

UNIVERSITÉ DE VERSAILLES-SAINT QUENTIN
FACULTÉ DE DROIT

MÉMOIRE DE MASTER 2 DROIT DES NOUVELLES TECHNOLOGIES
DE L'INFORMATION ET DE LA COMMUNICATION

**Le rôle des intermédiaires techniques dans la prévention et la cessation
des atteintes aux droits de propriété intellectuelle sur Internet.**



Réalisé par [Gaëtan Bourdais \(contact@gaetanbourdais.com\)](mailto:contact@gaetanbourdais.com)

Sous la direction de Monsieur Ronan Hardouin

ANNÉE UNIVERSITAIRE 2012-2013

À mes parents

REMERCIEMENTS

Je tiens à remercier Monsieur Ronan HARDOUIN pour m'avoir permis d'accomplir cette réflexion et d'avoir toujours répondu avec célérité et pertinence à mes interrogations.

Je remercie également Madame le professeur Valérie-Laure BENABOU pour nous avoir enseigné l'importance de revenir à la lettre des textes et d'en faire soi-même l'exégèse.

Je remercie enfin Maître Brad SPITZ, du cabinet YS AVOCATS, pour m'avoir permis de trouver le temps nécessaire au correct achèvement de ce mémoire.

«– Ne faudrait-il pas recommencer tous les jours ?

– Je recommencerais.

– Ce serait l'histoire de l'hydre de Lerne.»

Charles de Bernard, La Chasse aux amants

SOMMAIRE

INTRODUCTION.....	8
TITRE I. LA POSSIBILITÉ D'ENJOINDRE AUX INTERMÉDIAIRES TECHNIQUES DE PRÉVENIR ET FAIRE CESSER UNE ATTEINTE À DES DROITS DE PROPRIÉTÉ INTELLECTUELLE	12
Chapitre 1. L'interdiction d'imposer aux intermédiaires techniques une obligation générale de surveillance pour prévenir et faire cesser une atteinte à des droits de propriété intellectuelle.....	12
Section 1. Les raisons de l'interdiction d'une obligation générale de surveillance.....	12
A. Les considérations économiques justifiant l'interdiction d'une obligation générale de surveillance.....	12
§1. La justification de l'interdiction par les rédacteurs de la directive Commerce électronique.....	12
§2. La pertinence de la justification de nos jours.....	14
B. Les considérations juridiques justifiant l'interdiction d'une obligation générale de surveillance.....	16
Section 2. La nécessité d'équilibrer protection de la propriété intellectuelle et libertés fondamentales.....	17
A. La nécessaire conciliation de la propriété intellectuelle avec les droits fondamentaux.....	18
B. Les libertés fondamentales prises en compte par la CJUE.....	21
§1. La nécessité de ne pas porter atteinte aux libertés fondamentales des intermédiaires techniques.....	22
§2. La nécessité de ne pas porter atteinte aux libertés fondamentales des internautes.....	23
a. La nécessité de ne pas porter atteinte à la protection des données à caractère personnel.....	23
b. La nécessité de ne pas porter atteinte à la liberté de recevoir ou de communiquer des informations.....	25
Chapitre 2. La possibilité d'imposer aux intermédiaires techniques une obligation particulière de surveillance pour prévenir et faire cesser une atteinte à des droits de propriété intellectuelle.....	26
Section 1. La possibilité pour le juge d'imposer une obligation particulière de surveillance à un intermédiaire technique.....	26
A. Les fondements des obligations particulières de surveillance permettant de prévenir ou faire cesser une atteinte à des droits de propriété intellectuelle.....	26
§1. Les dispositions générales issues de la directive Commerce électronique.....	26
§2. Les dispositions propres à la propriété intellectuelle.....	28
B. Les contours de l'obligation particulière de surveillance.....	29

§1. La recherche d'une définition de la notion de généralité.....	29
§2. L'insécurité juridique née de l'absence de définition.....	31
Section 2. L'appréciation par le juge des obligations de surveillance imposées aux intermédiaires techniques.....	31
A. Les critères retenus par la CJUE.....	32
§1. La durée de la surveillance.....	34
§2. L'étendue de la surveillance.....	34
§3. Le public visé par la surveillance.....	35
§4. Le coût de la surveillance.....	38
§5. La surveillance préventive.....	39
B. Les critères retenus par la Cour de Cassation.....	40
§1. L'état de la jurisprudence avant les arrêts du 12 juillet 2012.....	41
§2. L'apport des arrêts du 12 juillet 2012.....	42
CONCLUSION DU TITRE I.....	43
TITRE II. LA RESPONSABILITÉ DE L'INTERMÉDIAIRE TECHNIQUE SUITE À LA MISE EN PLACE DE MESURES TECHNIQUES DESTINÉES À PRÉVENIR ET FAIRE CESSER UNE ATTEINTE À DES DROITS DE PROPRIÉTÉ INTELLECTUELLE.....	44
Chapitre 1. La compatibilité des mesures de surveillance ciblée avec le régime de responsabilité des intermédiaires techniques.....	44
Section 1. Les risques de la mise en place de mesures de filtrage sur le bénéfice du régime de responsabilité des intermédiaires.....	44
A. La mesure de filtrage au regard de la définition du service de la société de l'information.....	44
B. La mesure de filtrage au regard de la neutralité de l'intermédiaire technique.....	45
Section 2. La nécessaire compatibilité des mesures de filtrage avec le régime de responsabilité des intermédiaires techniques.....	47
A. Le filtrage imposé par le juge : une possibilité conforme à la directive.....	47
B. Le filtrage volontaire : une possibilité laissée par la directive.....	47
Chapitre 2. La responsabilité de l'intermédiaire technique en cas de défaillance des mesures de filtrage.....	49
Section 1. La responsabilité de l'intermédiaire technique à l'égard des ayants droit.....	49
A. Une responsabilité de l'intermédiaire technique possible.....	49
§1. Une responsabilité draconienne pour l'intermédiaire technique.....	49

a. L'impossibilité de mettre en place un filtrage parfait.....	49
b. L'impossibilité de déterminer un filtrage acceptable.....	50
§2. Une responsabilité dépassant les compétences de l'intermédiaire technique.....	51
B. Une responsabilité de l'intermédiaire technique contre-productive.....	52
§1. Une responsabilité de l'intermédiaire devant être limitée à une obligation de moyen.....	52
§2. Une collaboration nécessaire des ayants droit pour la mise en place d'un système de filtrage.....	52
a. Une collaboration technique nécessaire.....	53
b. Une collaboration pouvant prendre la forme de charte.....	53
Section 2. La responsabilité de l'intermédiaire technique à l'égard des internautes.....	55
A. Une responsabilité de l'intermédiaire technique possible.....	56
§1. Le risque de «faux positif».....	56
§2. Le risque d'atteinte à la liberté d'expression et de la communication.....	57
B. La nécessité d'intégrer l'internaute dans la décision de blocage.....	57
§1. Un droit de réponse pour l'internaute.....	58
§2. Un renforcement du rôle neutre de l'intermédiaire technique.....	58
CONCLUSION DU TITRE II.....	59
CONCLUSION GÉNÉRALE.....	60
BIBLIOGRAPHIE.....	62

INTRODUCTION

Internet est un lieu propice pour «*commettre aisément toute une série d'infractions aux droits de la propriété intellectuelle*». ¹ La poursuite de leurs auteurs s'apparente à un vain combat notamment du fait de leur localisation dans le monde, de leur anonymat sur le réseau, ou de leur maigre solvabilité. ²

Bien plus aisé est de s'adresser aux personnes qui proposent des services de la société de l'information permettant indirectement de commettre ces atteintes pour les faire cesser. C'est ce que permet la directive 2000/31/CE 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*» ³, en prévoyant un régime de responsabilité spécial dérogeant du droit commun pour les intermédiaires techniques. Ce terme d'intermédiaire recoupe divers acteurs de la société de l'information : fournisseurs d'accès, fournisseur de cache, hébergeurs de contenus. Ainsi, les hébergeurs de contenus ne peuvent voir leur responsabilité engagée que si, ayant eu la connaissance d'un contenu manifestement illicite, ils n'ont pas agi promptement pour le retirer.

Les intermédiaires techniques collaborent aisément aux demandes de retrait de contenus illicites qui leurs sont adressées par les ayants droit. Pourtant, la lutte contre la contrefaçon des œuvres de l'esprit sur Internet que mènent ces derniers s'apparente au mythe de Sisyphe. Le professeur Laure Marino souligne fort bien les faiblesses du système de notification à travers la métaphore du ping-pong : «*Ping, les internautes postent des vidéos protégées par des droits d'auteur sans autorisation des ayants droit ; les sociétés d'auteur adressent alors des notifications à l'hébergeur, lequel retire les vidéos. Pong, les internautes repostent. Ping, les sociétés d'auteur re-notifient et l'hébergeur retire à nouveau les vidéos. Pong, les internautes re-postent...*». ⁴

La réapparition du contenu illicite est d'ailleurs souvent sans commune mesure avec la première publication litigieuse, du fait de ce qu'il convient d'appeler sur Internet l'effet Streisand ⁵, à savoir un «*phénomène qui se manifeste par l'augmentation considérable de la diffusion d'informations ou de documents par le simple fait d'avoir été l'objet d'une tentative de retrait ou de censure*». ⁶ Cette situation donne aux défenseurs de la propriété intellectuelle le sentiment de se retrouver à combattre l'Hydre de Lerne.

¹ Rapport sur l'application de la directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, COM(2010) 779 final , 22 décembre 2010, page 7 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:FR:PDF>.

² CASTETS-RENARD Céline, «Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet», *Recueil Dalloz* 2012, p. 827.

³ Nous désignerons ci-après cette directive comme la directive «Commerce électronique».

⁴ MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 18 octobre 2012, n°292, p. 12.

⁵ Pour une illustration jurisprudentielle de ce phénomène, voir les observations sous *TGI Paris, réf. 10 février 2012* de SAINT MARTIN (de) Axel, «Blocage de contenus illicites et fournisseurs d'accès - Précisions sur le principe de subsidiarité», *RLDI* 2012/82, n°2745.

