent » et « Blanchette, tapette à bicots », qui étaient disponibles sur le site <<http://www.costes.org>>. Après avoir été attaqué au civil, dans une procédure qui sera considérée comme nulle sur pied des règles de la loi du 29 juillet 1881 sur la presse, M. Costes prend l'initiative de rééditer, la veille du prononcé de la décision, alors qu'il s'attend à une condamnation, et pour échapper à celle-ci, les textes incriminés à une adresse différente. L'Union des Étudiants Juifs de France (UEJF) et la LICRA font alors constater que coexistent deux sites à deux adresses différentes et que, dans la mesure où il s'agit d'une nouvelle édition, l'action n'est pas prescrite. Le dossier est transmis au parquet; le tribunal correctionnel saisi va estimer que dans la mesure où il s'est écoulé plus de trois mois entre la publication initiale et le premier acte de poursuite, la prescription de trois mois de l'action publique prévue à l'article 65 de la loi du 29 juillet 1881 est acquise. Une question nouvelle est ici posée : comment déterminer le premier jour de la publication dans le cas de diffusion sur Internet ? Dans cette affaire *Costes*, la Cour de Paris va, par un arrêt du 15 décembre 1999, souligner qu'en matière d'écrits ou d'images diffusés sur support papier ou audiovisuel, « la détermination du premier jour de mise à disposition du public est aisée, ne serait-ce que parce qu'elle résulte du support lui-même (journaux, messages audiovisuels) ». S'agissant de la mise à disposition par le biais d'un site web, la Cour va estimer que l'acte de publication devient continu et qu'un nouveau délai de prescription court donc à la date où il a été constaté que les textes figuraient sur le site. Par ailleurs, le fait de modifier l'adresse constitue une nouvelle mise à disposition du public. Le pourvoi a été rejeté par un arrêt de la Cour de cassation du 21 mars 2000 (23). L'action publique n'est donc pas éteinte et l'affaire a été renvoyée pour l'examen du fond.

Affaire Faurisson (France)

M. Faurisson a été poursuivi, sur pied de la loi française condamnant le racisme et le révisionnisme, pour avoir posté sur Internet un

(23) Voir <http://www.legalis.net/jnet/decisions/illicite-divers/ca-paris-210300.htm> (le rejet est motivé par le fait que le pourvoi contre les arrêts des cours d'appel ayant statué, en matière de presse, sur les incidents et exceptions autres que les exceptions d'incompétence, ne peut être formé, à peine de nullité, qu'après l'arrêt sur le fond et en même temps que le pourvoi contre ledit arrêt).

texte intitulé « Les visions cornues de l'holocauste ». Par une décision du 13 novembre 1998, le tribunal de grande instance de Paris a acquitté le professeur Faurisson aux motifs que l'imputabilité des écrits révisionnistes à ce dernier n'avait pas été correctement établie par le Ministère public.

Ce qui est plus intéressant, c'est que le tribunal a reconnu sa compétence, alors que le prévenu déniait celle-ci en invoquant le fait que le site était hébergé par un serveur américain. Selon le tribunal, *« en matière de presse, il est constant que le délit est réputé commis partout où l'écrit a été diffusé, l'émission entendue ou vue. En l'espèce, dès lors que le texte incriminé, diffusé depuis un site étranger, a été reçu et vu dans le ressort territorial de Paris, ainsi qu'il ressort de l'enquête, celui-ci est compétent pour connaître de la poursuite »*.

Un raisonnement similaire a été suivi par d'autres juges, notamment le tribunal correctionnel de Bruxelles dans l'affaire Elbers (voir *supra*) (24).

Un problème pratique lié à la production de documents provenant de l'étranger pourra se poser dans ce genre de procès pénal. Le Ministère public peut-il produire, sans passer par une commission rogatoire, des documents dont l'origine se trouve manifestement à l'étranger ?

Sur cette question pratique, elle aussi essentielle, la loi belge relative à la criminalité informatique apporte un début de réponse : en effet, le nouvel article 88^{ter} à insérer dans le Code d'Instruction Criminelle entend permettre au juge d'instruction qui procède à une recherche dans un système informatique d'étendre cette recherche « vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée », par exemple si le système se trouve hébergé à l'étranger.

Affaire Proxis (Belgique)

« Proxis.be », qui s'est imposé en Belgique comme site de vente en ligne de livres et de disques compact, a fait l'objet d'une enquête de la police judiciaire, après que l'on ait constaté qu'il était possible de commander par le biais de ce site des livres révisionnistes (parmi lesquels la prose de Faurisson). Désormais, ces livres se trouvent

(24) En ce sens : Th. VERBIEST, « La presse électronique : quel cadre juridique ? », in *journalistes*, nov.-déc. 1999, n° 5, p. 13 (voir aussi *l'Echo* du 16 sept. 1999).

encore référencés dans l'énorme catalogue en ligne de Proxis, mais il est devenu impossible de les commander, sauf à justifier d'un usage scientifique (25). Apparemment, les responsables du site n'étaient pas au courant de la présence de ces titres douteux dans le catalogue (constitué de serveurs interconnectés).

Le même problème s'est posé ailleurs, avec des réponses différentes. Aux États-Unis, ce ne sont pas les autorités judiciaires qui se sont intéressées à la question, mais des groupements divers ; à la suite des protestations de ceux-ci, Amazon.com n'a pas supprimé les ouvrages qui niaient l'holocauste de son catalogue, mais les a classés dans une sous-rubrique, alors qu'ils se trouvaient dans la catégorie des références consacrées à l'histoire de la seconde guerre mondiale (26). Où l'on perçoit toute la différence entre le traitement américain et européen de la question.

Affaire Vrije Historische Onderzoek (Belgique)

En 1996, la distribution d'autocollants portant le texte « Y avait-il des chambres à gaz à Auschwitz ? » ou « Gab es gaskammern in Auschwitz ? » et renvoyant non seulement à l'adresse du V.H.O. à Anvers, mais à divers sites web contenant de la littérature révisionniste a donné lieu au dépôt d'une plainte par le Centre pour l'égalité des chances. L'une des pages web, intitulée « Auschwitz : myths and facts », contenue dans les trois sites référencés, remettait clairement en cause l'existence des camps d'extermination (27). Le problème était que ces textes étaient hébergés aux États-Unis et/ou au Canada. En l'espèce, les poursuites pouvaient néanmoins être entreprises puisque le responsable du V.H.O., M. S. Verbeke, se rendait, par l'entremise de la distribution d'autocollants à Bruxelles, complice de l'infraction à la loi du 23 mars 1995 en permettant que soit ainsi exposés au regard du public des écrits minimisant le génocide commis par le régime national-socialiste allemand. Aucune décision n'a été rendue dans cette affaire.

(25) Voir *L'Echo*, 27/01/00 (« Proxis : le succès n'empêche pas les couacs »).

(26) Voir l'article de L. CHAUDHRY, « Online Hate Gets Five Stars », <http://www.wired.com/news/politics/0,1283,36499,00.html> consulté à la date du 25 mai 2000.

