IRIS plus
OBSERVATIONS JURIDIQUES
DE L'OBSERVATOIRE EUROPEEN DE L'AUDIOVISUEL

Filtrage des contenus protégés par le droit d'auteur sur Internet en Europe

par Christina Angelopoulos

EDITORIAL

La question de la diffusion sans autorisation de contenus protégés par le droit d'auteur sur Internet a déjà été abordée à plusieurs reprises dans le cadre d'IRIS *plus* Collection. L'une des solutions permettant d'éviter, au moins partiellement, les contrefaçons qui en résultent consiste à mettre en place des filtres Internet. C'est le thème choisi pour ce numéro d'IRIS *plus*.

Le présent rapport examine notamment quels sont les services (simple hébergement ou services Internet) pour lesquels ces filtres s'avèrent utiles et donc courants, ce qui pose ensuite la question de savoir si leur utilisation doit être volontaire ou imposée par la loi ou la justice.

À la lumière de plusieurs décisions judiciaires récentes, Christina Angelopoulos illustre comment la recherche d'une solution s'avère délicate, tant il est difficile de concilier les réponses juridiques prévues aux violations concrètes du droit d'auteur et une obligation générale de surveillance potentiellement illicite. La question essentielle qui se pose consiste à définir dans quelle mesure les filtres Internet peuvent ou doivent restreindre le droit fondamental à la liberté d'information.

L'articulation entre, d'une part, la Directive sur le commerce électronique et, d'autre part, la Directive sur le droit d'auteur, joue également un rôle central pour déterminer dans quelles circonstances et dans quels cas il convient d'imposer l'usage de filtres Internet en cas de besoin. La révision de la Directive sur le commerce électronique ne manquera pas d'avoir un impact sur l'avenir des filtres Internet. L'auteur nous livre un aperçu des perspectives d'évolution, parmi lesquelles figure la possibilité d'une autorégulation, avec quelques exemples à l'appui.

Strasbourg, mars 2009

Susanne Nikoltchev
Coordinatrice IRIS
Responsable du département Informations juridiques
Observatoire européen de l'audiovisuel

IRIS *plus* est un supplément à **IRIS,** *Observations juridiques de l'Observatoire européen de l'audiovisuel,* **Edition 2009-4**

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

76 ALLEE DE LA ROBERTSAU • F-67000 STRASBOURG
TEL. +33 (0)3 88 14 44 00 • FAX +33 (0)3 88 14 44 19
http://www.obs.coe.int
e-mail: obs@obs.coe.int

IRIS plus
OBSERVATIONS JURIDIQUES
DE L'OBSERVATOIRE EUROPEEN DE L'AUDIOVISUEL

Filtrage des contenus protégés par le droit d'auteur sur Internet en Europe

Christina Angelopoulos
Institut du droit de l'information (IViR) de l'Université d'Amsterdam

Introduction

Au cours de la dernière décennie, les filtres Internet se sont retrouvés sous les feux de la rampe. Proclamés comme offrant un réel potentiel de contrôle sur la diversité déconcertante des cyber-contenus, les filtres sont de plus en plus considérés comme le moyen le plus efficace de combattre des phénomènes aussi disparates que la pédopornographie, les jeux en ligne, les atteintes à la sécurité sur Internet et la contrefaçon[1]. Cependant, leur faisabilité et leur pertinence sont remises en question, d'aucuns soulignant que les filtres actuels ne sont pas suffisamment sensibles, ni intelligents pour classer correctement les contenus rencontrés[2]. Néanmoins, il n'est pas du ressort de cette édition d'IRIS *plus* de procéder à l'analyse des capacités technologiques des nouveaux logiciels de filtrage. L'objet du présent rapport consiste à étudier le caractère légal de l'usage des filtres en présumant que les filtres sont capables de distinguer correctement les contenus audiovisuels licites et illicites. À partir de là, nous analyserons le cadre législatif européen actuel pour déterminer qui peut, et dans quelles conditions, exiger l'usage de filtres en Europe pour bloquer ou filtrer l'accès aux contenus audiovisuels protégés par le droit d'auteur. Dans ce cadre, l'examen portera en premier lieu sur le régime de responsabilité des intermédiaires en ligne, sur les réseaux et les sites desquels les filtres de protection du droit d'auteur seraient applicables, ainsi que sur l'interprétation de ces règles au vu de la jurisprudence récente des Etats membres. Le rapport se penchera ensuite sur les limites imposées à l'usage des filtres pour garantir le respect de la liberté d'expression, au vu de l'article 10 de la Convention européenne des Droits de l'homme et dans le cadre des dernières recommandations du Conseil de l'Europe relatives aux filtres Internet. Enfin, le rapport fera le point sur les pratiques volontaires (à la fois en termes d'autorégulation et de corégulation) de filtrage par les intermédiaires sur Internet.

1. Le cadre juridique européen en place en matière de filtrage

En principe, quiconque contribue directement ou indirectement à la violation d'un droit exclusif peut être tenu responsable d'une contrefaçon. Une exception a été introduite concernant la responsabilité des intermédiaires en ligne, lorsqu'ils agissent en qualité d'intermédiaires, par l'instauration, en Europe, d'un cadre règlementaire distinct pour les « services de la société de l'information ». La Directive sur le commerce électronique[3] comporte une série d'exonérations de responsabilité conditionnelles horizontales, ou dérogations, pour certaines activités ou fonctions exécutées par des intermédiaires, notamment le « simple transport » (« *mere conduit* » article 12), la forme de stockage dite « *caching* » (article 13) et l'hébergement (article 14). Chaque dérogation est régie par un ensemble spécifique de conditions devant être remplies pour que l'intermédiaire puisse bénéficier de cette dérogation. En outre, l'article 15 de la Directive interdit aux États membres d'imposer aux prestataires de ces services une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou de rechercher activement des faits ou des circonstances révélant des activités illicites. Nous examinerons ci-dessous le filtrage au niveau des sites Web et des fournisseurs d'accès à Internet (FAI), lesquels correspondent aux intermédiaires assurant l'hébergement et le simple transport visés par la Directive sur le commerce électronique.

Quelles sont les implications du régime de responsabilité mentionné ci-dessus pour l'usage prescrit par l'Etat de techniques de filtrage visant à protéger les contenus relevant du droit d'auteur ? D'une façon générale, le terme de filtrage désigne des applications logicielles de contrôle des contenus conçues pour bloquer automatiquement l'affichage ou le téléchargement de matériaux sélectionnés sur un navigateur Internet ou toute autre application Internet[4]. Cette opération peut être effectuée par divers moyens techniques ; comme nous le verrons plus loin, l'une des solutions consiste en un simple filtrage, en bloquant l'accès à un contenu sur la base de l'adresse IP ou URL où il se situe. Ce type de méthode qui repose sur la décision humaine de bloquer spécifiquement le matériau ciblé n'encourt pas l'article 15 de la Directive sur le commerce électronique. Par ailleurs, la nouvelle génération d'outils de filtrage, de plus en plus sophistiqués, est plus difficile à concilier avec l'interdiction d'imposer des obligations générales de surveillance[5]. Citons, à titre d'exemple, la technologie courante de reconnaissance par empreinte (*fingerprinting*) développée par des prestataires de services et de technologies tels qu'Audible Magic : la technologie de reconnaissance par empreinte utilise une représentation numérique unique de chaque élément du contenu protégé, par exemple d'un clip vidéo (une « empreinte » du contenu), en vue de les identifier parmi tous les contenus téléchargés sur un site d'hébergement ou transfé-