⁶ Définition donnée par le site français de Wikipédia, http://fr.wikipedia.org/wiki/Effet_Streisand.

De cette réalité naît pourtant quelques espérances avec les solutions techniques qui semblent permettre un contrôle sur les contenus transitant sur Internet. Il s'agit ici, à proprement parlé, des mesures de filtrage et de blocage.

Il convient au préalable de distinguer ces deux mesures techniques. Utilisé dans un sens commun, «filtrer» et «bloquer» peuvent vouloir désigner le même résultat d'un processus visant à empêcher la circulation ou la publication d'un contenu. Pourtant ces deux mesures, quoique intimement liées l'une à l'autre, désignent chacune une opération technique différente.

Pour Maître Alexandra Neri, le filtrage consiste à «contrôler l'ensemble des informations transférées ou stockées par les intermédiaires (...) afin de détecter celles qui contiennent des objets protégés par des droits de propriété intellectuelle et sont dès lors susceptibles de porter atteinte aux dits droits».⁷ La mesure de filtrage sert donc à identifier des contenus recherchés par l'intermédiaire technique afin de les «isoler»⁸. S'agissant de la mesure de blocage, le même auteur considère qu'elle «est censée (...) empêcher la transmission et le stockage des informations identifiées lors du filtrage comme pouvant porter atteinte à des droits de propriété intellectuelle».⁹

Ainsi, comme le note Monsieur Cédric Manara, «le filtrage peut être vu comme le fait d'immerger un filet, et le blocage d'en choisir la dimension des mailles afin d'attraper tel ou tel type de poisson».¹⁰

Toutefois, l'emploi du mot «filtrage» peut être entendu dans une acception large pour désigner l'ensemble du processus de filtrage et de blocage : «le premier objectif du filtrage d'Internet est d'empêcher un contenu d'atteindre un ordinateur personnel ou un poste informatique, à l'aide d'un produit logiciel ou matériel dont la fonction est de surveiller l'ensemble des communications Internet et de déterminer s'il y a lieu d'empêcher la réception et/ou l'affichage de contenus spécifiquement ciblés».¹¹

Ces mesures de filtrage et de blocage ne sauraient toutefois être observées que par le tropisme de la technique. Leur existence est, d'un point de vue politique, fortement contestée.

A cet égard, la définition qu'en donne, non sans humour, le Professeur Laure Marino témoigne de la passion que peut animer cette question : «Filtrage (de l'internet) : mot magique, sésame qui déclenche les passions. Il est la solution à tous les maux de la Toile pour certains, il est le masque de la censure pour les autres».¹²

⁷ NERI Alexandra, «L'injonction de filtrage rendue à l'égard d'un intermédiaire : une mesure controversée aux conséquences redoutables», *Communication Commerce Électronique*, n°1; janvier 2012, étude 3.

⁸ Sur les mesures de filtrage et de blocage, voir les Conclusions de l'Avocat Général M. Pedro Cruz Villalón dans l'affaire C-70/10, CJUE 24 novembre 2011, «Scarlet / SABAM», §46.

⁹ NERI Alexandra, *ibid.*

¹⁰ MANARA Cédric, «Bloquer le filtrage ! Une approche critique des affaires Sabam», *RLDI* 2011/76, n°2533.

¹¹ CALLANAN C., GERCKE M., DE MARCO E., DRIES-ZIEKENHEINER H., «Rapport Filtrage d'Internet : Equilibrer les réponses à la cybercriminalité dans une société démocratique», Octobre 2009, p. 10 <http://www.juriscom.net/documents/lib20100520.pdf>.

¹² MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 16 février 2012, n°47, p. 14.

Cette question du filtrage de l'Internet est effectivement «*au coeur d'un débat à l'échelle planétaire*»¹³, notamment en ce qu'elle s'oppose au principe de neutralité¹⁴, inhérent à l'idéologie du réseau. Il faut en outre souligner le rôle important de ces intermédiaires techniques «*en tant que secteur d'activité économique distinct et en tant que moyen de transport fondamental pour d'autres activités économiques*»¹⁵, faisant d'eux de véritables acteurs économique et social de l'Internet.¹⁶

Observons en outre que le filtrage ne concerne pas uniquement les questions de protection de la propriété intellectuelle, auxquelles nous consacrons la présente étude, mais qu'elle s'inscrit aussi dans la lutte d'autres phénomènes relevant de la cybercriminalité. A ce titre, on peut imaginer un filtrage des contenus (pédo)pornographiques, des contenus racistes¹⁷ ou d'autres contenus illégaux.¹⁸

Ainsi, aux États-Unis, les projets de loi «*SOPA*»¹⁹ et «*PIPA*»²⁰, qui prévoyaient notamment pour renforcer la protection de la propriété intellectuelle sur Internet des mesures de filtrage et de blocage, ont été fortement contestés — justifiant pour partie leur mise en sommeil — à la fois par des citoyens²¹, des associations²² et des acteurs importants de l'Internet.²³ L'exemple le plus parlant fut le black-out du site

¹³ TROIANIELLO Antonino, «La CJUE s'oppose au filtrage généralisé de l'internet», *RLDI* 2012/78, n°2613.

¹⁴ Wu. T. «Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High Technology Law*, 2003, Vol 2, p. 141 et s. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863###).

¹⁵ Accords OMC, Annexe sur les télécommunications, article 1 http://www.wto.org/french/tratop_f/serv_f/12-tel_f.htm.

¹⁶ L'OCDE relève dans son rapport « Le rôle économique et social des intermédiaires de l'Internet » du 30 juin 2010 que « *les intermédiaires de l'Internet mettent en contact des tierces parties ou facilitent des transactions entre elles sur l'Internet. Ils rendent accessibles, hébergent, transmettent et indexent sur l'Internet des contenus, produits et services provenant de tierces parties ou fournissent à des tiers des services reposant sur l'Internet* ».

¹⁷ Sur la question du filtrage des contenus à caractère raciste et la complexité de leur détection automatique, on renverra aux recherches de Monsieur Mathieu VALETTE, «Détection et interprétation automatique de contenus illicites et préjudiciables sur Internet» : http://faculty.arts.ubc.ca/winder/me/linguistique_du_corpus/Valette_PRINCIP.html.

¹⁸ Pour un aperçu des autres contenus non mentionnés que l'on peut filtrer (spam, sujets politiques, jeux d'argent en ligne illégaux, diffamation, contenus publiés par des organisations terroristes, etc.), CALLANAN C., GERCKE M., DE MARCO E., DRIES-ZIEKENHEINER H., *ibid*.

¹⁹ «*SOPA*» désigne «*Stop Online Piracy Act*». Ce projet de loi est consultable en ligne <http://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih>.

²⁰ «*PIPA*» désigne «*PROTECT IP ACT*», abréviation de «*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*». Ce projet de loi est consultable en ligne <http://www.gpo.gov/fdsys/search/pagedetails.action?packageId=BILLS-112s968rs>.

²¹ Le 18 janvier 2012, 2,4 millions de tweets relatifs au projet SOPA furent publiés sur Twitter.com (NETBURN Deborah, «Wikipedia : SOPA protest led 8 million to look up reps in Congress», Los Angeles Times, 19 janvier 2012 <http://latimesblogs.latimes.com/technology/2012/01/wikipedia-sopa-blackout-congressional-representatives.html>).

Également, le sénateur Ron Wyden rapportait que le Congrès avait reçu environ 14 millions de messages pour protester contre le projet PIPA (WEISMAN Jonathan, «After an Online Firestorm, Congress Shelves Antipiracy Bills», The New York Times, 20 janvier 2012 http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=0).

²² Le site American Censorship (<http://americancensorship.org/>), soutenu par les fondations Mozilla, Free Software Foundation, Creative Commons, Wikimedia, organisait le 16 novembre 2011 l'«American Censorship Day» pour dénoncer les projets PIPA et SOPA.

²³ Le moteur de recherche Google masqua son fameux logo d'une bannière noire (Doodle SOPA/PIPA visible ici <http://www.google.com/doodles/sopa-pipa>) et publia un article «Don't censor web» sur son blog officiel (<http://googleblog.blogspot.fr/2012/01/dont-censor-web.html>).

Wikipedia.com, rendu indisponible durant toute la journée d'opposition à ces projets de loi, le 18 janvier 2012.²⁴

Le débat existe également en Europe, avec toutefois moins de virulence qu'outre-Atlantique. Ainsi, la Commission dans la conclusion de son rapport du 22 décembre 2010 sur l'application de la directive n°2004/48/CE du 29 avril 2004 «*relative au respect des droits de propriété intellectuelle*»²⁵, relève que si «*le défi posé par l'internet par rapport à l'application des droits de propriété intellectuelle n'était pas entré en ligne de compte lors de l'élaboration de la directive*» et qu' «*un certain nombre de questions pourraient mériter un examen plus approfondi*»²⁶ elle souligne qu'«*il convient d'équilibrer soigneusement les différents intérêts*».

En France, le rapport de la Mission «*Acte II de l'exception culturelle*», dit rapport *Lescure*, remis le 10 mai 2013 au Président de la République, invite à «*promouvoir, à l'échelle européenne, une réflexion d'ensemble sur le rôle des intermédiaires de l'Internet dans la prévention et la cessation des comportements délictueux ou criminels sur Internet*».²⁷ Ce même rapport, dans ces développements sur la responsabilité des hébergeurs, souligne qu'«*une refonte globale du statut de l'hébergeur n'est ni souhaitable ni nécessaire*».²⁸

Effectivement, l'arsenal de textes tant internes que communautaires est de nature à permettre la mise en place de mesures de filtrage. Toutefois, celles-ci doivent nécessairement se concilier avec l'interdiction d'imposer une surveillance générale aux intermédiaires techniques. Se pose ici la délicate question de savoir comment prévenir la réapparition d'un contenu violant des droits de propriété intellectuelle sans imposer à un intermédiaire technique une obligation générale de surveillance (TITRE I). S'il est possible de mettre en place des mesures de surveillance ciblée il conviendra également de s'interroger quant à savoir si ces mesures de surveillance ciblée mises en place par l'intermédiaire technique sont de nature à affecter sa responsabilité (TITRE II).