(27) On pouvait lire par exemple sur le site « www.kaiman.com » : « *The Auschwitz extermination story originated as wartime propaganda. Now, more than 40 years after the end of the Second World War, it is time to take another, more objective look at this highly politicized chapter of history. The Auschwitz legend is the core of the Holocaust story. If hundreds of thousands of Jews were not systematically killed there, as alleged, one of the great myths of our time collapses* ».

B. Quelques difficultés particulières

1. L'hébergement à l'étranger : exemple du site du Front Nouveau de Belgique

Lorsque l'on ouvre un site web, l'anonymat est plus difficile à préserver que dans l'hypothèse de la participation à un groupe de discussion. Mais de délicats problèmes d'application du droit peuvent néanmoins surgir dès lors que le site est par exemple enregistré sous un nom de domaine géographique étranger et que l'organisme d'attribution du nom de domaine ne demande aucune preuve d'identification, l'enregistrement pouvant même se faire en ligne, ce qui est le cas du nom de domaine géographique « .to » (pour « Tonga »). Les responsables du front nouveau de Belgique (fnb) ont cherché à profiter de cette procédure d'enregistrement. Dans le cas du site « fnb.to », l'adresse est elle-même trompeuse : le site n'est en réalité pas hébergé sur un serveur des îles Tonga, mais en Californie. La poursuite judiciaire est ainsi rendue plus ardue, les autorités américaines n'étant pas spontanément disposées à poursuivre la diffusion d'écrits racistes. « Aux États-Unis, notait un commentateur, l'interdiction de la propagande haineuse est considérée contraire à la liberté d'expression » (28).

2. Le cas des hyperliens vers des sites haineux

Pour faire bref, la question est de savoir si celui qui établit des hyperliens (des « liens hypertexte » ou plus simplement des « liens » (29)) vers un site contenant des propos tombant sous le coup des lois prohibant la diffusion d'idées racistes peut être tenu pour complice de cette infraction. Doit-on considérer qu'à travers la création du lien, donc d'une nouvelle voie d'accès à ces documents en ligne, il y a une forme de diffusion illicite ? En cas de réponse positive à cette question (qui demeure controversée), il deviendrait possible de contrer en partie la pratique consistant à faire héberger des

(28) P. TRUDEL et alii, *Droit du cyberspace*, Université de Montréal et éd. Thémis, 1997, pp. 5-20.

(29) Un « lien hypertexte » est une indication interactive des coordonnées d'une page Web. L'indication va permettre d'être directement lié au document qui fait l'objet du lien hypertexte en cliquant simplement sur le texte ou l'image qui se réfère à ce document. Les « liens hypertextes » (ou « pointeurs », ou « hyperliens ») sont généralement des mots soulignés et en bleu.

contenus illicites dans des paradis juridiques o ? il s'avère très difficile d'agir.

On peut présenter cette problématique spécifique à partir d'une décision allemande relative à la diffusion de propos diffamants (30).

Affaire J. Steinhöfel c. M. Best (R.F.A.)

Dans cette affaire (31), le demandeur contestait l'établissement par le défendeur d'un lien à partir de son site (www.emergency.de) vers des informations disponibles en ligne et portant atteinte à son honneur. L'action fondée sur une atteinte au droit à l'honneur, ainsi que sur le droit de la responsabilité délictuelle (art. 823 et 824 du BGB), a donné lieu à une décision du Landgericht d'Hambourg le 12 mai 1998.

Le défendeur avait en l'occurrence inséré une mention d'exonération de responsabilité sur son site, et prétendait qu'en vertu de la liberté d'expression, on ne pouvait l'empêcher d'offrir au public un ensemble d'opinions (« eine Markt der Meinungen ») relatives au demandeur. Nonobstant l'invocation par le défendeur de l'article 5 de la Loi fondamentale relatif à la liberté d'expression, le juge a considéré, dans la mise en balance entre l'intérêt lié à la liberté d'expression et celui tenant à la protection de la personnalité, que les informations vers lesquelles pointaient les liens allaient au-delà de ce qu'autorise la liberté d'expression. En effet, selon les termes de la décision, le défendeur n'a pas rassemblé, à l'aide des liens, un kaléidoscope d'affirmations (« ein Kaleidoskop von Behauptungen ») permettant d'approfondir une affaire publique et « d'aider ainsi à la recherche de la vérité », mais bien un florilège d'articles injurieux (« Zusammenschau eheverletzender Artikel »). En fait, le défendeur avait exclusivement établi des liens vers des articles diffamants, et le tribunal a considéré que le défendeur ne s'en était pas suffisamment distancié, et était donc coupable d'une distribution propre (« eigene Verbreitung ») pour laquelle il fut condamné à payer une somme de 40.000 Deutsche Mark à titre de dommages-intérêts.

(30) Pour plus de détails, voir A. STROWEL, « Liaisons dangereuses et bonnes relations sur l'Internet - A propos des hyperliens », *A & M*, 1998, pp. 296-308; voir aussi A. STROWEL et N. IDE, « La responsabilité des intermédiaires sur Internet : actualités et question des hyperliens », partie II à paraître in *RIDA*, sept. 2000.

(31) Landgericht Hamburg, 12 mai 1998, disponible à l'adresse <http://www.netlaw.de/urteile/lghh-6.htm>, consultée le 20 avril 2000.

Dans ce cas, le fournisseur de liens pouvait difficilement nier avoir connaissance du caractère illicite de ce contenu vu l'existence d'une mise en demeure. La solution pourrait être différente si le caractère illicite du contenu des sites reliés n'est pas flagrant, ou si le fournisseur de liens fait preuve de suffisamment de neutralité et de distance par rapport au contenu relié (en insérant une mention par laquelle il se distancie de ce contenu), la question délicate étant de déterminer à partir de quand il « avalise » ce contenu.

D'autres circonstances particulières peuvent influencer sur l'issue d'une action en responsabilité pour établissement de liens. Que se passe-t-il au cas où le site vers lequel une personne a établi un lien est parfaitement légal au moment de l'établissement de ce lien, mais que des modifications du contenu, intervenues après l'établissement du lien, rendent ce contenu illicite ? Un cas de ce type s'est présenté en Allemagne, dans une affaire introduite au pénal.

Affaire Radikal (R.F.A.)

Le parquet allemand a poursuivi Mme Angela Marquardt pour avoir établi un lien avec un magazine d'écoterrorisme en ligne, qui était interdit en RFA suite à la publication d'un article contenant les instructions à suivre pour saboter les voies ferrées. Selon le parquet, la création du lien était assimilée à un acte de distribution de textes illicites. L'action publique n'avait en l'espèce pas abouti parce que la prévenue avait installé le lien avant que ne paraisse l'article incriminé. Devant décider si la prévenue avait commis une faute pénale en s'abstenant de vérifier périodiquement le contenu vers lequel renvoyait l'hyperlien créé, le tribunal considéra qu'on ne pouvait retenir une telle faute dans le chef de la prévenue (32). Le faire aurait abouti à mettre à charge de celui qui place le lien une obligation très lourde. De plus, comment déterminer la périodicité selon laquelle quelqu'un serait tenu de vérifier le contenu des sites avec lesquels il a établi des liens ? Comme pour d'autres infractions pénales, il faudra établir que la personne qui a créé le lien avait connaissance de la nature illicite du contenu du site lié.