© 2009, Observatoire européen de l'audiovisuel, Strasbourg (France)

rés sur un réseau, sur la base d'une comparaison avec une vaste base de données de référence contenant toutes les empreintes prélevées. Les ayants droit qui souhaitent protéger leur œuvre en ligne peuvent fournir une empreinte de cette œuvre pour la base de données[6]. Un contenu correspondant à cette empreinte et identifié sur le cyber-trafic est alors bloqué. L'avantage de la technologie de reconnaissance par empreinte, par rapport au blocage des adresses IP, réside dans le fait que la détection du contenu indésirable est automatique ; en revanche, ce système présente l'inconvénient, d'un point de vue juridique, d'impliquer la surveillance[7] de l'intégralité des informations qui passent par un fournisseur d'accès Internet (FAI). Aux États-Unis, le *Digital Millennium Copyright Act* (loi sur le droit d'auteur numérique-DMCA) dispose explicitement que pour se prévaloir des exonérations de responsabilité prévues par le texte de loi, les prestataires de services doivent héberger et ne pas entraver les dispositifs techniques standards permettant aux ayants droit d'identifier et de protéger leurs œuvres, sous réserve que cela n'entraîne pas de frais substantiels pour le prestataire, ni une surcharge de leur système ou de leurs réseaux[8]. En revanche, aucune condition de ce type n'est prévue dans la législation européenne, ce qui, dans un premier temps, a permis aux commentateurs de conclure que les exonérations de l'UE échappaient totalement aux technologies de filtrage, puisque l'exemption visée à l'article 15 d'une obligation générale de surveillance était absolue[9]. Cette conception s'est néanmoins vue infirmée à plusieurs reprises, ces dernières années, dans la mesure où les tribunaux se sont montrés réticents à dégager toute responsabilité des intermédiaires en ligne pour défaut de filtrage. En outre, les exonérations sont uniquement conçues pour dégager la responsabilité des FAI en matière de réparation, néanmoins des injonctions peuvent leur être adressées aux fins de prévention des atteintes au droit d'auteur. Nous exposons ci-après une sélection de cas de jurisprudence illustrant les différentes tactiques adoptées en vue d'imposer un contrôle renforcé de ces services. Le premier volet concerne les tentatives visant à engager la responsabilité des FAI pour n'avoir pas eu recours à un dispositif de filtrage, et le second volet traite des ordonnances judiciaires contraignant les FAI à se soumettre à cette obligation.

1.1. Responsabilité des intermédiaires et obligation de filtrage

A. L'affaire MySpace

En juin 2007, le Tribunal de Grande Instance de Paris (TGI de Paris) a réfuté le statut d'hébergeur pour le site de réseau social en ligne MySpace, le plaçant ainsi hors du champ d'application de la dérogation visée à l'article 14 de la Directive sur le commerce électronique [10].

Le tribunal a considéré que le fait d'imposer à ses membres une structure préconçue de présentation pour leur profil personnel, en lien avec la diffusion, à chaque consultation, de publicités manifestement lucratives, conférait à MySpace le statut d'éditeur. Des décisions similaires avaient déjà été rendues par les tribunaux français[11]. Si l'on considère que le régime de responsabilité des éditeurs est nettement plus contraignant que celui des hébergeurs, cette décision, en classant MySpace comme éditeur, encourage effectivement le site à utiliser des systèmes de filtrage automatique de façon à éviter le placement de contenus illicites susceptibles de compromettre sa situation juridique. Lorsqu'un service de la société de l'information ne peut bénéficier d'aucune dérogation prévue par la Directive sur le commerce électronique, il est assujetti à la législation nationale en matière de droit d'auteur, qui fixe les critères définissant la contrefaçon directe et indirecte et les moyens de défenses disponibles[12].

B. L'affaire Dailymotion

Début 2007, suite à la découverte de copies illégales du film *Joyeux Noël* hébergées sur Dailymotion, une plateforme d'échange vidéo alimentée par les usagers, le producteur, le réalisateur et le distributeur du film ont entamé des poursuites contre le site Web pour contrefaçon[13]. Dans cette affaire, l'argument des demandeurs selon lequel Dailymotion fonctionnait comme un éditeur a été rejeté ; en revanche, en juillet 2007, le TGI de Paris a établi que le modèle commercial de Dailymotion basé sur la publicité n'entamait en rien le fait que les contenus soient postés par les internautes, ce qui confère à Dailymotion le statut d'hébergeur[14]. Ceci dit, le tribunal a ensuite établi que l'article 6-1-2 de la loi pour la confiance dans l'économie numérique (LCEN) [15] du 21 juin 2004, qui transpose l'article 14 de la Directive sur le commerce électronique, ne prévoit pas une exonération de responsabilité, mais une simple limitation. Il poursuit en estimant que l'architecture et les moyens mis en œuvre par Dailymotion permettaient les activités illicites, alors que le succès même du site reposait sur la mise en ligne par les internautes de contenus protégés par le droit d'auteur. Attendu que l'article 6-1-2 de la LCEN exige que, pour se prévaloir d'une exonération de responsabilité, un hébergeur doive :

a) ne pas avoir eu effectivement connaissance d'activités illicites ou de faits et de circonstances faisant apparaître ce caractère illicite, et
b) dès le moment où il en a eu cette connaissance, avoir agi promptement pour retirer ces données ou en rendre l'accès impossible,

le TGI de Paris a considéré que la société Dailymotion ne pouvait bénéficier de cette exonération. Il convient de noter que ces considérations concernent uniquement les hébergeurs et non les services de simple transport ou de *caching*. Dailymotion a ensuite invoqué la dérogation à l'obligation générale de surveillance, telle qu'elle est visée à l'article 6-1-7 de la LCEN (transposition de l'article 15 de la Directive sur le commerce électronique). Le tribunal a rejeté cet argument au motif que cette dérogation ne s'appliquait pas en cas d'activités illicites générées ou induites par le prestataire lui-même. En

revanche, le tribunal considère que les intermédiaires qui fournissent aux internautes les moyens de commettre une contrefaçon ont pour obligation d'effectuer un contrôle préalable afin de prévenir tout usage illicite de la part des internautes. En s'abstenant de mettre en place un dispositif bloquant l'accès au film, Dailymotion a manqué à cette obligation. Par conséquent, Dailymotion a été reconnu coupable de contrefaçon et condamné à verser des dommages et intérêts.

Cette décision a donné lieu a un certain nombre de débats et de critiques, en particulier concernant l'instauration d'une nouvelle obligation, pour les prestataires de services, de mettre en place *a priori* des moyens techniques de filtrage pour prévenir le piratage en ligne. Le raisonnement du tribunal laisse perplexe, en particulier, si l'on considère que dans l'exposé des faits, il apparaît que Dailymotion s'est abstenu de retirer toutes les vidéos illicites de son site, même après notification de la part des ayants droit. Cette attitude aurait dû normalement interdire toute application de la dérogation accordée aux hébergeurs en vertu de l'article 14. Au vu du manquement de la société Dailymotion à son obligation de réagir pour empêcher les activités illicites dont elle avait connaissance, la nécessité d'imposer une obligation en amont aux intermédiaires hébergeurs pour bloquer un contenu illicite est contestable et difficile à concilier avec l'article 15 de la Directive sur le commerce électronique. En effet, au sens strict, la nouvelle obligation annule la plupart des avantages de la dérogation en mettant de fait sur le même plan la responsabilité d'une plateforme d'hébergement et celle d'un éditeur[16]. Cette décision est actuellement en appel.

C. L'affaire Tranquility Bay

En octobre 2007, le TGI de Paris a déclaré que Google Video, plateforme d'échange de vidéos postées par les internautes, était coupable de contrefaçon sur la base des multiples copies illicites du documentaire « Les enfants perdus de Tranquility Bay » présentes sur son site Internet[17]. À l'instar de l'affaire Dailymotion, le tribunal a de nouveau reconnu que Google Video pouvait bénéficier de l'exonération de responsabilité applicable aux services d'hébergement en vertu de l'article 14 de la Directive sur le commerce électronique.

En outre, l'exposé des faits révèle que cette fois-ci, le prestataire a réagi promptement pour bloquer l'accès aux copies du film suite à la notification des ayants droit. Pourtant, chaque retrait du contenu illicite était suivi immédiatement d'une remise en ligne sur le site, contraignant ainsi les ayants droit, le site Internet et les internautes à un jeu sans fin du chat et de la souris. Le tribunal a conclu qu'après avoir été informé de l'existence de copies illicites, Google était dans l'obligation de mettre en œuvre tous les moyens nécessaires pour éviter leur diffusion ; par conséquent, bien que le blocage rapide de l'accès à la vidéo illicite à la suite de la première notification lui permette de se prévaloir de l'exonération de responsabilité pour cette première contrefaçon, Google a néanmoins manqué à ses obligations, issues des dispositions de l'article 6-1-2 de la LCEN, pour toutes les remises en lignes ultérieures. Le tribunal a donc considéré que la responsabilité de Google était engagée.