²⁴ Pour plus d'informations sur cette action, voir la page Wikipedia «Protests against SOPA and PIPA» http://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA#Wikimedia_community.

²⁵ Rapport du 22 décembre 2010 sur l'application de la directive n° 2004/48/CE du 29 avril 2004 «*relative au respect des droits de propriété intellectuelle*», consultable en ligne <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:FR:PDF>.

²⁶ Le rapport de la Commission, (page 10) cite alors «*l'utilisation des mesures provisoires et conservatoires telles que les injonctions*», permettant d'imposer des mesures de type filtrage-blocage.

²⁷ Rapport de la Mission «Acte II de l'exception culturelle», tome I, proposition n°62, page 477 <http://www.culturecommunication.gouv.fr/content/download/67145/514833/file/Rapport%20Lescure%20498.pdf>.

²⁸ *Ibid*, page 399.

TITRE I. LA POSSIBILITE D'ENJOINDRE AUX INTERMEDIAIRES TECHNIQUES DE PREVENIR ET FAIRE CESSER UNE ATTEINTE À DES DROITS DE PROPRIETE INTELLECTUELLE

Quoique les textes communautaires et internes posent l'interdiction d'imposer aux intermédiaires techniques une obligation générale de surveillance pour prévenir ou faire cesser une atteinte aux droits de propriété intellectuelle (Chapitre 1), il reste possible de leur imposer une obligation particulière de surveillance (Chapitre 2).

Chapitre 1. L'interdiction d'imposer aux intermédiaires techniques une obligation générale de surveillance pour prévenir et faire cesser une atteinte à des droits de propriété intellectuelle

La directive Commerce électronique pose comme principe l'interdiction d'imposer aux intermédiaires techniques une obligation générale de surveillance : *«les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée 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 révélant des activités illicites»*.²⁹

Les raisons de l'interdiction d'imposer une obligation générale de surveillance (Section 1) justifient la nécessité d'équilibrer, dans les activités de surveillance, la protection de la propriété intellectuelle avec les libertés fondamentales (Section 2).

Section 1. Les raisons de l'interdiction d'une obligation générale de surveillance

L'interdiction de l'obligation générale de surveillance posée par la directive Commerce électronique se justifie tant par des considérations économiques (A) que par des considérations juridiques (B).

A. Les considérations économiques justifiant l'interdiction d'une obligation générale de surveillance

Si les considérations économiques ont justifié, pour les rédacteurs de la directive Commerce électronique l'interdiction de l'obligation générale de surveillance (§1), on peut s'interroger sur la pertinence de celles-ci de nos jours (§2).

§1. La justification de l'interdiction par les rédacteurs de la directive Commerce électronique

La justification de l'interdiction de l'obligation générale de surveillance découle de l'objet même de la directive Commerce électronique. Son intitulé exact, *«directive relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur»*³⁰ indique que son objet tend à la réalisation du marché intérieur. Cet objectif est d'ailleurs rappelé dans le premier³¹ considérant de la directive et le second considérant souligne les opportunités économiques du

²⁹ Article 15 § 1 de la directive Commerce électronique.

³⁰ Nous soulignons.

³¹ Considérant premier de la directive Commerce électronique : *«L'Union européenne vise à établir des liens toujours plus étroits entre les États et les peuples européens et à assurer le progrès économique et social. Conformément à l'article 14, paragraphe 2, du traité, le marché intérieur comporte un espace sans frontières intérieures dans lequel la libre circulation des marchandises et des services ainsi que la liberté d'établissement sont assurées. Le développement des services de la société de l'information dans l'espace sans frontières intérieures est un moyen essentiel pour éliminer les barrières qui divisent les peuples européens»*.

commerce électronique.³² Comme le relève le Professeur Laure Marino, «*la directive sur le commerce électronique instrumentalise la technique juridique au profit d'un objectif économique de libre circulation des services de la société de l'information*»³³ ce qui ressort d'ailleurs du huitième considérant³⁴ de la directive.

A la lumière de cet objectif s'explique tant le régime de responsabilité *ob favorem* pour les intermédiaires techniques que l'interdiction de l'obligation générale de surveillance. De telles dispositions permettent d'abord pour ces intermédiaires techniques de ne pas devoir mettre en place des dispositifs de surveillance extrêmement contraignants — sinon impossibles à mettre en place. Ensuite, elles limitent le risque juridique d'être condamné et de devoir payer des dommages et intérêts. Ces dispositions sont de nature à rassurer les acteurs de l'Internet.

La clarification des droits et des obligations de ces acteurs de l'Internet était heureuse si l'on s'intéresse à la jurisprudence française de l'époque. Ainsi, dans une affaire «*Valentin Lacambre c/ Estelle Hallyday*»³⁵, la Cour d'appel de Paris avait condamné le représentant légal de l'hébergeur Altern, Valentin Lacambre, pour un contenu posté par un internaute portant atteinte à la vie privée d'Estelle Hallyday.

L'arrêt retenait «*qu'en offrant, comme en l'espèce, d'héberger et en hébergeant de façon anonyme, sur le site ALTERN.ORG qu'il a créé et qu'il gère toute personne qui, sous quelque dénomination que ce soit, en fait la demande aux fins de mise à disposition du public ou de catégories de publics, de signes ou de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondances privées, Valentin LACAMBRE excède manifestement le rôle technique d'un simple transmetteur d'informations et doit, d'évidence, assumer à l'égard des tiers aux droits desquels il serait porté atteinte dans de telles circonstances, les conséquences d'une activité qu'il a, de propos délibérés, entrepris d'exercer dans les conditions susvisées et qui, contrairement à ce qu'il prétend, est rémunératrice et revêt une ampleur que lui-même revendique*».³⁶

L'affaire avait fait grand bruit à l'époque de l'élaboration de la directive Commerce électronique et avait notamment fait réagir le ministre de l'économie de l'époque — Dominique Strauss-Khan — dans un e-mail adressé à Valentin Lacambre. Il écrivait notamment que «*les incertitudes sur les modalités précises d'application du droit peuvent créer un sentiment d'instabilité juridique qui peut générer des dépenses importantes pour les entreprises. Ces coûts peuvent être particulièrement lourds pour les PME/PMI qui n'ont*

³² Considérant second de la directive Commerce électronique : «*Le développement du commerce électronique dans la société de l'information offre des opportunités importantes pour l'emploi dans la Communauté, en particulier dans les petites et moyennes entreprises. Il facilitera la croissance économique des entreprises européennes ainsi que leurs investissements dans l'innovation, et il peut également renforcer la compétitivité des entreprises européennes, pour autant que tout le monde puisse accéder à l'Internet*».

³³ MARINO Laure, «Le fabuleux destin de la responsabilité des hébergeurs, à propos des arrêts Dailymotion et autres», *Resp. civ. et assur.* n°6, Juin 2011, étude 8.

³⁴ Considérant huit de la directive Commerce électronique : «*L'objectif de la présente directive est de créer un cadre juridique pour assurer la libre circulation des services de la société de l'information entre les États membres et non d'harmoniser le domaine du droit pénal en tant que tel*».

³⁵ CA Paris 10 février 1999 Estelle H. c/ Valentin L.

³⁶ Pour un commentaire de l'arrêt, voir THOUMYRE Lionel, «Le mannequin et l'hébergeur», <http://lthoumyre.chez.com/pro/1/resp19990225.htm>.

pas toujours les structures ou les moyens pour supporter ces dépenses. Le cas d'altern.org en est une illustration».³⁷

C'est donc la volonté de ne pas faire peser sur les intermédiaires techniques une surveillance, nécessairement technique³⁸, qui en raison de son coût représenterait une barrière économique, qui explique cette interdiction de l'obligation générale de surveillance.

Toutefois, on peut s'interroger si la question du coût prohibitif d'une telle surveillance serait aujourd'hui encore pertinente.

§2. La pertinence de la justification de nos jours

Adoptée le 8 juin 2000, la directive Commerce électronique a été réfléchiée et rédigée notamment en considération des possibilités techniques existantes à l'époque. Or, l'évolution rapide de la technique fait aujourd'hui apparaître ces préoccupations comme antédiluviennes par rapport aux technologies existantes pour détecter des contenus illicites. Cette constatation transparait notamment dans un document de travail de la Communication de la Commission européenne du 11 janvier 2012 où la question est abordée en ces termes : « (...) *one can imagine that if filtering techniques had become flawless and costless, the need for a prohibition on imposing a general monitoring obligation would have become obsolete* ». ³⁹

Il existe de nos jours diverses technologies permettant d'identifier des contenus pouvant violer des droits de propriété intellectuelle. Sans que l'énumération soit exhaustive, on peut citer Audible Magic⁴⁰, Signature⁴¹, Content ID⁴², Gracenote⁴³, BayTSP⁴⁴ : elles utilisent la technologie de l'empreinte numérique pour détecter des contenus similaires circulant sur le réseau.

Il convient toutefois d'observer que si ces technologies tendent à se généraliser, elles sont avant tout utilisées par des acteurs importants de l'Internet. La démocratisation de leur implémentation doit donc être

³⁷ Message E-mail de Dominique Strauss-Kahn à Monsieur Valentin Lacambre, 25 février 1999 <http://altern.org/alternb/defense/Strauss-Kahn.html>.

³⁸ Sur le fait qu'un contrôle humain soit illusoire, voir HARDOUIN Ronan, «Fascicule 464 : La responsabilité des intermédiaires techniques de l'internet», Lamy droit des médias et de la communication 2012, §464-116.

³⁹ Nous traduisons : « On peut imaginer que si les techniques de filtrage étaient devenues parfaites et gratuites, la nécessité d'une interdiction d'imposer une obligation générale de surveillance serait devenue obsolète », «A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services», 11 janvier 2012, SEC(2011) 1641 final, page 50 http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.