Celui qui a établi le lien n'est pas toujours conscient de ce qu'il contribue à la diffusion de contenus illicites et il peut être pleine-

(32) AG Tiergarten, 30 juin 1997, MMR, 1998/1, p. 49, note St. Hütig. Voir encore : Reuter, « Germans weigh the right to link », 17 janvier 1997 (à l'adresse www.news.com/News/Item/0,47124.html : le site a déménagé).

ment disposé à supprimer de son propre chef ces liens. Ainsi, il s'est avéré que le site de la Chambre proposait des liens vers le site du FN, qui présentait par ex. feu Jean Gol comme un « apatride », dans la pire tradition du délire antisémite; le président de la Chambre a donné suite à la plainte qui lui a été adressée à ce propos (33).

§ 2. — *La responsabilité des fournisseurs de service*

Dans de nombreux cas, celui qui place sans autorisation un contenu raciste sur Internet afin d'élargir sa distribution pourra être attaqué. Mais cette personne sera parfois difficile à identifier (34); elle peut en outre être insolvable, ce qui diminue en conséquence l'intérêt qu'il y aurait de l'assigner en responsabilité; enfin, vu le caractère par essence transnational d'Internet, cette personne, quand bien même serait-elle identifiable et solvable, sera souvent domiciliée à l'étranger, parfois dans des pays où le système judiciaire est largement déficient, ce qui peut constituer un frein supplémentaire à l'introduction d'une action en justice à son encontre. Autrement dit, dans une série d'hypothèses, le recours à l'encontre du fournisseur de contenu risque de ne pas aboutir aux résultats escomptés.

Du point de vue des personnes subissant le dommage lié à une communication en ligne et du point de vue du Ministère public, il apparaît donc tentant de mettre en cause un intermédiaire dans la chaîne de communication (35).

Habituellement, on distingue trois acteurs principaux : le fournisseur d'infrastructure (*network provider*), le fournisseur d'accès (*access provider*) et le fournisseur de services ([*hosting*] *service provider*).

Le *fournisseur d'infrastructure* ou opérateur de télécommunications s'occupe de mettre en place et d'administrer le réseau et les facilités de transmission, tels que les câbles, les routeurs, les commutations, etc. Il paraît très difficile de pouvoir mettre en cause la responsabilité de l'opérateur, sauf pour défaillance technique.

(33) *Le Soir*, 13 avril 2000.

(34) Cela dit, Internet ne garantit pas l'anonymat absolu. La plupart du temps, il est possible de retrouver l'identité de la personne qui a pu être à l'origine d'un message illicite (soit en la contactant directement par le biais de l'adresse e-mail indiquée par exemple sur le site, soit par l'entremise du fournisseur d'accès qui peut être identifié en utilisant les bases de données en ligne du RIPE, l'organisme chargé d'attribuer les blocs d'adresses IP en Europe).

(35) On considère ici comme synonymes les termes « intermédiaire », « fournisseur de service » et « ISP » (abréviation du mot *Internet Service Provider*, couramment utilisé en français).

Le *fournisseur d'accès* est celui qui offre l'accès au réseau Internet. Très souvent, son service comprend aussi la fourniture d'un compte e-mail. En pratique, beaucoup de fournisseurs d'accès offrent d'autres services, par exemple de l'hébergement, ce qui est susceptible d'affecter leur responsabilité.

La situation du *fournisseur de services* est plus complexe, d'autant que les services que ce dernier peut offrir sont multiples. Le service le plus courant est celui d'hébergement : autrement dit, le fournisseur dispose d'un espace (mesuré en Megabites) sur son serveur, qu'il loue à un usager afin que ce dernier y place un site web par exemple. La responsabilité de l'hébergeur pourrait être mise en cause dans le cas où il a connaissance de la présence de documents haineux sur l'un des sites qu'il héberge.

Il existe d'autres intermédiaires fournissant par exemple des services de recherche de l'information en ligne. Il s'agit des moteurs de recherche, tel que Lycos, Alta Vista, Hotbot, etc. ou des annuaires (Yahoo!) qui offrent des systèmes de localisation de l'information, ce qui s'avère indispensable pour aider les utilisateurs à trouver l'information pertinente, compte tenu de l'énorme dispersion de l'information disponible sur Internet. On peut s'attendre à ce que les affaires mettant en cause la responsabilité de ces intermédiaires se multiplient à l'avenir.

Avant de passer en revue quelques décisions de jurisprudence relative aux fournisseurs d'accès, d'hébergement et d'autres services (de localisation de l'information), on peut revenir sur le mécanisme de la responsabilité en cascade.

1. *La responsabilité en cascade et l'Internet*

Après nous être demandé si les règles de responsabilité en cascade qui existent dans différents pays pour les médias traditionnels sont applicables à l'Internet, on évoquera quelques projets de lois qui entendent créer une nouvelle forme de responsabilité en cascade pour les acteurs de l'Internet.

En France, la loi sur la réglementation de la presse de 1881 (art. 42 et suiv.) prévoit un système de responsabilité en cascade, valable pour le domaine pénal. En principe, les directeurs de publication ou éditeurs sont responsables en première ligne, et « à leur défaut », c'est-à-dire s'ils ne sont pas identifiés ou s'ils ne peuvent

pas ou ne peuvent plus être poursuivis (36), « les auteurs; 3° à défaut des auteurs, les imprimeurs; 4° à défaut des imprimeurs, les vendeurs, les distributeurs et afficheurs ». De même, la loi de septembre 1986 sur la communication audiovisuelle a retenu le principe de la responsabilité en cascade pour l'audiovisuel (37) et certains estiment qu'elle est applicable à l'Internet (38).

Aux Pays-Bas, les articles 53 et 54 du Code pénal créent une forme de responsabilité en cascade pour le domaine de l'écrit qui exonère l'éditeur ou l'imprimeur, entendus comme de simples opérateurs économiques qui ne participent pas à la rédaction des propos ou à la décision de publier, et ce à la condition que, premièrement, ceux-ci identifient l'auteur des propos par son nom et son adresse et que, deuxièmement, l'auteur réside aux Pays-Bas et puisse donc être poursuivi (39).

En Belgique, la règle de la responsabilité en cascade, consacrée à l'article 25, al. 2 de la Constitution (40), vaut uniquement pour le domaine de l'écrit (41). Cette disposition ne se substitue pas aux principes de la responsabilité civile, mais règle la question préalable de l'imputabilité de la responsabilité, tant pénale que civile (42). Cette règle oblige, sous peine d'irrecevabilité, d'assigner d'abord l'auteur s'il est connu et domicilié en Belgique; ce n'est qu'à défaut de pouvoir identifier l'auteur que la victime du dommage peut se retourner contre l'éditeur, puis l'imprimeur, et enfin le distributeur.