En dépit d'une formulation plus circonspecte que dans la précédente affaire Dailymotion (la question de l'instauration d'une obligation générale de surveillance *a priori* de tous les contenus protégés postés sur le site par les internautes est éludée[18]), la décision rendue dans l'affaire Tranquility Bay soulève également des questions quant à sa compatibilité avec l'article 15 de la Directive sur le commerce électronique. Comme l'ont fait remarquer certains commentateurs, le TGI de Paris fonde, semble-t-il, son interprétation sur l'article 6-1-7, alinéa 2 de la LCEN, qui permet d'imposer une obligation de surveillance « ciblée et temporaire ». En fait, selon le raisonnement du tribunal, même si les multiples remises en ligne sont imputables à différents internautes, le contenu reste identique, ce qui implique que l'obligation de surveillance vise ici un élément en particulier. Il n'en reste pas moins que Google a retiré promptement toutes les copies illicites repérées par les soins des ayants droit, alors que, par ailleurs, l'obligation d'empêcher de futures infractions - laquelle est difficilement conciliable avec l'interdiction d'une surveillance générale de la part des intermédiaires - n'a pas été remplie. Selon le tribunal, si les hébergeurs souhaitent dégager leur responsabilité, ils sont tenus, à la réception d'une notification, de repérer toutes les copies illicites restantes ou remises en ligne, c'est-à-dire d'effectuer concrètement un contrôle général sur tous les contenus de leur site, y compris ceux qui sont licites. En fait, étant donné que les notifications risquent de s'accumuler rapidement, le seul moyen pratique d'y parvenir est d'utiliser une technologie de filtrage automatique par empreinte ou similaire. Par conséquent, la spécificité de l'objet de l'obligation est annulé par la portée des implications de cette décision, qui met en jeu la responsabilité de tous les hébergeurs pour toutes les œuvres pour lesquelles une notification relative à une seule copie illicite leur a été adressée. Une approche plus fiable permettant de garantir le respect du critère de spécificité consisterait à prononcer une injonction ordonnant l'obligation *ex post* d'empêcher les contrefaçons, limitée au cas particulier en cause (voir ci-dessous paragraphe 1.2), soit, en l'occurrence, aux contrefaçons portant exclusivement sur « Tranquility Bay ». Dans cette affaire, il n'y a pas eu de mesure judiciaire de cette nature. Au contraire, le tribunal semble avoir placé entre les mains des ayants droit des compétences d'extension du champ de responsabilité avec un effet *ex ante*, ce qui permet de suspendre la dérogation prévue pour les hébergeurs par l'article 14 à la demande des ayants droit, sans qu'il soit besoin de procéder à un examen juridique préalable[19].

Comme le fait apparaître l'analyse, ci-dessus, des incohérences et de l'évolution maladroite du raisonnement de la jurisprudence au sein d'un seul et même État membre, les tribunaux

© 2009, Observatoire européen de l'audiovisuel, Strasbourg (France)

semblent perplexes en ce qui concerne l'application correcte des dispositions dérogatoires et ils tâtonnent pour trouver les moyens, dans le nouveau cadre juridique restreint, d'imposer une responsabilité, dans un contexte de piratage massif, marqué par la difficulté d'identifier et d'assigner en justice les internautes personnellement responsables[20].

1.2. Injonction et obligation de filtrage

Les règles de la Directive sur le commerce électronique en matière de responsabilité sont exclusivement limitées aux demandes de dommages et intérêts des ayants droit à l'encontre des prestataires Internet. L'ordonnance d'injonctions, quelles qu'elles soient, par un tribunal ou une autorité administrative est formellement autorisée par le dernier paragraphe de chacune des dispositions dérogatoires des articles 12 à 14, qui prévoient la possibilité pour « une juridiction ou une autorité administrative » d'exiger du prestataire qu'il « mette fin à une violation ou qu'il prévienne une violation ». Par ailleurs, l'article 8 (3) de la Directive sur le droit d'auteur[21] prescrit explicitement aux États membres de « veiller à ce que les titulaires de droits puissent demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin », tandis que la Directive de 2004 relative au respect des droits de propriété intellectuelle[22] réaffirme cette obligation à l'article 9 (1) en se référant à la Directive sur le droit d'auteur et en reprenant cette disposition.

Pourtant, en matière de filtrage, concilier cette possibilité avec l'article 15 de la Directive sur le commerce électronique relève d'un exercice périlleux. Dans son préambule, la Directive sur le commerce électronique explicite la portée admissible d'une telle ordonnance : des injonctions peuvent être prononcées afin de « prévenir toute violation en retirant les informations illicites ou en rendant l'accès à ces dernières impossible » (considérant 45), mais ne peuvent imposer une obligation de surveillance que dans des « cas spécifiques » (considérant 47). Par conséquent, des injonctions exigeant la mise en place de dispositifs techniques de filtrage peuvent être légalement prononcées à l'encontre des prestataires, sous réserve qu'elles ne concernent que des personnes, des sites ou des contenus spécifiques[23].

A. L'affaire SABAM/ Tiscali

Dans une affaire qui fait figure de référence, la Société Belge des Auteurs (Belgische Auteurs Maatschappij - SABAM) a entamé une procédure contre la société IAP Scarlet (anciennement Tiscali), en invoquant le fait que cette dernière autorisait délibérément le téléchargement illégal d'œuvres protégées de la SABAM par l'échange de fichiers *peer-to-peer* sur son réseau. La SABAM réclamait une ordonnance contraignant l'IAP à prendre des mesures en amont afin d'empêcher ses abonnés d'échanger illégalement des œuvres protégées. Le Tribunal de Première Instance de Bruxelles a fait appel aux services d'un expert afin d'évaluer la faisabilité des mesures envisagées et en juin 2007, il a ordonné à Scarlett d'installer un système de gestion et d'identification des contenus par empreinte, développé par Audible Magic[24]. Scarlet s'est vu accorder un délai de six mois pour se conformer à cette injonction, sous peine d'une astreinte de 2 500 EUR par jour de retard. Sur la base du considérant 40 de la Directive sur le commerce électronique, selon lequel « les dispositions de la présente directive sur la responsabilité ne doivent pas faire obstacle au développement et à la mise en œuvre effective, par les différentes parties concernées, de systèmes techniques de protection et d'identification ainsi que d'instruments techniques de surveillance rendus possibles par les techniques numériques », le tribunal en a conclu que la proscription d'une obligation générale de surveillance n'excluait pas l'utilisation de dispositifs de filtrage. Ce raisonnement pose néanmoins un problème, dans la mesure où le considérant 40, pris dans son ensemble, se réfère à des « accords volontaires négociés » entre toutes les parties intéressées, de préférence à des ordonnances judiciaires. Toutefois, cet élément ne constitue pas une objection irréfragable dans la mesure où le considérant 45 de la directive prévoit la possibilité d'injonctions légales exigeant des mesures de prévention d'une infraction. En revenant à l'article 15 proprement dit, le tribunal a établi de façon catégorique que l'injonction requise n'exigeait pas de la société Scarlet qu'elle « surveille » son réseau ou « recherche activement des faits ou des circonstances révélant des activités illicites ». Cette conclusion est sujette à débat et dépend probablement de la technologie employée, de même que des instructions requises par le tribunal. Le TPI de Bruxelles a donc conclu qu'aucune obligation générale de surveillance n'était imposée, puisque les instruments de filtrage étaient limités au blocage de certaines informations spécifiques. Il s'agit une fois de plus d'un état de fait qui dépendra de la façon dont l'instrument spécifique utilisé exécutera ses fonctions de filtrage. Le tribunal n'a donné aucun élément concernant son raisonnement sur ces questions, néanmoins, comme nous l'avons exposé ci-dessus, il est difficile de considérer la technologie d'empreinte numérique employée par Audible Magic comme distincte d'une pratique de surveillance générale. Il convient de souligner que Scarlet était réticente à utiliser des méthodes de filtrage, craignant que les modifications apportées aux informations circulant sur son réseau ne compromettent son statut de simple routeur. Cette objection a été rejetée de façon convaincante par le tribunal : en effet, l'autorisation formelle du considérant 40 quant à l'utilisation de ce type de technologie, de même que l'autorisation des injonctions visée par le considérant 45 devraient suffire à exclure une telle éventualité.

Comme chacun s'y attendait, Scarlet a fait appel de cette décision. Une audience est prévue en octobre 2009, tandis qu'entretemps, le déroulement des évènements n'a fait que ren-

forcer la complexité de cette affaire : en octobre 2008[25], Scarlet a obtenu un délai supplémentaire, soit jusqu'à la fin du mois, pour mettre en œuvre les mesures requises visant à empêcher les infractions, après avoir fait la démonstration que, sur son système, le logiciel de filtrage d'Audible Magic s'avérait techniquement inexploitable. Néanmoins, le TPI de Bruxelles a considéré qu'il n'était pas déraisonnable d'exiger que Scarlet fasse des efforts supplémentaires pour se conformer à l'injonction et lui a demandé d'examiner d'autres solutions de filtrage[26].