⁴⁰ Audible Magic est la technologie de filtrage de contenu vidéo notamment utilisé par Dailymotion. <http://audiblemagic.com/>.

⁴¹ Signature est une technologie de filtrage de contenu vidéo, développée par l'Institut National de l'Audiovisuel pour son catalogue et commercialise une version licence pour des tiers. <http://www.institut-national-audiovisuel.fr/en/products-services/signature.html>.

⁴² Content ID est une technologie de filtrage de contenu vidéo utilisée par YouTube. <http://www.youtube.com/t/contentid>.

⁴³ Gracenote est notamment utilisé par iTunes pour identifier la musique ajoutée sur ce logiciel par un utilisateur. <http://www.gracenote.com/>.

⁴⁴ BayTSP est une technologie de filtrage utilisée pour identifier des contenus violant les droits d'auteur. <http://irdeto.com/>.

relativisée et on peut s'interroger sur leur accessibilité pour les acteurs de taille moindre dans notre réflexion sur l'obsolescence ou non de la barrière économique que ces technologies représentent.

On peut dans cette démarche citer le professeur Pierre Sirinelli qui, à propos du Rapport de la commission CSPLA «Prestataires de l'Internet»⁴⁵ qu'il présidait, fait remarquer que « *la réflexion conduite au sein de cette enceinte avait montré, d'une part, que les coûts de réalisation des empreintes et de l'implémentation des systèmes de reconnaissance – pour réels qu'ils soient – n'étaient pas dirimants* ». ⁴⁶ Cet enthousiasme est à relativiser dans la mesure où ces techniques d'empreintes s'appliquent principalement aux contenus audios et vidéos.⁴⁷

Toutefois, peu importe que le coût de l'implémentation de tels systèmes de reconnaissance soit dirimant ou non avec pour objectif de rechercher des contenus violant les droits de la propriété intellectuelle. En effet, la directive Commerce électronique a vocation à s'appliquer à l'égard de tous les prestataires fournissant un service de la société de l'information, notion qui, de l'aveu du législateur européen, « *[englobe] un large éventail d'activités économiques qui ont lieu en ligne* ». ⁴⁸

Ainsi, la directive opte pour une approche transversale consistant à appréhender de manière globale⁴⁹ la responsabilité des intermédiaires techniques, peu importe la nature du délit. On peut noter que c'est une approche autre que celle retenue par les Etats-Unis (approche verticale) où le DMCA⁵⁰ n'a trait qu'au droit d'auteur. Que cette solution satisfasse ou non⁵¹, les possibilités techniques que l'on peut envisager pour la protection de la propriété intellectuelle ne sont pas substituables aux autres phénomènes illicites.⁵²

En outre, les considérations économiques que nous avons précédemment développées ne sont pas les seules à justifier l'interdiction d'une obligation générale de surveillance.

⁴⁵ CSPLA, Commission spécialisée sur les prestataires de l'Internet, rapport du 4 juillet 2008.

⁴⁶ SIRINELLI Pierre, Chronique de jurisprudence, RIDA, oct. 2012, p. 465.

⁴⁷ A contrario, on peut donner l'exemple des oeuvres littéraires enregistrées dans un format PDF dit «aplati» qui affiche le texte sous forme d'image et ne permet pas le fonctionnement d'un filtrage textuel, comme le note la Communication de la Commission européenne du 11 janvier 2012, *op. cit.* plus spécialement page 51.

⁴⁸ Considérant 18 de la directive Commerce électronique. On peut noter que la notion de «*service de la société de l'information*» avait été introduite par la directive 98/34/CE comme étant «*tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services*».

⁴⁹ Notons toutefois qu'est exclu du champ de la directive Commerce électronique les activités de jeux d'argent (Considérant 16).

⁵⁰ Digital Millennium Copyright Act (DMCA), 28 octobre 1998, consultable en ligne <http://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf>.

⁵¹ On peut ici noter certains auteurs qui regrettent qu'une approche verticale n'ait pas été retenue : «*Quoi qu'on dise, ce n'est pas la même chose de pourchasser les pédophiles, racistes ou négationnistes et de faire respecter la propriété intellectuelle en général et le droit d'auteur en particulier...*» A. et H.-J. Lucas, Traité de la propriété littéraire et artistique : Litec, 3e éd. 2006, n° 980, p. 687.

⁵² S'agissant, par exemple, des contenus racistes, on renverra aux observations de Monsieur Ronan HARDOUIN dans le «Fascicule 464 : La responsabilité des intermédiaires techniques de l'internet», Lamy droit des médias et de la communication 2012, §464-118 citant notamment les recherches de Monsieur Mathieu VALETTE, «Détection et interprétation automatique de contenus illicites et préjudiciables sur Internet» : http://faculty.arts.ubc.ca/winder/me/linguistique_du_corpus/Valette_PRINCIP.html.

B. Les considérations juridiques justifiant l'interdiction d'une obligation générale de surveillance

Au delà des considérations économiques, les considérations juridiques semblent bien plus être en mesure de justifier cette interdiction d'imposer une obligation générale de surveillance aux intermédiaires techniques.

L'interdiction posée à l'article 15 de la directive Commerce électronique doit d'abord s'observer comme le corollaire du régime de «*responsabilité aménagée*»⁵³ créé par les articles 12, 13 et 14 de la directive Commerce électronique, à savoir que les intermédiaires techniques, qu'ils soient fournisseurs d'accès, fournisseurs de cache ou hébergeurs «*ne peuvent voir leur responsabilité engagée dès lors qu'ils s'en tiennent à [leur] rôle, et ne sont pas à l'origine de la circulation de contenus illicites, ou n'en ont pas le contrôle, ou encore font de leur mieux pour les retirer dès qu'ils en ont connaissance*». ⁵⁴ Or, ne pas interdire que les États membres puissent imposer à ces intermédiaires techniques une obligation de surveillance générale conduirait simplement à court-circuiter le mécanisme de notification.⁵⁵

De manière plus générale, tant l'absence d'obligation de surveillance générale que le régime de responsabilité aménagée s'expliquent par le fait que les intermédiaires techniques jouent un rôle vital dans la société de l'information. L'OCDE, dans son rapport du 30 juin 2010 sur «*Le rôle économique et social des intermédiaires de l'Internet*» le soulignait fort bien : «*les intermédiaires de l'Internet mettent en contact des tierces parties ou facilitent des transactions entre elles sur l'Internet. Ils rendent accessibles, hébergent, transmettent et indexent sur l'Internet des contenus, produits et services provenant de tierces parties ou fournissent à des tiers des services reposant sur l'Internet* ». ⁵⁶

Les intermédiaires techniques se situent donc à la croisée des chemins des communications électroniques. Dans une société démocratique, l'attente à leur égard est qu'ils n'exercent pas d'influence intellectuelle sur les contenus transmis.

Cette neutralité⁵⁷ est un gage de l'exercice des libertés fondamentales sur Internet car elle assure que les communications électroniques transitant sur le réseau ne fassent l'objet d'aucune discrimination. En

⁵³ La formule est celle du professeur François Terré, «Etre ou ne pas être... responsable : à propos des prestataires de services par internet», JCP 2011. I. 1175.

⁵⁴ MANARA Cédric, «Bloquer le filtrage ! Une approche critique des affaires *Sabam*», *RLDI* 2011/76, n°2533.

⁵⁵ Monsieur Cédric MANARA parle de «*neutralisation du mécanisme de notification*», *ibid.* et Messieurs Étienne MONTERO et Quentin VAN ENIS relèvent quant à eux que «*L'intérêt des exonérations de responsabilité instituées — sous conditions — au bénéfice des prestataires intermédiaires auraient été réduit pratiquement à néant si celles-ci n'avaient été complétées par le principe d'interdiction de toute obligation générale de surveillance*», «Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'internet : la quadrature du cercle ?», *RLDI* 2010/60, n°2028.

⁵⁶ Rapport consultable en ligne, <http://www.oecd.org/fr/internet/ieconomie/45847774.pdf>.

⁵⁷ Voir sur le sujet, Wu. T. «Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High Technology Law*, 2003, Vol 2, p. 141 et s. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863###) • On peut observer que les hypothèses de filtrage ne sont envisagés que comme des exceptions au principe de neutralité et se justifie au regard de finalités purement techniques, propres au réseau (p. 169 et 170).

cela, elle «favorise l'exercice des libertés fondamentales telles la liberté d'expression, la liberté du commerce et de l'industrie ou encore la liberté d'accès au réseau». ⁵⁸

L'interdiction d'une obligation générale de surveillance peut effectivement avoir des effets vertueux sur la liberté du commerce et de l'industrie et ce d'une double façon. Premièrement, libérés d'une obligation contraignante, les intermédiaires techniques peuvent diversifier leurs services mais aussi voir le nombre de personnes proposant de tels services augmenter, au bénéfice de la société de l'information. Deuxièmement, l'interdiction peut aussi contraindre les intermédiaires techniques à rester neutres, c'est-à-dire à éviter de la part de ces derniers des excès de zèle dans la recherche d'activités illicites. L'hypothèse n'est pas farfelue si l'on considère le fait que ces intermédiaires techniques tendent de plus en plus à diversifier leurs activités, ne se contentant plus uniquement de servir de contenant mais aussi de servir du contenu. ⁵⁹ L'effet d'une obligation générale de surveillance aurait alors un effet potentiellement anti-concurrentiel. Les intermédiaires techniques en situation de position dominante pourraient ainsi épargner aux contenus qu'ils proposent les mesures de filtrage qui, au contraire, impacteraient ceux de leurs concurrents. Ces mesures pouvant avoir pour effet négatif de bloquer ou ralentir la communication de ces contenus.