(36) E. DERIEUX, *Droit de la communication*, Paris, LGDJ, 1999, 3^e éd., p. 367.

(37) Dans ce système, c'est le directeur de la publication (tout service de communication audiovisuelle étant tenu d'avoir un directeur de publication) ou le codirecteur de la publication, et, « à défaut, l'auteur, et à défaut de l'auteur, le producteur sera poursuivi comme auteur principal » (art. 93-3 de la loi du 29 juillet 1982).

(38) Voir P. AUVRET, *L'application du droit de la presse au réseau Internet*, J.C.P., éd. G, 3 février 1999, doctr. I 108, p. 257-263. *Contra*, mais nuancé : E. DERIEUX, *op. cit.*, p. 368 (« En l'absence de mesure spécifique, c'est sans doute ce régime qui s'applique à Internet ... sauf à qualifier ce moyen de 'communication audiovisuelle' »).

(39) K. KOELMAN et B. HUGENHOLTZ, *Online Service Provider Liability for Copyright Infringement*, Genève, étude pour l'OMPI, Workshop des 9 et 10 déc. 1999, texte accompagnant la note 88.

(40) « Lorsque l'auteur est connu et domicilié en Belgique, l'éditeur, l'imprimeur ou le distributeur ne peut être poursuivi ».

(41) Voir : Cass., 9 décembre 1981, *Pas.*, 1982, I, p. 482 : « L'article 25 de la Constitution est étranger aux émissions de télévision ou de télédistribution, celles-ci n'étant pas des modes d'expression de la pensée par des écrits imprimés ». La doctrine demeure partagée à cet égard (voir E. MONTERO, « La responsabilité civile des médias », in A. STROWEL et F. TULKENS (sous la dir.), *Prévention et réparation des préjudices causés par les médias*, Larcier, 1998, p. 101).

(42) L'application du mécanisme de cascade à la responsabilité civile ne fait plus de doute depuis que la Cour de cassation a tranché le problème (Cass., 31 mai 1996, *J.T.*, 1996, p. 597, avec les concl. conf. de M. LECLERCQ (avocat général)).

La doctrine demeure partagée sur l'opportunité d'étendre une règle de cascade, éventuellement adaptée, au monde de l'Internet (43).

La question de l'applicabilité de ces règles à l'Internet demeure donc ouverte; en même temps, il faut constater que plusieurs législateurs envisagent de subordonner la responsabilité des intermédiaires au respect de certaines conditions et l'on peut aussi parler de cascade de responsabilité dans cette hypothèse.

Ainsi, aux Pays-Bas, un projet d'adaptation du Code pénal en matière de criminalité informatique envisage d'étendre la règle de la cascade des articles 53 et 54 Code pénal (voir *supra*) aux ISP et autres intermédiaires. D'après ce projet, le fournisseur pourrait échapper à la responsabilité en se faisant connaître, en indiquant qui a commis l'acte répréhensible et en communiquant toute information pertinente afin de retrouver l'auteur (44). Ce système envisagé pour la responsabilité pénale pourrait, selon certains (45), s'avérer intéressant en matière civile, en ce qu'il inciterait les fournisseurs de services à intégrer dans les contrats avec les fournisseurs de contenu (abonnés) des clauses prévoyant la levée de l'anonymat et la possibilité de supprimer les matériaux illicites.

En France, le texte adopté en seconde lecture (en mars 2000) à l'Assemblée nationale concernant le projet de loi sur la communication audiovisuelle (voir *infra*) (46) oblige les professionnels à identifier les auteurs d'un site. A défaut, l'hébergement d'un contenu illégal pourrait leur coûter 60.000 francs d'amende et 6 mois de prison par site.

L'objectif de ces dispositions, on le voit, est grosso modo de conditionner l'exonération de responsabilité de l'intermédiaire à la possibilité de se retourner contre le fournisseur de contenu illicite,

(43) Voir pour la Belgique : D. FESSLER, « Responsabilités en cascade ou la responsabilité aquilienne sur Internet », in *Internet sous le regard du droit*, éd. Jeune Barreau de Bruxelles, 1997, pp. 67-111; E. MONTERO, « La responsabilité civile des médias », *op. cit.*, p. 96; D. VOORHOOF, « De regel van de getrapte verantwoordelijkheid : van de 19de naar de 21ste eeuw? », *Recente Arresten van het Hof van Cassatie*, 1996, pp. 385-390. De manière générale, il faut éviter d'appliquer de manière analogique à Internet les concepts développés dans le cadre d'autres formes de communication (notion d'éditeur, de diffuseur, transmetteur, etc.). Cf. en droit canadien, P. TRUDEL, *op. cit.*, pp. 5-3 et s.

(44) P.B. HUGENHOLTZ, « Het Internet : het auteursrecht voorbij? », in *Recht en Internet*, Handelingen Nederlandse Juristen-Vereniging, Deventer, W.E.J. Tjeenk Willink, 1998, p. 233 (le projet auquel il était fait référence est le « Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met nieuwe ontwikkelingen in de informatietechnologie, concept-wetsvoorstel 10 november 1997 »).

(45) *Ibidem*.

(46) Voir : <http://www.senat.fr/leg/legencours.html>.

donc d'obliger l'intermédiaire à lever le voile de l'anonymat protégeant son abonné.

2. La responsabilité des fournisseurs d'accès

On se limitera ici à revenir sur l'une des affaires qui a eu un retentissement certain (en première instance), l'affaire *Compuserve Allemagne*.

Ministère public c. Mr Somm (affaire Compuserve – R.F.A.)

Les faits étaient les suivants. La société américaine *Compuserve Inc.* hébergeait, sur son serveur news, des news groups à caractère pédophile (par exemple du type « alt.sex.pedophilia ») et raciste. La société allemande *Compuserve GmbH* permettait aux abonnés allemands d'accéder à ces news groups à des coûts de connexion réduits. *Compuserve Inc.* était la seule société à avoir des liens contractuels avec les abonnés allemands. A la suite d'une perquisition, le ministère public allemand avait communiqué une première liste de cinq news groups illicites à Mr Somm, directeur de *Compuserve GmbH*. *Compuserve GmbH* n'ayant pas les moyens techniques de couper l'accès aux news groups, Mr Somm avait immédiatement transmis la première liste à *Compuserve Inc.*, lui demandant de supprimer les news groups litigieux. Une fois ceux-ci supprimés, le ministère public avait communiqué une seconde liste de 282 news groups illicites à Mr Somm qui, cette fois également, avait répercuté la demande à *Compuserve Inc.* A ce stade, *Compuserve Inc.* avait déclaré, par voie de presse, qu'elle estimait ne plus devoir intervenir, puisque tant *Compuserve Inc.* que *Compuserve GmbH* mettaient maintenant à disposition de leurs clients (en particulier les parents) un outil de contrôle appelé « Cyber Patrol – Parental Control », également disponible en langue allemande, qui permettait à l'abonné de censurer lui-même l'accès aux news groups de son choix.