B. L'affaire Pirate Bay

En août 2008, le *Giudice Per le Indagini Preliminari* (tribunal des enquêtes préliminaires) de Bergame avait placé sous séquestre préventif le site Web suédois de liens BitTorrent, Pirate Bay, dans le cadre d'une enquête judiciaire ouverte à l'encontre de ses propriétaires, accusés d'avoir favorisé et encouragé le partage illicite de fichiers. À cette fin, les FAI italiens avaient été contraints de mettre en place des mécanismes permettant de bloquer l'accès à ce site. En septembre, cette décision a été revue et finalement infirmée : selon le tribunal de Bergame[27], la saisie préventive est un outil judiciaire qui peut s'appliquer à un produit spécifique et dont les effets sont opposables aux tiers (*erga omnes*), dans la mesure où elle débouche sur l'interdiction applicable à tout un chacun d'utiliser ledit produit. Dans le cas d'un site Internet basé hors du territoire national, le seul moyen d'obtenir le même effet consiste à prononcer une ordonnance contraignant tous les FAI nationaux à bloquer l'accès au site Internet saisi, ce qui dénature totalement la mesure prise : une interdiction *erga omnes* devient ainsi une injonction personnelle à l'encontre des intermédiaires en ligne ; or, dans le cadre de la législation italienne, ceci n'est autorisé que dans certains cas bien précis, qui n'englobent pas les infractions au droit d'auteur.

Cette décision est conforme à l'interprétation susmentionnée des directives sur le commerce électronique et sur le droit d'auteur : si, en vue de prévenir toute infraction, des injonctions peuvent être prononcées par des autorités nationales pour ordonner une obligation de surveillance, avec retrait des informations illicites ou blocage de l'accès à ces informations, à l'encontre des intermédiaires en ligne dont la responsabilité n'est pas engagée, mais qui transmettent des copies illicites de tiers sur leurs réseaux, cela ne peut se faire que dans des cas particuliers et en conformité avec la législation nationale[28].

Curieusement, cette conclusion a été confirmée par un arrêt danois qui va exactement dans la direction opposée : en novembre 2008, une cour d'appel danoise a rendu un arrêt ordonnant au FAI danois DMT2/Tele2, de bloquer l'accès au site de Pirate Bay. La même année[29], le tribunal de grande instance danois avait au préalable reconnu que le FAI était dégagé de toute responsabilité en vertu des dérogations prévues par la Directive sur le commerce électronique, tout en soulignant que rien, par ailleurs, ne dispensait le FAI de faire l'objet d'une ordonnance d'injonction. Par conséquent, la question cruciale ne porte pas sur l'engagement de la responsabilité du FAI, mais consiste à savoir si les conditions fixées par le droit procédural danois pour prononcer une injonction sont réunies ou non. Il s'est avéré que tel était le cas : le tribunal a établi que Pirate Bay avait porté atteinte au droit d'auteur et que DMT2 avait contribué à cette infraction au droit d'auteur en assurant la transmission des contenus illicites sur ses réseaux. Par ailleurs, le tribunal a également jugé que DMT2 avait lui-même enfreint le droit d'auteur en procédant au stockage automatique, intermédiaire et provisoire desdits contenus au cours de leur transmission. Le tribunal a estimé que cette affaire ne pouvait pas attendre un jugement ordinaire et qu'une ordonnance imposant à DMT2 de verrouiller l'accès au site Web n'occasionnait pas un préjudice disproportionné au FAI. Cette décision repose sur une argumentation conforme à la jurisprudence précédente de la Cour suprême du Danemark[30].

1.3. Projets d'amendement et de clarification législatifs

L'article 21 de la Directive sur le commerce électronique enjoint la Commission à préparer un rapport bisannuel relatif à l'application de la présente directive, accompagné, le cas échéant, de propositions visant à l'adapter à l'évolution juridique, technique et économique. Le lancement d'une consultation publique afin d'identifier les lacunes du cadre législatif en place était imminent au moment de l'impression de la présente édition d'IRIS *plus*. Cette consultation devrait déboucher sur un nouveau rapport, au second semestre 2009, puis sur une nouvelle proposition législative[31]. Le nouveau rapport accordera une place particulière à la question de la responsabilité des intermédiaires et au rôle de surveillance des FAI[32]. On peut espérer que ce nouvel examen apportera plus de clarté à la fois sur la question de la méthode la plus appropriée pour appliquer les trois cas d'exonération de responsabilité[33] et de la démarche à adopter pour trouver un équilibre entre les directives sur le droit d'auteur et sur le commerce électronique en cas d'injonction. Si les tribunaux peuvent prononcer des injonctions à l'encontre des intermédiaires qui transmettent sur un réseau une contrefaçon commise par un tiers d'une œuvre protégée, conformément à la Directive sur le droit d'auteur, ces ordonnances constituent-elles une obligation générale de surveillance, et partant, dérogent-elles à l'article 15 de la Directive sur le commerce électronique ? Si tel n'est pas le cas, quand peut-on considérer qu'une obligation de surveillance est limitée à un cas particulier, au sens visé par la Directive sur le commerce électronique, et la différence entre un FAI et un hébergeur est-elle pertinente dans ce cadre ? L'utilisation d'outils de filtrage constitue-t-elle une surveillance générale et, si oui, quels sont les outils concernés ? Toutes ces questions urgentes ne pourront trouver une réponse coordonnée de la part des tribunaux de l'Union européenne sans une harmonisation législative ou un guide de jurisprudence.

© 2009, Observatoire européen de l'audiovisuel, Strasbourg (France)

Un certain nombre d'ajustements ou de clarifications sont également en cours concernant d'autres directives de l'UE : fin 2007, le premier rapport de la Commission sur l'application de la Directive sur le droit d'auteur a été publié[34]. La réponse du Parlement européen (PE), désigné sous le terme de Rapport Médina[35], devrait être soumise au vote en mars 2009. La dernière version, qui se base sur une présomption d'illégalité pesant sur tout téléchargement *peer-to-peer*, prône le blocage de Pirate Bay par ordonnance judiciaire, encourage le lancement des technologies de filtrage et invite à une réflexion sur la question de la responsabilité des FAI dans la lutte contre le piratage.

S'il est adopté, ce rapport marquera une volte-face du PE par rapport à la position qu'il affichait au printemps dernier dans le Rapport Bono[36], dont les amendements déposés aux fins d'obliger les FAI à adopter des technologies de filtrage avaient été retirés du texte final.

En outre, dans ce contexte, la réforme du paquet de directives UE règlementant le marché européen des télécommunications (le « paquet »Télécom) [37] pourrait également avoir des répercussions. À cet égard, l'amendement 112 (article 33 2(a)) du Rapport Harbour[38] joue un rôle central, puisqu'il prescrit aux régulateurs nationaux des télécoms de surveiller la « coopération » entre les FAI et les ayants droit. Cette coopération pourrait prendre la forme de mesures de filtrage[39]. Pour compenser, le Parlement européen a introduit les amendements controversés 166 du Rapport Harbour et 138 du Rapport Trautmann[40]. Ces amendements stipulent que les droits des utilisateurs d'accéder aux contenus, services et applications licites de leur choix ne peuvent en aucun cas être restreints sous peine de porter atteinte à leurs droits fondamentaux, notamment la liberté d'expression, et que les restrictions doivent être proportionnelles et requièrent une décision préalable émanant d'une autorité judiciaire. Ces deux amendements ont été écartés par la suite, le premier dans les propositions amendées de la Commission[41] et le second dans l'accord politique du Conseil, tandis que des rumeurs circulent sur leur réintégration dans la période actuelle de préparation à la seconde lecture. Le vote en séance plénière est prévu le 21 avril 2009. S'ils sont adoptés les amendements vont introduire explicitement la liberté d'expression dans le dispositif central des directives UE concernant le filtrage, aux côtés des autres considérations faisant contrepoids.

2. Trouver l'équilibre entre filtrage et liberté d'expression

Dans une récente recommandation[42], le Comité des Ministres du Conseil de l'Europe a attiré l'attention sur le fait que l'usage des méthodes de filtrage sur Internet pourrait constituer une restriction à la liberté d'expression et d'accès à l'information dans l'environnement en ligne. Même en l'absence des amendements du « paquet » Télécom susmentionné, ce risque subsiste dans les directives CE : le considérant 9 de la Directive sur le commerce électronique dispose que « les directives couvrant la fourniture de services de la société de l'information doivent assurer que cette activité peut être exercée librement en vertu de [l'article 10, paragraphe 1, de la CDHL[43]], sous réserve uniquement des restrictions prévues au paragraphe 2 du même article », tandis que la Directive sur le droit d'auteur entend se rapporter au « respect des principes fondamentaux du droit et notamment [...] de la liberté d'expression ». La recommandation du Conseil de l'Europe fait la distinction entre le filtrage obligatoire imposé par l'intervention de l'État et le filtrage des acteurs privés.