L'interdiction d'une obligation générale de surveillance favorise également la liberté d'expression en ce que les contenus circulent librement. La règle nous apparaît servir la société de l'information, notamment si l'on imagine ce qu'il en aurait été autrement : «*Sans doute n'aurait-on pas pu voir émerger et fleurir autant les sites communautaires et participatifs, tels les réseaux sociaux (Facebook...), wikis (Wikipédia...), et blogs, les sites de partage de contenus (Youtube, Dailymotion...) ou encore les places de marché électronique (eBay...)*». ⁶⁰

Le souci de protéger les libertés fondamentales justifie donc pour partie la raison de l'interdiction d'une obligation de surveillance générale. La protection de la propriété intellectuelle suppose alors de trouver un équilibre avec ces libertés fondamentales, ce que rappelle régulièrement la Cour de Justice de l'Union Européenne.

Section 2. La nécessité d'équilibrer protection de la propriété intellectuelle et libertés fondamentales

Si l'on veut exiger des intermédiaires techniques qu'ils veillent au respect de la propriété intellectuelle, cela suppose de se conformer aux libertés fondamentales qui peuvent être affectées par ces mesures de prévention et de cessation. La jurisprudence de la CJUE a déjà pu souligner que l'exercice requiert de mettre en place un savant équilibre entre la protection intellectuelle et ces libertés fondamentales (A). La Cour de Justice a d'ailleurs eu l'occasion, en matière de système de filtrage, d'identifier les libertés fondamentales qui sont alors en jeu (B).

⁵⁸ HARDOUIN Ronan, «Fascicule 464 : La responsabilité des intermédiaires techniques de l'internet», Lamy droit des médias et de la communication 2012, §464-119.

⁵⁹ Illustration de ce phénomène, l'entrée de la société Orange au capital de Deezer.com, service d'écoute de musique à la demande. Voir : «*Orange va investir dans Deezer et le fusionner avec son site Wormee*», Les Echos n°20724, 22 juillet 2010, p. 11 http://www.lesechos.fr/22/07/2010/LesEchos/20724-67-ECH_orange-va-investir-dans-deezer-et-le-fusionner-avec-son-site-wormee.htm.

⁶⁰ MONTÉRO Étienne & VAN ENIS Quentin, «Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'internet : la quadrature du cercle ?», RLDI 2010/60, n°2028, p 87.

A. La nécessaire conciliation de la propriété intellectuelle avec les droits fondamentaux

La propriété intellectuelle jouit d'une protection non négligeable en droit de l'Union européenne puisque celle-ci est inscrite au paragraphe 2 de l'article 17 («*Droit de propriété*») de la Charte des droits fondamentaux de l'Union européenne : «*La propriété intellectuelle est protégée*». ⁶¹ Cette Charte, adoptée à Nice le 7 décembre 2000 et entrée en vigueur avec le traité de Lisbonne du 1er décembre 2009, bénéficie de la même force obligatoire qu'un traité. La jurisprudence ne saurait ignorer pareil principe aussi concis. Soulignons toutefois le truisme de la Cour de Justice qui prend soin de bien préciser que «*les droits de propriété intellectuelle, tels que le droit d'auteur, [...] font partie du droit de propriété*». ⁶² Érigée en droit fondamental, la propriété intellectuelle siège donc au plus haut niveau de la hiérarchie des normes européennes.

Pour autant, la protection reconnue à la propriété intellectuelle n'est pas absolue mais doit partager son trône avec les autres droits fondamentaux. La Cour de Justice de l'Union Européenne a déjà eu l'occasion de l'affirmer, dans une affaire «*Promusicae*» ⁶³, où il était question de la conciliation de droits fondamentaux à savoir, d'une part, le droit au respect de la vie privée et, d'autre part, la protection de la propriété intellectuelle (ainsi qu'au droit à un recours effectif). ⁶⁴ La Cour avait alors pu considérer qu'il incombe «*aux autorités et aux juridictions nationales, dans le cadre des mesures adoptées pour protéger les titulaires des droits d'auteur, d'assurer un juste équilibre entre la protection de ce droit et celle des droits fondamentaux des personnes qui sont affectées par de telles mesures*». ⁶⁵ La recherche de ce juste équilibre fut également rappelée par la Cour de Luxembourg dans une affaire «*Padawan*». ⁶⁶

⁶¹ Charte des droits fondamentaux de l'Union européenne consultable en ligne http://www.europarl.europa.eu/charter/pdf/text_fr.pdf.

⁶² CJCE 2 septembre 2006, *Laserdisken*, C-479/04, point 65
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=63876&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=289148>.

⁶³ CJCE, 29 janv. 2008, aff. C-275/06 «*Promusicae*».

⁶⁴ Voir plus spécialement les points 62 à 68 de l'arrêt *Promusicae* sur la conciliation des droits fondamentaux qu'effectue la CJCE.

⁶⁵ Point 68 de l'arrêt *Promusicae*.

⁶⁶ CJUE, 21 octobre 2010, aff. C-467/08, «*Padawan*». La Cour de Justice s'appuyait sur le considérant 31 de la directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information qui dispose qu'«*Il convient de maintenir un juste équilibre en matière de droits et d'intérêts entre les différentes catégories de titulaires de droits ainsi qu'entre celles-ci et les utilisateurs d'objets protégés*».

Plus récemment encore, la CJUE prit soin de souligner cet impératif dans les affaires «*Sabam c/ Scarlet*»⁶⁷ et «*Sabam c/ Netlog*»⁶⁸, particulièrement riches d'enseignements pour notre étude.

Dans son arrêt du 24 novembre 2011, la Cour était saisie à propos d'une mesure de filtrage demandée par la Société belge des auteurs, compositeurs et éditeurs (SABAM), laquelle avait demandé au tribunal de première instance de Bruxelles d'enjoindre au fournisseur d'accès Scarlet de mettre en place un système de filtrage des communications électroniques de type *peer-to-peer* afin de déceler et de bloquer les échanges de fichiers portant atteintes aux droits des auteurs que celle-ci représente. Si le tribunal de première instance accueillit favorablement la demande de la SABAM, la juridiction d'appel fit preuve quant à elle de plus de retenue et posa une double question préjudicielle à la Cour de Justice :

«1) Les directives 2001/29 et 2004/48, lues en combinaison avec les directives 95/46, 2000/31 et 2002/58, interprétées notamment au regard des articles 8 et 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales⁶⁹, permettent-elles aux États membres d'autoriser un juge national, saisi dans le cadre d'une procédure au fond et sur la base de la seule disposition légale prévoyant que: '[i] [les juges nationaux] peuvent également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou à un droit voisin, à ordonner à un [FAI] de mettre en place, à l'égard de toute sa clientèle, in abstracto et à titre préventif, aux frais exclusifs de ce FAI et sans limitation dans le temps, un système de filtrage de toutes les communications électroniques, tant entrantes que sortantes, transitant par ses services, notamment par l'emploi de logiciels 'peer-to-peer', en vue d'identifier sur son réseau la circulation de fichiers électroniques contenant une œuvre musicale, cinématographique ou audiovisuelle sur laquelle le demandeur prétend détenir des droits et ensuite de bloquer le transfert de ceux-ci, soit au niveau de la requête soit à l'occasion de l'envoi ?

2) En cas de réponse positive à la [première] question [...], ces directives imposent-elles au juge national, appelé à statuer sur une demande d'injonction à l'égard d'un intermédiaire dont les services sont utilisés par

⁶⁷ CJUE 24 novembre 2011, affaire C-70/10 «SABAM / Scarlet», voir notamment les commentaires de BENABOU Valérie-Laure, «Chroniques», *Propriétés Intellectuelles*, Janvier 2012, n°42, p. 47 ; CASTETS-RENARD Céline, «Protection du droit d'auteur confrontée aux droits fondamentaux : point trop n'en faut !», *RLDI* 2012/79, n°2622 ; COSTES Lionel, «Affaire Sabam : l'analyse de la CJUE», *RLDI* 2011/77, n°2541 ; DEBET Anne, «Des limites strictes posées au filtrage des contenus sur Internet par la CJUE», *Communication Commerce Électronique*, n°6, Juin 2012, comm. 63 ; DERIEUX Emmanuel, «Filtrage par les FAI - Opposition aux obligations générales de filtrage imposées aux fournisseurs d'accès à internet», *RLDI* 2012/78, n°2611 ; DERIEUX Emmanuel, «Fournisseurs d'hébergement - Impossible obligation générale mais possibles obligations particulières de surveillance et de filtrage», *RLDI* 2012/81, N°2699 ; FRANCILLON Jacques, «Téléchargement illégal d'oeuvres protégées par un droit d'auteur...», *Revue de science criminelle*, 2012 p. 163 ; GUTHFREUND-ROLAND Florence & MARRACHE Élisabeth, «Arrêt Sabam : requiem pour "Hadopi 3" ?», *RLDI* 2012/78, n°2614 ; MANARA Cédric, «Le droit du commerce électronique après l'arrêt Scarlet», *RLDI* 2012/78, n°2612 ; MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 16 février 2012, n°47, p. 14 ; NERI Alexandra, «L'injonction de filtrage rendue à l'égard d'un intermédiaire : une mesure controversée aux conséquences redoutables», *Communication Commerce Électronique*, n°1, janvier 2012, étude 3 ; PETIT Cécile, «Google, une obligation de surveillance proportionnée ?», *Recueil Dalloz*, 2012, p. 2071 ; TROIANELLO Antonino, «La CJUE s'oppose au filtrage généralisé de l'internet», *RLDI* 2012/78, n°2613.

⁶⁸ CJUE 16 février 2012, affaire C-360/10 «SABAM / Netlog», voir notamment les commentaires de DEBET Anne, «Des limites strictes posées au filtrage des contenus sur Internet par la CJUE», *Communication Commerce Électronique*, n°6, Juin 2012, comm. 63 ; MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 2 août 2012, n°215, p. 11.

⁶⁹ Nous soulignons.

un tiers pour porter atteinte à un droit d'auteur, d'appliquer le principe de proportionnalité⁷⁰ lorsqu'il est amené à se prononcer sur l'efficacité et l'effet dissuasif de la mesure demandée ?»