Suite à ce changement d'attitude, le ministère public avait accusé Mr Somm de faciliter la consultation de news groups à caractère pédophile. L'Amtgericht de Munich l'avait condamné, par jugement du 28 mai 1998 (47), à une peine d'emprisonnement de deux ans avec sursis. Entre autres, l'Amtgericht n'avait pas pris sérieusement

(47) AG München, 28 mai 1998, *Computer und Recht*, 1998, p. 500 et s.; *Multimedia und Recht*, 1998/8, p. 429; voir *A&M*, 1998, p. 359 (où une erreur de date s'est glissée) pour une synthèse en français.

en considération le fait que *Compuserve Inc.* offre ses services à plus de 5 millions d'utilisateurs et qu'il lui était techniquement impossible, au cours de la période pertinente, de bloquer l'accès aux news groups uniquement pour les utilisateurs allemands. Par son arrêt du 8 décembre 1999, le Landgericht de Munich a réformé ce jugement, et acquitté Mr Somm.

En ce qui concerne l'épineuse question de la tierce complicité, le Landgericht a rappelé que celle-ci nécessite la preuve d'une faute dans le chef de Mr Somm. En l'espèce, une telle faute ne pouvait résulter que de deux abstentions coupables. D'une part, Mr Somm n'avait pas bloqué tout trafic avec le serveur news de *Compuserve Inc.* (donc également avec du contenu licite). A ce sujet, le Landgericht a considéré qu'une telle obligation de faire n'avait pas de fondement (la motivation sur ce point n'est pas très claire, mais le caractère disproportionné de la mesure de coupure d'accès semble avoir pesé sur la motivation du tribunal). D'autre part, Mr Somm n'avait pas réitéré les demandes de couper l'accès auprès de *Compuserve Inc.* A ce sujet, le Landgericht a considéré que les chances de succès d'une telle démarche étaient à ce point faibles, vu la position officielle de *Compuserve Inc.* (communiquée par voie de presse; voir *supra*), que Mr Somm n'avait donc pas commis pas de faute en s'abstenant d'insister auprès de la société mère.

Cette affaire met en évidence une difficulté majeure pour la « police » de l'Internet : lorsque l'on ne peut se retourner contre le fournisseur de contenu (ou son hébergeur), soit pour des raisons pratiques, soit parce que le contenu en question demeure licite selon le droit du pays où il se trouve, la seule mesure est la coupure d'accès, que l'on peut exiger depuis l'étranger, mais cette mesure peut apparaître soit disproportionnée (si la coupure d'accès est obtenue pour l'ensemble du réseau, donc aussi pour les pays où le contenu demeure illicite), soit inefficace (si la coupure est sélective et ne vise que les internautes en provenance d'un pays déterminé que l'on peut identifier à partir de leur adresse IP, elle permettra toujours à certains de faire transiter leur demande d'accès par des machines localisées dans des pays tiers, ce qui signifie qu'ils échapperont à la mesure de blocage d'accès). On retrouve le même problème dans l'affaire Yahoo! (voir *infra*).

3. La responsabilité des fournisseurs d'hébergement

Plutôt que de passer en revue l'abondante jurisprudence à ce sujet (48), on peut synthétiser l'apport d'une récente directive communautaire. C'est dans la *directive relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (49) (ci-après : « la directive sur le commerce Électronique ») que l'on trouve une section 4 (art. 12 à 15) consacrée à la responsabilité des fournisseurs de services (le texte communautaire préfère parler de « prestataires intermédiaires »). Ces dispositions qui doivent encore Être transposées valent indépendamment du type de droits auxquels la communication en ligne est susceptible de porter atteinte; l'approche préconisée par l'Union est horizontale et donc applicable à l'hébergement de propos haineux.

Il importe de souligner tout d'abord que la directive reconnaît l'absence d'obligation positive pour les intermédiaires, et notamment les hébergeurs, de contrôler et de rechercher l'information illicite (50), tout en reconnaissant que « les prestataires de services ont, dans certains cas, le devoir d'agir pour éviter les activités illégales ou pour y mettre fin » (voir considérant n° 40).

La directive ne vise pas à harmoniser les droits nationaux en ce qui concerne les conditions de la responsabilité, elle entend avant tout créer au profit des intermédiaires des « havres de responsabilité », autrement dit des cas d'exonérations de responsabilité, valables à la fois sur le plan civil et sur le plan pénal. Sur le plan civil, le texte communautaire limite la responsabilité en matière de dommages-intérêts, tout en laissant ouverte la possibilité d'agir en cessation (en référé). Ces exonérations couvrent à la fois les cas où

(48) Voir A. STROWEL et N. IDE, « La responsabilité des intermédiaires sur Internet : actualités et question des hyperliens », partie I à paraître in *RIDA*, juillet 2000.

(49) Directive 2000/31/CE du 8 juin 2000, *J.O.C.E.*, 17.7.2000, L 178/1.

(50) Voir l'article 15 (*Absence d'obligation générale en matière de surveillance*) :

1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visés aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances indiquant des activités illicites.

2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services, ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.

le prestataire pourrait être directement responsable et les cas où il n'est responsable qu'à titre accessoire (par ex. en tant que complice). Les exonérations ne sont pas accordées en fonction du type d'opérateur (par ex. entreprise de télécommunications, etc.), mais en considération du type d'activité exercé. Le fournisseur d'hébergement est exonéré dans les termes suivants :

Article 14 Hébergement

1. *Les États membres veillent à ce qu'en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :*

- a) *le prestataire n'ait pas effectivement connaissance de l'activité ou l'information illicite et, en ce qui concerne une demande en dommages-intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente; ou*
- b) *le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.*

2. *Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.*

3. *Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation, et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.*

L'exonération ne vaut qu'en cas d'hébergement à la demande d'un client (totalement indépendant du fournisseur de service) et à condition que le fournisseur n'ait pas connaissance de la présence de l'information illicite sur son site. Toute la question est de savoir comment définir ce seuil de connaissance à partir duquel la responsabilité joue pleinement. L'envoi d'une notification ne constitue pas la seule hypothèse de connaissance, cette dernière pouvant résulter aussi de « faits ou circonstances » donnant l'apparence que le contenu est illicite. Une fois la connaissance établie, l'exonération ne jouera que si le fournisseur de services agit prestement pour enlever (ou bloquer l'accès à) l'information illicite.

4. *La responsabilité d'autres fournisseurs de services*

a) *Le cas des moteurs de recherche*

Affaire Yep.com (USA)

Sans vouloir aborder ici la question pointue de la responsabilité de ces intermédiaires que sont les moteurs de recherche, il est intéressant de mentionner une affaire dénoncée par le Centre Simon

Wiesenthal. Ce dernier a publiquement mis en cause un fournisseur de service, Yep.com, qui référence des sites et les classe notamment à l'aune de leur popularité. Ce logiciel de recherche permet(tait ?) de faire une recherche sur des mots-clés tels que « nazi », « sale juif », « musique haineuse » ; les sites haineux référencés se voyaient attribuer une, deux ou davantage d'étoiles (la recherche sur base du mot « jew » aboutissait apparemment à ce que le Jewish Museum de Vienne était moins bien coté qu'un obscur site antisémite du nom de Global Domination (51)). L'issue de cette affaire relatée par la presse en ligne ne nous est pas connue.