Le filtrage résultant d'une intervention de l'État doit toujours être conforme aux exigences de l'article 10 (2) de la CDHL, c'est-à-dire que tout recours au filtrage doit être prescrit par la loi aux fins de satisfaire à l'un des objectifs légitimes énoncés par l'article 10 et pouvoir se justifier dans une société démocratique. Conformément aux lignes directrices de la recommandation en matière de filtrage, il convient, entre autres, de :

(a) recourir au filtrage uniquement pour les raisons exposées à l'article 10. Ces dernières englobent la protection des droits d'autrui et, partant, du droit d'auteur[44]. Le rapport qui sert de base à la recommandation reconnaît expressément que le filtrage peut être utilisé pour bloquer l'accès à des contenus protégés diffusés de façon illicite ;
(b) ne prendre des mesures étatiques de blocage ou de filtrage général que si le filtrage concerne un contenu spécifique et clairement identifiable, une autorité nationale compétente a pris une décision au sujet de l'illégalité de ce contenu et la décision peut être réétudiée par un tribunal ou une entité de régulation indépendant et impartial ;
(c) veiller à ce que les effets du filtrage soient en adéquation avec l'objectif de la restriction[45]. Conformément à la recommandation, cela implique de procéder à l'évaluation de tous les filtres avant et pendant leur mise en œuvre, afin d'éviter tout blocage excessif des contenus.

L'intervention de l'État aura lieu non seulement dans le cadre d'une action des pouvoirs publics directement imputable à l'État, mais aussi lorsque des organismes privés agissent sur instruction de l'État. Ceci englobe le blocage des contenus par un FAI à la suite d'une décision émanant d'une autorité de l'État, ce qui implique qu'une telle décision devrait se conformer aux lignes directrices de la recommandation. Ces lignes directrices semblent suivre la même logique que l'analyse exposée ci-dessus concernant la responsabilité du FAI qui s'abstient de mettre en œuvre un dispositif de filtrage pour empêcher les infractions au droit d'auteur sur ses réseaux et concernant les injonctions imposant une telle obligation. Ainsi, l'instauration *ex ante* d'une obligation de contrôle *a priori* pour les intermé-

diaires en ligne, comme celle qui a été établie dans l'affaire Dailymotion, résulte, semble-t-il, d'un raisonnement juridique douteux vis-à-vis de l'article 10 de la CDHL. En revanche, une ordonnance judiciaire pouvant être attaquée selon les voies de recours habituelles du système judiciaire et selon laquelle un FAI est tenu d'installer une technologie de filtrage, dans le cadre de la législation nationale, afin de bloquer l'accès à un site Web particulier clairement identifiable après avoir constaté un acte illicite de la part dudit site, comme ce fut le cas dans l'affaire danoise DMT2, une telle ordonnance, donc, est conforme aux exigences de la CDHL. La Déclaration sur la liberté de communication sur Internet de 2003 du Conseil de l'Europe confirme par ailleurs cette conclusion en affirmant qu'« à condition que les garanties de l'article 10, paragraphe 2, de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales soient respectées, des mesures peuvent être prises pour supprimer un contenu Internet clairement identifiable ou, alternativement, faire en sorte de bloquer son accès si les autorités nationales compétentes ont pris une décision provisoire ou définitive sur son caractère illicite. »[46]

Mais l'équilibre extérieur entre le droit d'auteur et la liberté d'expression n'est pas le seul élément à fixer des limites au droit d'auteur et, partant, à justifier l'usage de filtres pour prévenir les contrefaçons. Il existe également des mécanismes internes au sein même du corps de la loi sur le droit d'auteur qui garantissent la liberté d'expression par le biais de la doctrine des exceptions et limitations au droit d'auteur[47]. Pour les États membres de l'UE, les exceptions et limitations possibles sont répertoriées de façon exhaustive à l'article 5 de la Directive sur le droit d'auteur. Le considérant 59 de la Directive établit que les titulaires de droits doivent avoir la possibilité de demander qu'une ordonnance sur requête soit rendue à l'encontre d'un intermédiaire, même lorsque les actions de l'intermédiaire font l'objet d'une exception au titre de l'article 5 de la directive. Ainsi, par exemple, le fait qu'un FAI ait copié un contenu protégé de façon provisoire ou fortuite, au sens visé à l'article 5 (1) de la Directive, ne saurait être un argument suffisant pour le protéger d'une ordonnance d'une injonction. Mais que se passe-t-il si les actes des internautes eux-mêmes relèvent du champ de protection de l'article 5 ? Dans l'affaire SABAM, Scarlet avait souligné que « la licéité d'une transmission est une donnée inaccessible à la technique ».

En outre, indépendamment des exceptions et limitations de l'article 5, l'échange en ligne de contenus culturels, par le biais de sites *peer-to-peer* ou d'autres moyens, peut être autorisé, soit parce que l'œuvre elle-même n'est pas protégée (si, par exemple, elle ne remplit pas le critère de l'originalité ou est tombée dans le domaine public), soit parce qu'elle a été placée sous licence. C'est pourquoi la décision préalable d'une autorité compétente attestant de son caractère illicite revêt une importance majeure, puisqu'elle garantit qu'une intervention humaine a lieu dans le processus décisionnel qui mène au blocage. En cas de blocage de l'accès à des sites complets, comme dans l'affaire Pirate Bay, une telle décision garantit également le caractère proportionnel du blocage involontaire de contenus autorisés diffusés de façon licite par rapport à l'objectif poursuivi et, par conséquent, son caractère nécessaire dans une société démocratique. Pour la même raison, l'existence de moyens de recours efficaces et facilement accessibles après le filtrage est essentielle.

Outre l'intervention de l'État ordonnant le filtrage automatique de contenus, les outils de filtrage peuvent également être utilisés sur une base volontaire, aussi bien par les acteurs privés que publics, en vue de limiter l'accès à certains contenus. Ces acteurs peuvent être des individus, par exemple des parents qui souhaitent installer un filtre sur leur connexion Internet pour protéger leurs enfants contre des contenus préjudiciables, ou des institutions du secteur public et privé telles que bibliothèques, universités, établissements scolaires ou entreprises. Cette seconde catégorie est sans doute l'une des plus engagées sur les questions de droit d'auteur : aux États-Unis, par exemple, les universités ont adopté des filtres pour réduire les échanges de fichiers illicites sur leurs réseaux[48]. Ces filtres peuvent être installés au niveau de l'ordinateur personnel ou au niveau institutionnel, au niveau du site Web ou au niveau du fournisseur d'accès Internet[49]. Comme le note le document de travail qui accompagne la recommandation, le filtrage déployé volontairement par les acteurs privés ne relève pas directement de l'article 10 (2) de la CDHL. Toutefois, considérant que l'État, selon la jurisprudence de la Cour européenne des Droits de l'Homme, est « l'ultime garant du pluralisme », c'est toujours à lui qu'incombe la tâche de sauvegarder le principe de la liberté d'expression[50].

La recommandation du Conseil de l'Europe comporte également un certain nombre de règles directrices concernant l'usage volontaire de filtres. Ces règles incitent :

a) à évaluer et à réétudier régulièrement l'efficacité de la mise en place de filtres, et son caractère proportionnel ;
b) à renforcer les informations et les conseils aux utilisateurs, notamment sur l'existence de filtres et les raisons qui peuvent les justifier, ainsi que sur les critères de fonctionnement des filtres ;
c) à coopérer avec les utilisateurs afin d'améliorer la transparence, l'efficacité et le caractère proportionnel des filtres.

En outre, la société civile devrait être encouragée à suivre les développements dans ce domaine et veiller à ce que soit garantie la liberté d'expression des utilisateurs.

L'observation des dernières tendances dans le domaine de l'application des filtres fait apparaître toute l'importance de ce chapitre de la recommandation. Les acteurs privés se tournent de plus en plus vers des solutions techniques d'identification et de régulation, soit comme la meilleure riposte aux allégations de responsabilité, soit dans le cadre des compromis conclus avec les ayants droit et leurs représentants.