Avant de juger que la mesure de filtrage était contraire — ce qui fera l'objet d'observations approfondies de notre part au prochain chapitre — la CJUE rappelle que la protection de la propriété intellectuelle est «certes consacrée»⁷¹ par la Charte des droits fondamentaux de l'Union européenne mais que «cela étant, il ne ressort nullement de cette disposition, ni de la jurisprudence de la Cour, qu'un tel droit serait intangible et que sa protection devrait donc être assurée de manière absolue».⁷²

La même précision fut développée dans l'arrêt du 16 février 2012. L'affaire «SABAM / Netlog» est pour ainsi dire la sœur jumelle de la précédente, tant dans les faits que dans la solution apportée par la CJUE.⁷³ En effet, là où l'affaire *Scarlet* concernait un fournisseur d'accès, l'affaire *Netlog* concernait un hébergeur auquel la SABAM avait demandé au président du tribunal de première instance de Bruxelles d'imposer un filtrage similaire à l'hébergeur *Netlog* à savoir l'obligation pour ce dernier de cesser immédiatement toute mise à disposition illicite sur son réseau social des oeuvres musicales ou audiovisuelles du répertoire de SABAM. Le tribunal de grande instance questionna préjudiciellement la CJUE sur le point de savoir si «les directives 2001/29 et 2004/48, lues en combinaison avec les directives 95/46, 2000/31 et 2002/58, interprétées notamment au regard des articles 8 et 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales [signée à Rome, le 4 novembre 1950], permettent-elles aux États membres d'autoriser un juge national, saisi dans le cadre d'une procédure au fond et sur la base de la seule disposition légale prévoyant que [les juges nationaux] peuvent également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par des tiers pour porter atteinte au droit d'auteur ou à un droit voisin, à ordonner à un prestataire de services d'hébergement de mettre en place, à l'égard de toute sa clientèle, in abstracto et à titre préventif, à ses frais et sans limitation dans le temps, un système de filtrage de la plus grande partie des informations stockées sur ses serveurs, en vue d'y repérer des fichiers électroniques contenant des œuvres musicales, cinématographiques ou audiovisuelles sur lesquelles SABAM prétend détenir des droits et d'en bloquer ensuite l'échange ?».

La solution tranchée dans l'affaire *Netlog* se situe dans la continuité de l'affaire *Scarlet* puisque qu'elle juge dans une formule identique que «la protection du droit de propriété intellectuelle est certes consacrée à l'article 17, paragraphe 2, de la charte des droits fondamentaux de l'Union européenne (...). Cela étant, il ne ressort nullement de cette disposition, ni de la jurisprudence de la Cour, qu'un tel droit serait intangible et que sa protection devrait donc être assurée de manière absolue»⁷⁴ et de rappeler la jurisprudence *Promusicae* selon laquelle «il incombe aux autorités et aux juridictions nationales, dans le

⁷⁰ Nous soulignons.

⁷¹ Point 43 de l'arrêt *Scarlet*.

⁷² Point 43 de l'arrêt *Scarlet*.

⁷³ Le professeur Laure MARINO relève en outre que «La similarité justifie même que l'arrêt *Netlog* n'ait pas été précédé des conclusions de l'avocat général et qu'il multiplie les références à l'arrêt *Scarlet*». «Chronique de jurisprudence», *Gaz. Pal.* 2 août 2012, n°215, p. 11

Soulignons en outre qu'il est fait référence dans cet arrêt, par quinze fois, à l'arrêt *Scarlet*.

⁷⁴ Point 41 de l'arrêt *Netlog*.

cadre des mesures adoptées pour protéger les titulaires de droits d'auteur, d'assurer un juste équilibre entre la protection de ce droit et celle des droits fondamentaux de personnes qui sont affectées par de telles mesures»⁷⁵ ce qu'en l'espèce, le filtrage litigieux ne permet pas.

La recherche de ce juste équilibre doit donc s'apprécier au regard de diverses libertés fondamentales, toutes identifiées par la CJUE, ce qu'il convient d'étudier présentement.

B. Les libertés fondamentales prises en compte par la CJUE

Dans les affaires *Scarlet* et *Netlog*, la CJUE analyse dans un premier temps les modalités nécessaires pour que les dispositifs de filtrage souhaités par la SABAM soient mis en place⁷⁶, puis affirme que dans les deux cas, ceux-ci conduiraient à imposer aux intermédiaires techniques une obligation générale de surveillance prohibée par l'article 15 de la directive 2000/31/CE.⁷⁷ Dans un même trait de plume, la Cour de Justice se livre à un profond examen des libertés fondamentales que de tels dispositifs de filtrage ébranleraient.

La Cour de Justice remplit certes là sa mission, les demandes de décision préjudicielle dans ces affaires portant toutes deux sur l'interprétation des directives 2000/31/CE (Commerce électronique)⁷⁸, 2001/29/CE (Droit d'auteur et Droits voisins)⁷⁹, 2004/48/CE (Respect des droits de propriété intellectuelle)⁸⁰, 95/46/CE (Données personnelles)⁸¹ et 2002/58/CE (Vie privée et communications électroniques).⁸² Toutefois, elle donne l'impression de justifier son appréciation du caractère général de la mesure de surveillance sollicitée au regard des libertés fondamentales que celle-ci vient malmener. Ce n'est pas tant les modalités du filtrage litigieux qui conduisent à ce que l'on soit en présence d'une obligation générale de surveillance. C'est, à notre sens, les conséquences que porteraient ces modalités sur les libertés

⁷⁵ Point 43 de l'arrêt *Netlog*.

⁷⁶ S'agissant de l'arrêt *Scarlet*, points n°38 et 39 et s'agissant de l'arrêt *Netlog*, points n°36 et 37.

⁷⁷ S'agissant de l'arrêt *Scarlet*, point n°40 et s'agissant de l'arrêt *Netlog*, point n°38.

⁷⁸ 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 (JO L 178, p. 1) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML>.

⁷⁹ 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 (JO L 167, p. 10) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:FR:NOT>.

⁸⁰ Directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle (JO L 157, p. 45, et rectificatif JO L 195, p. 16) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:01:FR:HTML>.

⁸¹ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, p. 31) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>.

⁸² Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JO L 201, p. 37) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML>.

individuelles qui justifient aussi, pour partie, que la mesure soit prononcée incompatible avec les dispositions de l'article 15 de la directive Commerce électronique.⁸³

D'où l'examen minutieux par la CJUE des libertés fondamentales mises à mal dans pareil cas. On doit ici souligner la façon toute singulière qu'à la CJUE d'effectuer son contrôle de proportionnalité. En effet, elle ne raisonne non point *in abstracto*, opposant principe contre principe, mais bien *in concreto*, recherchant quels impacts produiraient le système de filtrage litigieux. En l'espèce, la Cour de Justice retient dans les affaires *SABAM* que les systèmes de filtrage litigieux porteraient atteinte à la liberté d'entreprise, au droit de la protection des données à caractère personnel ainsi qu'à la liberté de recevoir ou de communiquer des informations.

Ce faisant, la Cour de Justice entend protéger tant les libertés fondamentales des intermédiaires techniques (§1) que celles des internautes (§2).

§1. La nécessité de ne pas porter atteinte aux libertés fondamentales des intermédiaires techniques

La CJUE relève dans les affaires *Scarlet* et *Netlog* que «*les autorités et les juridictions nationales doivent notamment assurer un juste équilibre entre la protection du droit de propriété intellectuelle, dont jouissent les titulaires de droits d'auteur, et celle de la liberté d'entreprise dont bénéficient les [intermédiaires techniques] en vertu de l'article 16 de la charte*». ⁸⁴ Or celle-ci semblait compromise en l'espèce, du fait que le coût de la mise en place du système de filtrage pour l'intermédiaire technique serait «*complexe, coûteux, permanent et à ses seuls frais ce qui serait d'ailleurs contraire aux conditions prévues à l'article 3, paragraphe 1, de la directive 2004/48, qui exige que les mesures pour assurer le respect des droits de propriété intellectuelle ne soient pas inutilement complexes ou coûteuses*». ⁸⁵

Cette préoccupation semble apparaître toute nouvelle pour la CJUE, la liberté d'entreprise des intermédiaires techniques n'ayant pas fait l'objet de référence dans les questions préjudicielles posées, ni même suscitée quelconque observation de l'Avocat général dans ses conclusions.⁸⁶ De même, la référence à l'article 16 de la Charte par la Cour de Justice serait inédite selon une doctrine autorisée.⁸⁷ C'est donc autant d'indices qui invitent à considérer la liberté d'entreprendre des intermédiaires techniques comme majeure. Les raisons nous apparaissent évidentes tant ces acteurs de l'Internet jouent un rôle important —

⁸³ Pour une opinion inverse, voir les observations du professeur Valérie-Laure BÉNABOU : «*(...) est-ce le poids économique de la surveillance générale qui justifie qu'on interdise de l'imposer aux intermédiaires techniques, ou des considérations d'autre nature, relatives à la liberté de communication des internautes ? Si l'on se réfère à la ratio legis de la directive commerce électronique, il semble que c'est bien la première lecture qui prévaut, à savoir d'impulser une dynamique favorable aux opérateurs de l'internet s'aventurant dans un monde inconnu aux perspectives économiques instables*» BÉNABOU Valérie-Laure, «Chroniques», *Propriétés Intellectuelles*, Janvier 2012, n°42, plus spécialement page 50.

⁸⁴ Point 46 de l'arrêt *Scarlet* et point 44 de l'arrêt *Netlog*.

⁸⁵ Point 48 de l'arrêt *Scarlet* et point 46 de l'arrêt *Netlog*. La Cour de Justice avait également eu l'occasion, dans un arrêt *L'Oréal c/ eBay* de retenir la même appréciation (CJUE 12 juillet 2011, aff. C-324/09, plus particulièrement §139. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009CJ0324:FR:HTML>).

⁸⁶ Conclusions de l'Avocat Général M. Pedro Cruz Villalón dans l'affaire C-70/10, CJUE 24 novembre 2011, «*Scarlet / SABAM* » <http://curia.europa.eu/juris/document/document.jsf?text=&docid=81776&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=364346>.