Affaire MP3Board.com v. RIAA (USA)

Une affaire qui est susceptible d'avoir des conséquences décisives sur le fonctionnement des outils de recherche sur Internet vient d'être introduite par la société MP3Board.com Inc. qui offre un moteur de recherche en ligne de fichiers MP3. Pour rappel, le MP3 est une norme de compression de fichiers musicaux qui a permis à de nombreux internautes de mettre en ligne des fichiers facilement télé-déchargeables, parmi lesquels on trouve de nombreux fichiers (morceaux) musicaux illicites. Comme d'autres « search engines », le logiciel de recherche de MP3Board.com Inc. recense les sites sur lesquels sont hébergés de tels fichiers et établit des listes de liens vers ceux-ci. Suite aux lettres de mises en demeure adressées par l'association américaine des producteurs de phonogrammes, MP3Board.com Inc. a, à titre préventif, introduit une action déclaratoire afin de voir affirmer par un tribunal de San José que le processus automatique consistant à lier un site web vers d'autres sites ne peut constituer une atteinte au droit d'auteur si le site relié contient du matériel illicite (52).

Il est clair que l'issue de ce procès pourrait également avoir des conséquences sur la responsabilité potentielle des systèmes de recherche en ligne lorsqu'ils permettent, sur base de mots-clés, de trouver du contenu raciste (53).

(51) Voir l'article de L. CHAUDHRY, « Online Hate Gets Five Stars », <http://www.wired.com/news/politics/0,1283,36499,00.html> consulté à la date du 25 mai 2000.

(52) Voir l'article du 14 juin 2000 de B. SANDBURG, « Missing links », sur <http://www.law.com>.

(53) Sur la responsabilité des moteurs de recherche, voir V. SEDALLIAN, « A propos de la responsabilité des outils de recherche », *Chronique de France*, 19 février 2000, sur <http://www.juris-com.net>.

b) *Le cas des sites de ventes aux enchères*

Affaire Licra et UEJF c. Yahoo! (France)

La Licra (Ligue internationale contre le racisme et l'antisémitisme) et l'UEJF (Union des Étudiants juifs de France) ont assigné Yahoo Inc. et Yahoo France pour avoir rendu accessible en France un site Internet proposant la vente aux enchères d'objets nazis.

Le tribunal de grande instance de Paris a fait preuve d'audace en ordonnant, le 22 mai 2000, « à Yahoo Inc. de prendre toutes les mesures de nature à dissuader et à rendre impossible sur Yahoo.com toute consultation du service de ventes aux enchères d'objets nazis et de tout autre site ou service qui constitue une apologie du nazisme et une contestation de crimes nazis ». Le juge des référés a laissé à Yahoo Inc. deux mois de réflexion pour lui soumettre « les mesures qu'elle compte prendre pour mettre un terme au dommage et au trouble subi par les requérantes et pour prévenir tout nouveau trouble ». Lors de l'audience-relai du 24 juillet, il a été décidé de soumettre à un comité de trois experts la question de savoir comment filtrer l'accès au site américain de façon à « rendre impossible » la consultation des pages incriminées par les internautes français. Une nouvelle audience est fixée le 6 novembre. Cette décision concerne également la filiale française de Yahoo! qui n'a pas hébergé de sites litigieux mais qui, par un lien vers Yahoo.com, permet de visualiser les pages du site de ventes aux enchères contraires au code pénal français. Le tribunal a ordonné à cette filiale de prévenir tout internaute consultant yahoo.fr que, si le résultat d'une recherche l'amène à pointer sur des sites, pages ou forums dont le contenu constitue une infraction à la loi française, « il doit interrompre la consultation du site concerné sauf à encourir les sanctions prévues par la législation française ou à répondre des actions en justice initiées à son encontre ».

Le juge des référés a fait application de la loi pénale française (54) alors même que le site incriminé se trouve hébergé aux États-Unis, ce qui est apparu critiquable aux yeux de certains (55). Depuis long-

(54) Au-delà de la contravention à la loi française, il a souligné que la vente de ces objets nazis constitue « une offense à la mémoire collective du pays profondément meurtrie par les atrocités commises par et au nom de l'entreprise criminelle nazie à l'encontre de ses ressortissants et surtout de ses ressortissants de confession juive ».

(55) Voir E. WERY, « Aspects internationaux du réseau (DIP) : à propos de l'affaire Yahoo! », disponible sur le site www.droit-technologie.org dans les actualités de mai 2000.

temps, le droit vient borner le champ de média à portée transfrontalière. L'on ne voit pas *a priori* pourquoi Internet, réseau mondial, devrait échapper à cette emprise du droit (national). Le juge Jean-Jacques Gomez s'est donc estimé à juste titre compétent. Autre chose est de trouver une solution (technique) pour qu'un ordre de cessation valable en France puisse être exécuté sans empiéter sur d'autres espaces juridiques.

SECTION II. – LE RECOURS À L'AUTORÉGLEMENTATION (exemple de la Belgique)

En Belgique, les ISP réunis au sein de leur association, l'ISPA (56), ont signé, le 29 mai 1999, un accord de collaboration avec les Ministres de la Justice et des Télécommunications. Le préambule explique clairement pour quelles raisons cette forme de collaboration des acteurs professionnels de l'Internet se justifie :

« Considérant que dans une société de l'information, les libertés individuelles, en particulier la liberté d'expression doivent ... être garanties ;

Considérant qu'il convient toutefois d'encadrer le développement de l'Internet, notamment afin de protéger les citoyens, et en particulier les plus faibles d'entre eux, contre les abus que peuvent engendrer ces progrès technologiques ;

Considérant en particulier que certaines infractions pénales (pornographie infantile, racisme, infractions en matière de jeux de hasards, etc.) acquièrent une dimension spécifique lorsqu'elles sont commises via l'Internet, vu la circulation mondiale et « en temps réel » des contenus véhiculés par ce biais ;

Considérant que la lutte contre la mise à disposition du contenu illicite via l'Internet, en particulier concernant la pornographie infantile, est considérée comme une question prioritaire en Belgique ainsi qu'au niveau international et supranational, à la suite des initiatives prises notamment par les Ministres belges des Télécommunications et de la Justice ;

Considérant que les infractions commises via l'Internet peuvent être sanctionnées sur la base des dispositions du Code Pénal et des lois pénales particulières ;

Que toutefois des difficultés existent en ce qui concerne la recherche de ces infractions ; que les problèmes les plus importants dans la lutte contre la criminalité sur l'Internet sont le caractère transnational de l'Internet, le caractère immatériel des infractions et la nécessité impérieuse d'une réaction rapide ;

Considérant qu'outre une collaboration internationale entre autorités compétentes, la collaboration avec les fournisseurs de services (Internet Service Providers, ISP) est à cet égard primordiale ;

Considérant qu'au niveau international comme en Belgique, l'autoréglementation est considérée comme instrument privilégié »

(56) L'Internet Service Provider Association (ISPA) représenterait 80 % de la profession.