© 2009, Observatoire européen de l'audiovisuel, Strasbourg (France)

En fait, la Directive sur le commerce électronique encourage elle-même le développement de ce type d'initiatives : comme indiqué plus haut (paragraphe 1.2.A), le considérant 40 de la directive incite à l'adoption d'accords volontaires négociés entre les parties intéressées afin de permettre « l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible », tout en notant que rien, dans le texte, ne saurait être interprété comme excluant l'usage de dispositifs techniques de filtrage.

3. Une tendance au filtrage volontaire

Quelques jours après la décision du TGI de Paris dans l'affaire Joyeux Noël, Dailymotion a annoncé l'installation sur son site de la technologie d'empreinte d'Audible Magic. En octobre 2007, « Signature », la technologie d'empreinte vidéo de l'Institut national de l'audiovisuel (INA) a également été ajoutée à son arsenal de filtrage. Comme l'a déclaré Dailymotion en 2007 dans un communiqué de presse, « l'utilisation de ces technologies d'identification et de *fingerprinting* s'inscrit dans une stratégie étroite de collaboration avec les créateurs pour proposer un site de partage de vidéos qui protège leurs intérêts[51]. » MySpace utilise également Audible Magic pour identifier les contenus copiés de façon illicite sur son site[52], tandis que Google a installé une technologie de filtrage de son cru sur sa célèbre plateforme d'échange de vidéos YouTube[53]. L'adoption des technologies de filtrage peut être un mécanisme de défense contre l'imputation de responsabilité, une action préventive contre les injonctions ordonnant la mise en place de filtres et, également, une preuve de bonne volonté envers les ayants droit en vue de conclure des accords de licence. De cette façon, les fondations sont posées pour le développement d'un modèle commercial innovant de plateforme de contenus générés par les utilisateurs (UGC), lequel permet d'explorer une version légale de l'utilisation de contenus professionnels attirant les annonceurs que critiquait le TGI de Paris : les ayants droit fournissent les empreintes qui limitent l'apparition des copies illicites de leurs œuvres sur les sites d'hébergement et simultanément, offrent une plus grande visibilité de leurs œuvres au public du fait de la fourniture de contenus licites, tandis que l'intermédiaire attire un public plus large et, partant, des recettes publicitaires plus importantes[54]. Nous sommes loin du scepticisme initial suscité par le considérant 40 de la Directive sur le commerce électronique chez les commentateurs, qui ne voyaient aucune raison pour que les intermédiaires soient enclins à adopter volontairement des dispositifs techniques de protection[55]. Cela renforce également la nécessité d'une attitude d'auto-modération de la part du secteur privé, qui tient compte des problèmes liés à la liberté d'expression, comme le recommandent les lignes directrices du Conseil de l'Europe.

Au-delà de cet « auto-filtrage » adopté en toute indépendance par les sites Internet individuels, des accords volontaires négociés entre les différents secteurs, tels que les préconise la Directive sur le commerce électronique, commencent également à se mettre en place. Aux États-Unis, en octobre 2007, les grands studios de cinéma et de télévision et un certain nombre de sites Internet d'hébergement UGC ont signé une liste de « *Principles for User Generated Content Services* », principes de collaboration librement applicables, axés sur une coopération constructive dans le cadre de l'utilisation des technologies d'identification et de filtrage des contenus[56]. Ces principes prévoient l'installation des outils de filtrage les plus évolués sur les plateformes UGC dans un délai imparti avec une mise à jour régulière, l'objectif étant d'éliminer les contenus frauduleux. Les ayants droit s'engagent à fournir le matériel de référence permettant d'enrichir les bases de données d'empreintes des plateformes, tandis qu'ils renoncent à leur droit de poursuivre les intermédiaires en justice si des infractions subsistent malgré tout. De même, les ayants droit s'engagent à ne pas tenter de soustraire les intermédiaires à leur statut d'exonération de responsabilité en invoquant l'utilisation d'une technologie de filtrage. Bien qu'il s'agisse d'un document d'autorégulation et qu'aucune intervention de l'État sous forme d'évaluation préalable par une autorité publique ou de recours judiciaire consécutif ne soit envisagée, ces principes rappellent les lignes directrices énoncées par le Conseil de l'Europe pour les États membres dans sa recommandation, dans la mesure où ils prévoient :

(a) des garanties visant à limiter les fausses alertes. Ces garanties comprennent un avertissement général pour autoriser les téléchargements intégralement originaux et autorisés et aménager les exceptions et limitations légales au droit d'auteur, de même que des garanties procédurales telles que listes blanches de titulaires de licences autorisés et une option pour un contrôle manuel (humain, mais non judiciaire) ;
(b) un processus permettant de traiter les plaintes litigieuses des ayants droit, concernant les données de référence, et des plaintes des usagers en cas de blocage abusif.

De cette façon, le respect de la liberté d'expression à la fois des ayants droit et des internautes se retrouve en première ligne.

Ces principes ont fait l'objet de critiques du fait de l'absence des deux géants de l'Internet, Google et Facebook. On leur a également reproché d'acculer les intermédiaires sous la menace de procès[57]. D'un point de vue similaire, il est vrai qu'avec « l'auto-filtrage » mentionné plus haut, la principale motivation incitant les intermédiaires à conclure ce type d'accords volontaires basés sur des contreparties réside dans la perspective de réduire les procès. De cette façon, les accords volontaires négociés antre les différents secteurs procurent aux FAI un autre type d' « exonération » : lorsque le refuge n'est plus garanti dans la législation, les FAI érigent leur propre abri sur

la base de l'autorégulation et de stratégies commerciales de « bonnes pratiques » ciblées[58].

La société civile s'active également pour limiter le filtrage en fonction des exigences de la liberté d'expression : aux États-Unis, une coalition d'institutions concernées par la liberté d'expression a proposé une charte complémentaire intitulée « *Fair Use Principles for User Generated Video Content*. » [59] (Principes pour un usage loyal des contenus créés par les utilisateurs). Ces principes réaffirment la nécessité d'intégrer une protection des exceptions et limitations légitimes du droit d'auteur dans tous les logiciels de filtrage, en mettant particulièrement l'accent sur les pratiques de transformation. Cette charte souligne également le fait que «l'humain surpasse la machine », ce qui signifie que le filtrage ne doit pas entraîner un retrait automatique, mais une procédure d'investigation, avec envoi d'un avis à l'usager en lui permettant de contester l'accusation de contrefaçon. Dans la même logique, des moyens informels de surveillance sont également envisagés, notamment sous la forme d'une « *dolphin hotline* » (ligne pour les « dauphins ») qui met en place un « dispositif de secours » pour les « dauphins » loyaux pris dans les filets destinés à capturer les « thons » frauduleux. Cette charte est définie en fonction du principe d'usage loyal des États-Unis et ne peut s'appliquer dans les pays d'Europe que dans la mesure où elle est conforme à la législation nationale en matière de droit d'auteur.

Néanmoins, toutes les considérations exposées ci-dessus concernent uniquement les hébergeurs. Si dans un premier temps, on a pu avoir l'impression que le filtrage allait se généraliser au niveau des FAI, la situation semble maintenant prendre une autre tournure. Le filtrage est effectivement mentionné dans les récents Protocoles d'entente français et britanniques : en novembre 2007, la commission française de lutte contre le piratage sur Internet a présenté le rapport Olivennes[60], résultat d'un accord tripartite entre le gouvernement, les FAI et les ayants droit. Cet accord prévoit la mise en place progressive de technologies de filtrage sur les plateformes de partage de vidéos, avec la collaboration des détenteurs de contenus musicaux et audiovisuels. Néanmoins, il est principalement axé sur l'instauration d'un système de riposte graduée[61], avec l'envoi par une autorité publique de mises en garde aux internautes en infraction, et, en cas de récidive, l'application de sanctions telles que la suspension de l'abonnement Internet. Le parrainage de l'État français signifie que, contrairement aux principes mentionnés précédemment, il est prévu qu'une autorité judiciaire intervienne. Cependant, en l'état actuel des choses, les perspectives de la législation requise pour mettre en place cet accord dépendent de l'issue des débats européens sur la version définitive du paquet Télécom[62]. Entretemps, en juillet 2008, sur la base de la Recommandation 39 du rapport de Gower sur la propriété intellectuelle, commandité en 2005 par le ministère britannique de l'Économie et des Finances pour analyser le cadre britannique de la propriété intellectuelle[63], le Royaume-Uni a suivi la même démarche que la France : à l'initiative du gouvernement, un protocole d'entente[64] a été signé entre les principaux ayants droit, le service public et les FAI, afin d'enrayer les échanges illicites de fichiers en ligne par une méthode de corégulation. Ce protocole d'entente fait état du filtrage et propose que les signataires envisagent cette solution, mais le pilier central du protocole est une fois de plus le système de riposte graduée. En fait, le document de consultation d'accompagnement[65] ne mentionne le filtrage que dans le chapitre « *Other Options to be Considered* » (Autres options à envisager), en cas d'échec de la corégulation, qui reste la solution privilégiée.