⁸⁷ Monsieur Cédric MANARA relève que «*si l'on trouve dans la jurisprudence communautaire la reconnaissance de la liberté d'exercer une activité économique ou commerciale, jamais encore la Cour ne s'était appuyé sur l'article 16 de la Charte*». «Le droit du commerce électronique après l'arrêt *Scarlet*», *RLDI* 2012/78, n°2612.

sinon incontournable — dans la société de l'information.⁸⁸ En effet, d'une liberté d'entreprendre effective découle le bénéfice d'autres libertés fondamentales, propres aux internautes.

§2. La nécessité de ne pas porter atteinte aux libertés fondamentales des internautes

Les mesures de filtrage risquent effectivement d'avoir des effets sur les communications électroniques que s'échangent les internautes, leur objet étant précisément d'empêcher que des contenus violant la propriété intellectuelle puissent circuler. Cette lapalissade est toutefois utile à rappeler pour souligner la nécessité que ces dispositifs ne portent pas atteinte, outre mesure, aux libertés fondamentales des internautes, à savoir notamment la liberté de recevoir ou de communiquer des informations (a) ou encore la protection des données à caractère personnel (b).

a. La nécessité de ne pas porter atteinte à la protection des données à caractère personnel

La Cour de Justice dans l'affaire *Scarlet* relève que le système de filtrage litigieux serait «*susceptible de porter atteinte aux droits fondamentaux des clients [du] FAI, à savoir leur droit à la protection des données à caractère personnel*»⁸⁹ car ce filtrage «*impliquerait une analyse systématique de tous les contenus ainsi que la collecte et l'identification des adresses IP des utilisateurs qui sont à l'origine de l'envoi des contenus illicites sur le réseau, ces adresses étant des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs*».⁹⁰ Dans l'affaire *Netlog*, elle retient que «*le filtrage litigieux [est] également susceptible de porter atteinte aux droits fondamentaux des utilisateurs des services de ce prestataire, à savoir leur droit à la protection des données à caractère personnel*»⁹¹, or les profils créés par les utilisateurs sur le réseau social Netlog «*sont des données à caractère personnel, car elles permettent, en principe, l'identification desdits utilisateurs*».⁹² Dans ces deux affaires, elle s'appuie sur l'article 8 de la Charte des droits fondamentaux de l'Union européenne.⁹³

L'arrêt *Scarlet* est ici intéressant en ce qu'il qualifie les adresses IP des utilisateurs de données à caractère personnel. Comme le note l'Avocat général dans ses conclusions, la Cour n'a «*jamais encore eu l'occasion d'examiner si une adresse IP pouvait être considérée, en tant que telle, comme une donnée personnelle*».⁹⁴ La Cour de Luxembourg vient donc conforter la position de la CNIL et plus globalement celle

⁸⁸ Nous renvoyons à nos développements ci-haut, sur «Les considérations juridiques justifiant l'interdiction d'une obligation générale de surveillance» (Chapitre 1, Section 1, B).

⁸⁹ Point 50 de l'arrêt *Scarlet*.

⁹⁰ Point 51 de l'arrêt *Scarlet*.

⁹¹ Point 48 de l'arrêt *Netlog*.

⁹² Point 49 de l'arrêt *Netlog*.

⁹³ Article selon lequel : «*1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante*».

⁹⁴ Conclusion Monsieur l'Avocat général Pedro Cruz Villalón, *précité*, §75.

du groupe de travail G29⁹⁵, qui considèrent l'adresse IP comme étant une donnée à caractère personnel⁹⁶, position que ne partage cependant pas — encore ? — la Cour de Cassation.⁹⁷

Si l'on peut saluer la Cour de Justice d'avoir ainsi exprimé son avis sur cette question qui divisait, l'observateur de la décision regrette toutefois que celle-ci n'ait pas dénié apporter plus de précisions. Que les adresses IP soient des données à caractère personnel n'est pas *per se* un obstacle à la possibilité qu'elles fassent l'objet d'une collecte. En effet, et comme le souligne l'Avocat général, «*la question qui se pose est, dès lors, moins celle de savoir quel est le statut juridique des adresses IP que de déterminer dans quelles conditions et à quelles fins elles peuvent être collectées, dans quelles conditions il peut être procédé à leur résolution et au traitement des données personnelles qui en résulte, ou encore à quelles conditions il peut être exigé de procéder à leur collecte et à leur résolution*».⁹⁸ Sans doute est-ce l'imprécision quant au type de système de filtrage sollicité par la SABAM qui ne permettait pas à la Cour d'éclairer cette interrogation.⁹⁹

Toujours est-il que la Cour manque de précision dans sa décision, alors même que ces considérants sont censés permettre d'apprécier l'application du principe de proportionnalité entre la protection de la propriété intellectuelle et la protection des données à caractère personnel. On peut regretter la sagesse de la Cour de Justice dans l'affaire «*Promusicae*», au sujet de la lutte contre la contrefaçon sur les réseaux *peer-to-peer*, où elle avait retenue, conformément à l'article 15§1 de la directive 2002/58 dite «*Vie privée et communications électroniques*», que «*les États membres peuvent adopter des mesures législatives visant à limiter la portée, notamment, de l'obligation de garantir la confidentialité des données relatives au trafic lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour (...) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46*».¹⁰⁰ Elle en avait alors tirée la conséquence suivante : «*la directive 2002/58 n'exclut pas la possibilité, pour les États membres, de prévoir l'obligation de divulguer, dans le cadre d'une procédure civile, des données à caractère personnel*».¹⁰¹ Il reste à espérer que la Cour de Justice, dans l'arrêt *Scarlet*, avait en-tête sa jurisprudence antérieure lorsqu'elle affirmait, un peu trop

⁹⁵ Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, aussi appelé «Groupe de travail G29».

⁹⁶ Avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel, consultable en ligne http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf.

⁹⁷ Cass. Crim. 13 janvier 2009 «*Sacem et autres / Cyrille S.*» http://www.legalis.net/?page=jurisprudence-decision&id_article=2563.

⁹⁸ Conclusion Monsieur l'Avocat général Pedro Cruz Villalón, *précité*, §79.

⁹⁹ Madame Anne DEBET observe qu'il n'est pas certain que la question de la protection des données personnelles dans l'arrêt *Scarlet* se posait vraiment («Des limites strictes posées au filtrage des contenus sur Internet par la CJUE», *Communication Commerce Électronique*, n°6, Juin 2012, comm. 63), citant à l'appui les conclusions de l'Avocat général : «*Il y a une certaine difficulté à évaluer concrètement l'incidence d'un système de filtrage et de blocage sur le droit à la protection des données personnelles. Une première difficulté consiste à identifier les données personnelles en cause, ces dernières n'étant, hormis en ce qui concerne les «adresses IP» pas clairement identifiées. La neutralité technologique revendiquée par la Sabam implique, en effet, qu'il n'est pas possible, a priori, de déterminer si le système à mettre en place implique un traitement de données personnelles. Il n'est, a fortiori, pas possible de déterminer s'il implique la collecte et la résolution d'adresses IP*» §74.

¹⁰⁰ Point 49 de l'arrêt *Promusicae*.

¹⁰¹ Point 54 de l'arrêt *Promusicae*.

rapidement, que la collecte des adresses IP est contraire à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Pareille déception a pu être observée chez une commentatrice avisée, l'arrêt du 24 novembre 2011 laissant l'amère impression d'une décision «*rendue à l'emporte pièce*». ¹⁰²

Le même sentiment se retrouve dans l'argumentation de la Cour relative à la nécessité de ne pas porter atteinte à la liberté de recevoir ou de communiquer des informations.

b. La nécessité de ne pas porter atteinte à la liberté de recevoir ou de communiquer des informations

La Cour de Justice relève également que l'injonction litigieuse risquerait de «*porter atteinte à la liberté d'information, puisque ce système risquerait de ne pas suffisamment distinguer entre un contenu illicite et un contenu licite, de sorte que son déploiement pourrait avoir pour effet d'entraîner le blocage de communications à contenu licite. En effet, il n'est pas contesté que la réponse à la question de la licéité d'une transmission dépende également de l'application d'exceptions légales au droit d'auteur qui varient d'un État membre à l'autre. En outre, certaines œuvres peuvent relever, dans certains États membres, du domaine public ou elles peuvent faire l'objet d'une mise en ligne à titre gratuit de la part des auteurs concernés*». ¹⁰³

La CJUE se fonde ici sur l'article 11 de la Charte des droits fondamentaux de l'Union européenne, relatif à la liberté d'expression et d'information. La question de la liberté d'expression est en effet cruciale dans une société démocratique et les mesures de filtrage et de blocage apparaissent, de manière légitime et souvent passionnée, comme des dispositifs de censure. Pour opérer la balance des intérêts en présence, la CJUE se livre là encore à une analyse *in concreto* et s'intéresse aux spécificités de la propriété intellectuelle. D'après elle, il serait difficile d'identifier si un contenu contrefait ou non des droits d'auteur, notamment en raison de la complexité de la matière, citant notamment les exceptions légales au droit d'auteur ou du domaine public qui ne sont pas les mêmes dans chaque État membre. Consciente de la complexité de la matière, la CJUE a toutefois fait montre de simplicité en éludant la question dans un seul considérant.

Tout au contraire, une injonction adressée à un intermédiaire technique lui imposant une obligation de surveillance qui ne serait pas générale, c'est-à-dire une obligation particulière de surveillance, permettrait d'obliger cet intermédiaire à prévenir ou faire cesser une atteinte aux droits de la propriété intellectuelle.

¹⁰² BÉNABOU Valérie-Laure, *ibid.*

¹⁰³ Point 52 de l'arrêt *Scarlet*, Point 50 de l'arrêt *Netlog*.

Chapitre 2. La possibilité d'imposer aux intermédiaires techniques une obligation particulière de surveillance pour prévenir ou cesser une atteinte à des droits de propriété intellectuelle

Le droit de l'Union européenne, et le droit français qui le transpose, permettent au juge d'imposer aux intermédiaires techniques une obligation particulière de surveillance afin de prévenir ou de faire cesser des atteintes à des droits de propriété intellectuelle (Section 1). Toutefois, la frontière étant mince entre l'obligation générale de surveillance et l'obligation particulière de surveillance, et l'imprécision des textes aidant, l'interprétation qu'en font les juges européens et français doit être observée comme un véritable guide d'utilisation (Section 2).