Dans ce texte, on rappelle à la fois la vocation du droit pénal à s'appliquer à Internet et les difficultés pratiques de mise en œuvre qui justifient le recours à une forme d'autoréglementation.

Il ne s'agit pas d'obliger les ISP à passer Internet au crible afin d'identifier les éventuels contenus illicites. Aucune obligation de surveillance (ou de « monitoring ») n'est donc mise à charge de ces intermédiaires, à l'instar de ce que prévoit l'article 15 de la directive sur le commerce électronique (voir *supra*). S'agissant de son champ d'application, le Protocole ne couvre que les communications publiques d'information via l'Internet, non pas les communications privées telles qu'un courrier électronique à caractère privé, un « chat » privé ou un site web dont l'accès est limité.

Les principes de collaboration adoptés dans le cadre du Protocole sont les suivants :

- si l'ISP constate par lui-même un « contenu présumé illicite » (57) ou qu'un utilisateur attire son attention sur la présence d'un tel contenu, l'ISP en informera « le point de contact judiciaire central » qui est en fait le point de contact central de la computer crime unit nationale de la police judiciaire (adresse e-mail : contact@gpj.be);
- si l'ISP est averti par un tiers, il s'engage à informer le plus rapidement possible le point de contact judiciaire central;
- si le point de contact judiciaire central décide de prendre en considération le contenu présumé illicite, il transmet la plainte au parquet compétent. Parallèlement, l'ISP (ou l'utilisateur selon les cas) et l'ISPA reçoivent un avis spécifiant que le dossier a été pris en considération;
- l'ISPA communique alors à tous ses membres (près de 80 % des fournisseurs d'accès en Belgique) l'information selon laquelle le dossier est transmis au parquet;
- si le contenu est hébergé par un ISP qui n'est pas membre et qui est établi à l'étranger, l'ISPA communique dans les meilleurs délais le contenu à l'association des ISP du pays concerné, si une telle organisation existe, ou, à défaut, à l'ISP concerné.

L'engagement de collaboration des ISP ne va pas beaucoup plus loin; ce n'est que si le contenu visé est présumé constituer une infraction en matière de pornographie infantine que « les ISP s'en-

(57) La notion de « contenu présumé illicite » n'est pas définie dans le texte du Protocole.

gagent à bloquer par tous les moyens dont ils peuvent raisonnablement disposer, l'accès au contenu illicite ».

Le système mis en place qui doit faire l'objet d'une évaluation régulière, semble fonctionner plutôt bien.

SECTION III. – LA LUTTE PAR D'AUTRES MOYENS

La diffusion d'idées haineuses est un problème qui requiert d'autres mesures que celles qu'offre l'arsenal juridique, tout particulièrement pénal; lorsque le problème est celui de la présence de contenus illicites sur Internet, plus qu'ailleurs, le droit étatique n'apparaît pas comme la panacée. Une section de la présente contribution se devait donc de présenter d'autres mesures envisageables – parlons de réactions privées et citoyennes.

La vigilance des partis démocratiques et des associations

Les affaires impliquant des contenus racistes sur l'Internet doivent être mises sur la place publique de façon à faire réagir les divers acteurs de l'Internet.

Ainsi, le Parti vert canadien s'en est publiquement pris aux libraires en ligne que sont Amazon.com et Barnesandnoble.com, qui offraient en vente des ouvrages à contenu haineux, en insistant sur la volonté elle-même affichée par ces sociétés de se comporter en « entreprise citoyenne responsable » (*responsible corporate citizen*) (58).

Bien entendu, l'invocation d'une éthique des affaires n'a pas de sens lorsque la diffusion de ces contenus est davantage le fait de particuliers. Dans ce cas, les associations de lutte contre le racisme doivent assumer une mission d'information, qui peut par exemple prendre la forme de recensions de ressources en ligne permettant aux individus d'acquérir l'esprit critique indispensable.

(58) Voir <http://news.cnet/news/0-1007-200-1692486.html>, daté du 13 avril 2000.

*La pédagogie de la citoyenneté
et du multiculturalisme en ligne et à l'école*

Dans une note du 29 janvier 1996, M. Jean Cornil (59) soulignait que les sites propageant un discours scandaleux devaient être poursuivis et condamnés sur base des législations contre le racisme; il ajoutait qu'il importait par ailleurs « *de développer une pédagogie de la citoyenneté et de la tolérance au travers de sites, qui montrent positivement l'inanité des distinctions et des hiérarchies raciales et plaident pour l'enrichissement des cultures et le respect des différences* ». Ce complément à la lutte sur le plan judiciaire est bien entendu indispensable.

Et à cet égard, la première mission consiste à recenser les sites antiracistes, antirévisionnistes etc. La coopération antifasciste a réalisé un remarquable travail de compilation de sites luttant contre l'intolérance. La liste de ces sites disponible en ligne à l'adresse www.caf-afc.org est reproduite en annexe à la présente contribution.

Il ne suffit pas de les recenser, il faut encore inciter tout un chacun à les visiter, ne fût-ce que dans le cadre des cours d'apprentissage de la citoyenneté à l'école. La familiarité avec l'ordinateur et l'initiation à l'Internet ne feront pas seulement les entrepreneurs de demain, elle peuvent aussi contribuer à forger les démocrates de demain.

Les « acceptable use policies » et la Nétiquette

Les fournisseurs qui offrent la clé d'accès au réseau peuvent aussi définir les règles de jeu et les « usages acceptables », à commencer dans les contrats conclus entre les usagers et ces fournisseurs d'accès. Le non respect de ces normes contractuelles peut être sanctionné par la coupure de l'accès au réseau; c'est dire qu'une forme crédible de pression peut être exercée par ces intermédiaires sur leurs clients. En pratique, ces intermédiaires commerciaux sont très peu enclins à exercer un contrôle sur leurs abonnés au motif qu'ils risqueraient de les perdre rapidement au profit de concurrents, et cela reste vrai depuis que l'accès à Internet est devenu un service gratuit. L'accroissement des sanctions et risques liés à la mise en œuvre de la responsabilité des intermédiaires (voir *supra*) pourrait

(59) Premières réflexions relatives à la problématique de la propagande à caractère raciste sur Internet, Note du Centre pour l'égalité des chances et la lutte contre le racisme, 29 janvier 1996.

constituer pour ces opérateurs un incitant à « monitorer » davantage les contenus rendus publics par leurs clients.

Ajoutons que dans la mesure où ces réglementations des usages acceptables ont été au départ conçues au sein de la communauté universitaire américaine, la consécration de la liberté d'expression, indissociable du principe de la liberté académique, apparaît dans ces « polices » à ce point fondamentale qu'elle n'admet que très peu de limites. Généralement, on prévoit dans ces règles l'interdiction de diffusion de matériel « inapproprié », mais sans préciser ce qu'il faut entendre par là.