Le régime de la riposte graduée est en pleine expansion : l'Italie semble également désireuse de suivre le « modèle français »[66] et en janvier 2009, un accord inédit a été conclu en Irlande entre les détenteurs de contenus et le fournisseur d'accès irlandais Eircom. Les éditeurs musicaux avaient lancé la procédure en demandant qu'Eircom soit contraint d'installer un dispositif de filtrage sur ses réseaux. Mais l'accord s'est finalement orienté vers l'instauration d'une réponse graduée[67]. Outre-Atlantique, la Recording Industry Association of America (association interprofessionnelle de l'industrie du disque américaine - RIAA) a adopté une stratégie similaire et selon toute évidence, la Motion Picture Association of America (association interprofessionnelle de l'industrie du cinéma américain – MPAA) va s'orienter dans la même direction[68]. Un élément susceptible de fournir une explication sur ce retournement tactique nous est proposé par la consultation publique sur les contenus créatifs en ligne lancée par la Commission européenne : dans leurs réponses, les parties intéressées se montrent souvent sceptiques quant à la possibilité technique de filtrer le trafic général sur Internet, alors que, parallèlement, les FAI sont réticents à installer ce type de logiciels, de crainte de voir leurs services réseaux se dégrader. Enfin, le critère de connaissance de l'article 14 sur les services d'hébergement n'apparaît pas à l'article 12 visant le simple transport ; étant donné que dans les affaires Dailymotion et Tranquility Bay, l'établissement de la responsabilité, fondé sur le défaut d'installation d'un filtre, dépend de l'interprétation restrictive du terme « apparent », ce raisonnement, même s'il est correct, ne peut s'appliquer dans le cas des FAI. Si l'on considère que la situation n'est toujours pas clarifiée en ce qui concerne la faisabilité ou la licéité d'une technologie de filtrage intelligente et modulable, ce revirement est probablement judicieux. On notera avec intérêt que le Gouvernement britannique met en garde contre toute mesure législative impulsive, tout en pressentant que les filtres « peuvent très bien faire partie d'une solution, mais qu'ils ne sont certainement pas la panacée »[69].

Conclusion

Les dispositions de la Directive sur le commerce électronique prêtent elles-mêmes à des interprétations contradictoires. Les exonérations sont censées exclure l'engagement de

© 2009, Observatoire européen de l'audiovisuel, Strasbourg (France)

la responsabilité des intermédiaires du fait d'un défaut de filtrage, or les interprétations discutables des tribunaux ont conduit à une stricte application de la condition de connaissance, laquelle est déterminante pour la responsabilité des intermédiaires. Les injonctions prononcées à l'encontre des intermédiaires pour leur imposer l'utilisation d'un logiciel de filtrage se multiplient, alors qu'elles exigent une navigation prudente dans les eaux troubles des dispositions du préambule de la Directive. Pourtant, les contours de recevabilité des filtres imposés par l'État, tels qu'ils émergent de la Directive, coïncident, pour la plupart, avec ceux qui découlent des exigences de la liberté d'expression : les filtres ne peuvent être imposés que dans certains cas spécifiques, afin de bloquer des contenus dont le caractère illicite a été établi par une autorité publique et uniquement lorsque les moyens de contrôle sont facilement accessibles.

Les axes définis par les codes de conduite interprofessionnels volontaires suivent la même orientation. Cependant, le recours volontaire aux applications de filtrage automatique semble se limiter actuellement aux sites d'hébergement sur Internet. Au niveau des FAI, la tendance actuelle semble s'écarter des solutions de filtrage. Le système de « riposte graduée » est aujourd'hui le mot d'ordre sur toutes les lèvres. Par conséquent, si les solutions de filtrage ont de l'avenir, il semblerait que, pour le moment, le présent s'en passe.

---

1) Deibert, R. et al., *Access Denied - The Practice and Policy of Global Internet Filtering*, (*MIT Press*, 2007) et J Zittrain, *The Future of the Internet and How to Stop It* (*Penguin Books*, Londres 2008).
2) Cho, C., Feldman A. & Heins M., *Internet Filters – A Public Policy Report* (2e éd., *Brennan Center for Justice at NYU School of Law*) 2006, disponible sur : tinyurl.com/dneu22
3) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (Directive sur le commerce électronique), [2000] JO L 178/1.
4) Conseil de l'Europe, *Rapport du Groupe de spécialistes sur les droits de l'homme dans la société de l'information (MC S IS) sur l'utilisation et l'impact des mesures de filtrage technique pour divers types de contenus dans l'environnement numérique*, CM(2008)37, disponible sur : tinyurl.com/adyzoz
5) Rossenhövel, C. *Peer-to-Peer Filters: Ready for Internet Prime Time?* (Internet Evolution), disponible sur : tinyurl.com/64dp68
6) Voir la réponse d'Audible Magic Corporation à la consultation publique sur les contenus créatifs en ligne lancée par la Commission européenne, disponible sur : tinyurl.com/3cw4mq ; *U.S. House of Representatives, Committee on Science and Technology*, *The Role of Technology in Reducing Illegal Filesharing: A University Perspective* (*Hearing Charter*, 5 juin 2007), disponible sur : tinyurl.com/cteczv
et Horten, M., *Deep Packet Inspection, Copyright and the Telecoms Package*, disponible sur : tinyurl.com/bvj6av
7) NdT : « *To monitor* » dans le texte original. Voici la définition de *l'Oxford English Dictionary* : « a. *To check or regulate the technical quality of (a sound recording, radio transmission, television signal, etc.) without causing any interruption or disturbance; […] b. To listen to and report on (radio broadcasts, esp. from a foreign country). Also: to eavesdrop on (a telephone conversation). […] c. gen. To observe, supervise, or keep under review; to keep under observation; to measure or test at intervals, esp. for the purpose of regulation or control.* »
8) *Digital Millennium Copyright Act*, pub. L. n°. 105-304, 112 Stat. 2860 (1998) § 512 (i).
9) Koelman, K.J., *Online Intermediary Liability*, dans PB Hugenholtz (éd.) *Copyright and Electronic Commerce - Legal Aspects of Electronic Copyright Management*, (*Information Law Series* (n° 8), *Kluwer Law International* 2000) 34.
10) *Jean Yves L. dit Lafesse c. Myspace,* tribunal de grande instance de Paris, ordonnance de référé 22 juin 2007, disponible sur : tinyurl.com/bdpm3a. Une décision ultérieure a été rendue depuis par la cour d'appel, qui porte principalement sur des questions de procédure (voir *MySpace Inc c. Jean-Yves L dit Lafesse, SARL L Anonyme, Monsieur Daniel L, Monsieur Hervé L* CA Paris, 29 octobre 2008, disponible sur : tinyurl.com/dcgmpk).
11) *Tiscali Media c. Dargaud Lombard, Lucky Comics,* cour d'appel de Paris (4e chambre, section A) arrêt du 7 juin 2006, disponible sur : tinyurl.com/b3hk7q
12) En France, par exemple, en vertu de l'article 42 de la Loi du 29 juillet 1881 sur la liberté de la presse, l'éditeur d'un contenu imprimé ou audiovisuel est, en principe, tenu responsable dès lors qu'une infraction est constatée, tandis que, conformément au système de responsabilité en cascade en vigueur, l'auteur du texte illicite peut être considéré responsable au titre de complice ou, uniquement en l'absence d'un éditeur, responsable à titre exclusif. Par conséquent, l'éditeur est tenu de prévenir l'apparition même de toute activité illicite au premier chef. Ces règles ont été appliquées aux hébergeurs avant l'introduction de la Directive sur le commerce électronique (voir *Estelle H. c. Valentin L. et Daniel L.*, Tribunal de grande instance de Paris, Ordonnance de référé du 9 juin 1998, disponible sur : tinyurl.com/bvkxmx).
13) *Christian C., Nord Ouest Production c. Dailymotion, UGC Images,* tribunal de grande instance de Paris (3e chambre, 2e section) jugement du 13 juillet 2007, disponible sur : tinyurl.com/chv9lq
14) En fait, cette conclusion a été confirmée par plusieurs décisions, à tel point que cette question semble être réglée en France ; voir par exemple Courtinat, A., *Succès d'actions persistantes d'un humoriste contre les sites de partage de vidéos*, disponible sur : tinyurl.com/cc9gcf et Blocman, A., *Le TGI de Paris confirme le statut d'hébergeur de Dailymotion*, disponible sur : tinyurl.com/b5rdso
15) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
16) Jondet, N. *The Silver Lining in Dailymotion's Copyright Cloud*, disponible sur : ssrn.com/abstract=1134807
17) *SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud c. Sté Google Inc. et AFA,* tribunal de grande instance de Paris (3e chambre, 2e section), jugement du 19 octobre 2007, disponible sur : tinyurl.com/dbyyk6
18) Hardouin, R. *Observations sur les nouvelles obligations prétoriennes des hébergeurs*, disponible sur : tinyurl.com/cdomwd
19) Jondet, N. *Google Video held liable for the copyright infringement of "Tranquility Bay"* (TGI de Paris 19 octobre 2007), disponible sur : tinyurl.com/d79nvy