Par nétiquette, on désigne « les principes de bonne conduite généralement reconnus par la communauté des usagers de l'Internet » (60).

Selon ce code, les minorités sociales et religieuses ne doivent faire l'objet d'aucune discrimination, toute expression du racisme doit être combattue, etc. Et les réactions en ligne ont certainement permis d'éliminer quelques poignées de néonazis qui se sont faufilés dans des groupes de discussion. Tout cela est certes positif (et gentil), mais cela semble ne pas suffire pour policer les comportements de certains sur l'Internet.

Le « flaming » et autres réactions des internautes et modérateurs

Les internautes peuvent eux-mêmes prendre à partie ceux qui postent des contenus racistes en ligne à travers, par ex., la technique du *flaming*, qui consiste à initier un mouvement de critique et de représailles en ligne.

Les participants aux groupes de discussion ont développé, parfois avec humour, des techniques visant à décourager ceux qui ont un message à faire passer (message religieux, politique, etc. et qui peut s'avérer raciste), que l'on pourrait gentiment appeler les casse-bonbons en ligne (61). Le rôle des modérateurs de groupes de discussion est également essentiel, parce qu'ils sont amenés à entrer en dialogue avec ceux qui distillent l'intolérance dans ces groupes. Une for-

(60) P. TRUDEL et alii, *op. cit.*, pp. 3-41.

(61) Voir par ex. J. ROUILLARD, « Comment réussir à ne pas faire taire casse-bonbons », sur www.rouillard.org.

mation adaptée (une éducation citoyenne?) devrait pouvoir leur être prodiguée.

De manière parfois très organisée, des sites proposent aussi des stratégies de résistance. Voici un exemple de maximes de base à (faire) respecter :

- Faire connaître la présence d'un site intolérant en le faisant savoir à son ISP;
- Encourager les sites qui visent à mettre à jour les sites haineux en leur communiquant des adresses douteuses;
- Communiquer les adresses de ces sites aux moteurs de recherche qui seraient amenés à les recenser;
- Utiliser des moteurs de recherche « intelligents » qui prennent la peine d'éliminer les pages au contenu haineux;
- Déposer une plainte auprès des autorités;
- Privilégier les opérateurs et notamment les hébergeurs qui appliquent une politique de sélection des sites.

CONCLUSIONS

M. Faurisson aurait affirmé qu'avec l'apparition d'Internet, jamais sa pensée n'a été mieux diffusée et que, paradoxalement, jamais il n'a été aussi peu inquiété par les autorités judiciaires. Il est vrai qu'il n'a pu être condamné dans l'affaire liée à l'hébergement de certains de ses écrits aux États-Unis (voir *supra*), mais d'autres décisions de justice, plus audacieuses (par ex. dans l'affaire *Yahoo!*) pourraient venir contredire la thèse selon laquelle Internet garantit l'impunité. Certaines sanctions juridiques demeureront toutefois délicates à mettre en œuvre. C'est le premier problème lié à la lutte par des moyens judiciaires.

En outre, pour ce qui est de la définition des infractions liées à la présence de contenu haineux en ligne, la profonde divergence entre la culture américaine de la liberté d'expression et la formulation européenne de celle-ci freinera pendant longtemps les tentatives de régulation juridique du phénomène. Car il est clair que les règles à définir pour combattre le discours haineux en ligne n'ont de sens, comme le rappelait fin juin 2000 le Ministre allemand de la Justice lors d'un colloque consacré à l'extrémisme sur Internet, que si elles sont adoptées au niveau international, donc également par

les Etats-Unis ou d'autres Etats qui ont une tradition différente de la nôtre en ce qui concerne les limites à la liberté d'expression.

Cette régulation juridique risque donc de se heurter à d'importantes résistances.

En revanche, on peut s'attendre à ce que poussés par des associations, éventuellement relayées par des responsables politiques, les principaux acteurs d'Internet adoptent des mesures (formes d'autoréglementation ou collaboration à des initiatives citoyennes) qui limiteront la diffusion des discours liberticides en ligne. Telle nous semble être la voie à préconiser; elle passe par la prise de conscience des intermédiaires.

Fin 1998, des responsables de l'association « Actions interculturelles judéo-musulmanes » faisaient publier une carte blanche dans le journal *Le Soir* (5-6 déc. 1998) intitulée « Internet, les droits de l'homme et la loi belge » et consacrée au contenu haineux et illicite accessible en ligne; et ils concluaient dans les termes suivants :

« Nous sommes convaincus qu'en ce domaine, notre pays peut faire figure de pionnier. En comblant un vide juridique nuisible à la démocratie, le parlement belge pourrait entraîner à sa suite les États membres de l'Union européenne et les pays tiers ».

Cette conviction, je la partage et je voudrais vous la faire partager à un moment où certains signes semblent indiquer qu'un pays qui n'a, c'est un fait, plus de poids sur le plan des grands équilibres géopolitique et économique, pourrait toutefois garder un rôle de messager, messenger du sens démocratique.

N'est-ce pas par excellence au Sénat qui abritait le présent colloque que ce rappel du rôle symbolique de l'État démocratique devait être fait ?

ANNEXE

LISTE DE SITES LUTTANT CONTRE LES GROUPEMENTS LIBERTICIDES
ET LE DISCOURS HAINEUX SUR INTERNET (*)

ANTIRACISTES

Belgique

Antifa-info (AFI)

<http://www.antifa.net/afi/>

Antifascistisch front (AFF)

<http://www.antifa.net/aff/aff.htm>

Blokbuster

<http://www.antifa.net/blokbuster/>

Comité de vigilance antifasciste du cercle du Libre Examen de l'ULB (CVAF)

<http://www.ulb.ac.be/students/librex/cellules/CVAF/cvaf.html>

Coordination antifasciste de Belgique-Antifascistisch coordinatië van België (CAF-AFC)

<http://www.caf-afc.org>

Extrême droite, non merci! Extreem rechts, nee bedankt!

<http://digitaalbrussel.vgc.be/users/extreemrechts/>

Inter-régionale du Front antifasciste (IR-FAF)

<http://www.multimania.com/antifasciste/>

Résistances

www.antifa.net/resistances

Les Territoires de la mémoire

<http://www.liegeonline.be/fr/entr/termem01.html>*France*

L'Affront national

<http://www.geocities.com/CapitolHill/Lobby/3453/index.html>

Antifa (Annuaire des sites antifascistes)

<http://altern.org/antifaf/>

Centre d'étude et d'action contre le racisme et l'antisémitisme

<http://www.col.fr/cera/>

Fachoscope

<http://assoc.wanadoo.fr/decadi/FACHO.html>

(*) Cette liste réalisée par la coopération antifasciste est disponible à l'adresse www.caf-afc.org. Invitons le lecteur à poursuivre sa recherche en ligne.