20) Cabrera Blázquez, F.J. *Les plateformes de contenus générés par l'utilisateur et le droit d'auteur*, IRIS *plus* 2008-5, Observatoire européen de l'audiovisuel.
21) Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (Directive sur le droit d'auteur) [2001] JO L167/10.
22) Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle [2004] JO L 157/45.
23) P. van Eecke & B. Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11(4) J. Internet L. 3.
24) *SABAM c. SA Scarlet (anciennement Tiscali)*, tribunal de première instance de Bruxelles, 29 juin 2007, disponible sur : tinyurl.com/avnvj2
25) *SA Scarlet c. SABAM*, tribunal de première instance de Bruxelles, 22 octobre 2008.
26) *SA Scarlet Extended c. SABAM*, tribunal de première instance de Bruxelles, n° 07/15472/A, 22 octobre 2008.
27) Tribunale di Bergamo, *Sezione penale del dibattimento in funzione di giudice del riesame, ordinanza 24 Settembre 2008*, disponible sur : tinyurl.com/48j2ow
28) Arena, A. *Les juridictions italiennes interdisent Pirate Bay, puis lèvent cette même interdiction*, IRIS 2008-10 : 13, disponible sur : merlin.obs.coe.int
29) *IFPI Danmark mod DMT2 A/S, Frederiksberg Byrets kendelse af 29.januar 2008*.
30) Sandfeld Jacobsen, S. *Injonction de restriction faite en vertu du droit danois aux fournisseurs d'accès Internet*, IRIS 2008-6 : 7, disponible sur : merlin.obs.coe.int
31) Euractiv, *New EU Battle over Copyright Rules in Sight*, 30 janvier 2009, disponible sur : tinyurl.com/d4kweh.
32) van Hoboken, J., *L'incidence de la liberté d'expression sur la gouvernance des outils de recherche*, IRIS *Spécial*, *La recherche de contenus audiovisuels*, Observatoire européen de l'audiovisuel, 2008.
33) Valgaeren, E. & Roland, N., *YouTube et les plateformes de contenus créés par les utilisateurs – nouveaux acteurs ?* IRIS *Spécial*, *Les aspects juridiques de la vidéo à la demande*, Observatoire européen de l'audiovisuel, 2007.
34) Rapport de la Commission du 30 novembre 2007 SEC(2007) 1556, disponible sur : tinyurl.com/awo7gr
35) Rapport du Parlement européen sur le droit d'auteur dans l'Union européenne, INI/2008/2121, disponible sur : tinyurl.com/cgqfuy
36) Résolution du Parlement européen sur les industries culturelles en Europe, INI/2007/2153, disponible sur : tinyurl.com/djvoaj
37) Angelopoulos, C., *Première lecture du nouveau « paquet » Télécom*, IRIS 2008-10 : 4 et *Conseil de l'Union européenne : Nouvelles propositions législatives pour la réforme des télécommunications*, IRIS 2009-1 : 5, disponible sur : merlin.obs.coe.int
38) Résolution législative du Parlement européen du 24 septembre 2008, COM(2007)0698 – C6-0420/2007 – 2007/0248(COD), disponible sur : tinyurl.com/6qwfxc
39) Les amendements rejetés du rapport Bono mentionnaient explicitement le filtrage comme un exemple de coopération des FAI.
40) Résolution législative du Parlement européen du 24 septembre 2008, COM(2007)0697 – C6-0427/2007 – 2007/0247(COD), disponible sur : tinyurl.com/63t5pn
41) Commission, *Commission proposes a single European Telecoms Market for 500 million consumers*, disponible sur : tinyurl.com/d7nsb2
42) Recommandation CM/Rec(2008)6 du Comité des Ministres aux États membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet, 26 mars 2008, disponible sur : tinyurl.com/cna63u
43) Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (Convention européenne des droits de l'homme dans sa version amendée) (signée le 4 juin 1950 et entrée en vigueur le 3 septembre 1953).
44) Hugenholtz, P.B., *Copyright and Freedom of Expression in Europe*, dans Dreyfuss R. et al. (éd.), *Expanding the Boundaries of Intellectual Property. Innovation Policy for the Knowledge Society*, (Oxford University Press, New York 2001) 343-363.
45) Voir note 4 ci-dessus.
46) Comité des ministres du Conseil de l'Europe, *Déclaration sur la liberté de la communication sur Internet*, 28 mai 2003, disponible sur : http://tinyurl.com/cpb6o6. Voir également : Thórhallsson, P. *Déclaration sur la liberté de la communication sur Internet*, IRIS 2003-7 : 3, disponible sur : merlin.obs.coe.int
47) Barendt, E. *Freedom of Speech* (2e éd., OUP, New York 2005) 247.
48) Voir la réponse d'Audible Magic Corporation à la consultation, disponible sur : tinyurl.com/3cw4mq
49) Voir note 4 ci-dessus.
50) *Informationsverein Lentia c. l'Autriche*, (aff. n° 13914/88; 15041/89; 15717/89; 15779/89; 17207/90) CEDH 24 novembre 1993.
51) DailyMotion, *Dailymotion choisit la solution de fingerprinting d'Audible Magic pour détecter les vidéos protégées par des droits*, (13 juillet 2007) disponible sur : tinyurl.com/bqnkoc
52) Stone, B., Helft, M., *New Weapon in Web War Over Piracy*, *The New York Times*, 19 février 2007, disponible sur : tinyurl.com/38f527
53) BBC, *YouTube Rolls out Filtering Tools*, 16 octobre 2007, disponible sur : tinyurl.com/byb42n
54) Voir note 16 ci-dessus.
55) Voir note 9 ci-dessus et Julia-Barcelo, R., *On-Line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks* 22(3) EIPR 105.
56) *Principles for User Generated Content Services*, disponible sur : www.ugcprinciples.com
57) *The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance*, 121 *HarvLRev* 1387.
58) Ginsburg, J.C., *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, disponible sur : tinyurl.com/dxwjtn
59) *Fair Use Principles for User Generated Video Content*, disponible sur : tinyurl.com/demshm
60) Accord pour le développement et la protection des œuvres et programmes culturels sur les nouveaux réseaux, disponible sur : tinyurl.com/2k73mn
61) En anglais, ce système est appelé *three strikes (and you're out)*.
62) Courtinat, A., *La riposte graduée selon le projet de loi Création et Internet*, IRIS 2008-10 : 10, disponible sur : merlin.obs.coe.int
63) HM Treasury, *Gower's Review of Intellectual Property*, novembre 2006, disponible sur : tinyurl.com/7xnsvn.
64) *Joint Memorandum of Understanding on an Approach to Reduce Unlawful File-Sharing*, disponible sur : tinyurl.com/abed4x
65) *Department for Business, Enterprise and Regulatory Reform* (BERR), *Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing*, juillet 2008, disponible sur : tinyurl.com/5pxy6l
66) *Italy to Follow French Three Strikes Model for P2P*, 22 janvier 2009, disponible sur : tinyurl.com/cusoca
67) *Downloaders face disconnection following Eircom settlement*, *The Irish Times*, 28 janvier 2009, disponible sur : tinyurl.com/d45a3y
68) McBride S., Smith, E., *Music Industry to Abandon Mass Suits*, *The Wall Street Journal*, disponible sur : tinyurl.com/4h9omj
69) Voir les réponses de Microsoft, Google, EuroISPA et du Royaume-Uni à la consultation, disponible sur : tinyurl.com/3cw4mq

© 2009, Observatoire européen de l'audiovisuel, Strasbourg (France)