Section 1. La possibilité pour le juge d'imposer une obligation particulière de surveillance à un intermédiaire technique

Le législateur européen a prévu divers fondements juridiques permettant d'imposer aux intermédiaires techniques des mesures visant à prévenir ou faire cesser une atteinte à des droits de propriété intellectuelle (A). S'opposant à l'obligation générale de surveillance, le législateur n'en donne toutefois pas la définition, de sorte qu'il convient de s'interroger sur les contours de l'obligation particulière de surveillance pour la distinguer de la première (B).

A. Les fondements des obligations particulières de surveillance permettant de prévenir ou faire cesser une atteinte à des droits de propriété intellectuelle

Le législateur européen envisage le rôle particulier que peuvent jouer les intermédiaires techniques grâce à la possibilité de mettre en place des mesures ciblées permettant de prévenir ou de faire cesser des atteintes aux droits de la propriété intellectuelle. On retrouve ainsi divers fondements propres à leur imposer des obligations particulières de surveillance que ce soit, de façon générale, dans la directive Commerce électronique (§1) ou, de façon spéciale, dans les directives relatives à la propriété intellectuelle (§2).

§1. Les dispositions générales issues de la directive Commerce électronique

Si l'article 15 de la directive Commerce électronique pose comme interdit absolu la possibilité pour un État membre d'imposer à un intermédiaire technique une obligation générale de surveillance, ladite directive, en laissant la possibilité de prévoir des mesures propres à prévenir ou faire cesser toute violation, en atténue la portée.

En effet, le législateur européen fait montre d'autant de clarté lorsqu'il affirme, au considérant 47 de la directive que *«l'interdiction pour les états membres d'imposer aux prestataires de services une obligation de surveillance ne vaut que pour les obligations à caractère général»*.¹⁰⁴ Dans un même trait de plume, le considérant ajoute qu': *«elle ne concerne pas les obligations de surveillance applicables à un cas spécifique et, notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale»*.¹⁰⁵

Il ne faudrait pas mésestimer la portée de ces considérants ou les apprécier avec une valeur moindre que celle d'un article à proprement dit. Comme l'écrit le professeur Jean-Louis BERGEL,

¹⁰⁴ Nous soulignons.

¹⁰⁵ Nous soulignons.

«contrairement aux exposés des motifs et aux travaux préparatoires de droit interne, les préambules des actes communautaires sont des documents officiels, authentiques, qui permettent de placer les textes en perspective et de cerner leur finalité».¹⁰⁶ Ainsi que le note le professeur Célia ZOLYNSKI, «les objectifs formalisés dans les considérants s'imposent comme principe d'interprétation retenue en en asseyant sa pertinence».¹⁰⁷ Le considérant 47 vient donc distinguer très clairement l'obligation générale de surveillance de l'obligation particulière de surveillance et ne doit pas être perdu de vue lors de l'interprétation de l'article 15§1 de la directive.

De même, à son considérant 45, la directive Commerce électronique précise que le régime de responsabilité favorable aux intermédiaires est «sans préjudice de la possibilité d'actions en cessation de différents types». Le considérant en précise alors les contours, ajoutant que «ces actions en cessation peuvent notamment revêtir la forme de décisions de tribunaux ou d'autorités administratives exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible».¹⁰⁸

Il est ici intéressant de relever que l'autorité judiciaire n'est pas la seule à être en mesure d'imposer de telles activités de surveillance. Une autorité administrative nationale qui aurait reçu telle compétence d'un État membre pourrait elle aussi prononcer des mesures visant à prévenir ou faire cesser toute violation. On peut néanmoins dans cette hypothèse s'interroger quant à savoir si une autorité administrative serait meilleure gardienne des libertés individuelles que le juge. Quoique la directive offre cette possibilité, la CJUE pourrait fort bien, au regard de ses exigences accrues de respect des libertés fondamentales, contester que cette garantie soit effective.¹⁰⁹

Cette possibilité d'actions en cessation est rappelée à chaque article posant des limitations à la responsabilité des intermédiaires techniques. On la retrouve ainsi évoquée pour les fournisseurs d'accès à l'article 12§3¹¹⁰, pour les fournisseurs de cache à l'article 13§2¹¹¹ et pour les hébergeurs à l'article 14§3¹¹². La LCEN est venue l'intégrer à l'article 6 I 7, alinéa 2, qui dispose que «le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire»

¹⁰⁶ BERGEL Jean-Louis, La découverte du sens en droit par la finalité, p.67 in La découverte du sens en droit, Association Française de Philosophie du droit, 1991, édité par François Paychère.

¹⁰⁷ ZOLYNSKI Célia, Méthode de transposition des directives communautaires, Dalloz, Nouvelle bibliothèque des thèses, plus spécialement n°90.

¹⁰⁸ Nous soulignons.

¹⁰⁹ Cette inquiétude est notamment soulignée par le professeur Emmanuel DERIEUX. «Filtrage par les FAI - Opposition aux obligations générales de filtrage imposées aux fournisseurs d'accès à internet», *RLDI* 2012/78, n°2611.

¹¹⁰ Article 12§3 de la directive Commerce électronique : «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».

¹¹¹ Article 13§2 de la directive Commerce électronique : «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 fin à une violation ou qu'il prévienne une violation».

¹¹² Article 14§3 de la directive Commerce électronique : «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».

Ces dispositions ont vocation à s'appliquer à tout type de violation, la directive Commerce électronique appréhendant de manière transversale la question de la responsabilité des intermédiaires techniques. On doit relever que les directives intéressant directement la propriété intellectuelle traitent également des injonctions que peut prononcer un juge pour faire participer les intermédiaires techniques à la protection de la propriété intellectuelle.

§2. Les dispositions propres à la propriété intellectuelle

Outre la directive Commerce électronique, la directive 2001/29/CE «*Droit d'auteur et droits voisins*» et la directive 2004/48/CE «*Respect des droits de la propriété intellectuelle*», envisagent chacune les possibilités pour le juge de faire participer les intermédiaires techniques à la protection de la propriété intellectuelle.

La directive 2001/29/CE prévoit ainsi à son article 8§3 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*». Le considérant 59 de la directive témoigne particulièrement du rôle nécessaire des intermédiaires techniques, considérés comme «*les mieux à même de mettre fin à ces atteintes*» sur Internet, «*de plus en plus [utilisé] par des tiers pour porter atteinte à des droits*», qui justifie que «*les titulaires de droits doivent avoir la possibilité de demander qu'une ordonnance sur requête soit rendue à l'encontre d'un intermédiaire qui transmet dans un réseau une contrefaçon commise par un tiers d'une oeuvre protégée ou d'un autre objet protégé*».

La loi du 12 juin 2009 dite «*Hadopi*»¹¹³ a transposé à l'article L336-2 du Code de la propriété intellectuelle ce dispositif permettant qu' «*en présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits visées à l'article L321-1 ou des organismes de défense professionnelle visés à l'article L331-1, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier.*»

La directive 2004/48/CE complète¹¹⁴ quant à elle la possibilité de solliciter la collaboration des intermédiaires techniques pour protéger des droits de propriété intellectuelle. Son article 11 précise ainsi que : «*(...) les États membres veillent également à ce que les titulaires de droits puissent demander une injonction à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle, sans préjudice de l'article 8, paragraphe 3, de la directive 2001/29/CE.*» Son article 3 précise toutefois que les mesures prises pour assurer le respect des droits de propriété intellectuelle «*doivent être loyales et équitables, ne doivent pas être inutilement complexes ou coûteuses et ne doivent pas comporter de délais déraisonnables ni entraîner de retards injustifiés*».

¹¹³ Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

¹¹⁴ La directive 2004/48 a pour objectif d'offrir aux titulaires de droits «*la possibilité de demander une injonction à l'encontre d'un intermédiaire dont les services sont utilisés par un tiers pour porter atteinte au droit de propriété industrielle du titulaire*» (considérant 23).

On a vu précédemment que les mécanismes prévus par directive Commerce électronique permettant au juge d'enjoindre à un intermédiaire de mettre en place une surveillance spécifique s'appliquaient aussi en matière de propriété intellectuelle. Peut-on imaginer alors que les dispositions des directives spécifiques à la propriété intellectuelle soient quant à elle autonomes ? On doit ici répondre par la négative. En effet, le considérant 16 de la directive 2001/29 rappelle que la «*question de la responsabilité*» des intermédiaires est «*traitée de manière horizontale dans la directive 2000/31/CE*» et que «*la présente directive est sans préjudice des dispositions relatives à la responsabilité de ladite directive*». De la même manière, la directive 2004/48 à son article 2§3 précise que «*la présente directive n'affecte pas a) (...) la directive 2000/31/CE en général et les articles 12 à 15 de cette dernière directive en particulier*».

Dans les arrêts *Scarlet* et *Netlog*, la CJUE s'est livrée à la même analyse pour dégager sa solution. La directive Commerce électronique doit donc être observée comme le droit général de la responsabilité des intermédiaires auquel ne peut déroger les dispositions spéciales de la propriété intellectuelle. Cette solution n'est pas sans incidences sur la manière dont il est possible de mener une politique de lutte contre les atteintes aux droits de la propriété intellectuelle. Elle conduit à donner une sorte de primauté à la directive 2000/31, du fait de son approche horizontale. Quand bien même le législateur européen souhaiterait introduire des dispositions spécifiques à la lutte contre la contrefaçon en ligne, par exemple pour prendre en compte l'évolution de la technique, celles-ci ne pourraient jamais venir bousculer l'assise de la «*séculaire*»¹¹⁵ directive 2000/31. Comme le note le professeur Valérie-Laure BENABOU commentant la décision *Scarlet*, «*il semble donc que les juges aient entendu par la présente décision faire de l'interdiction de surveillance généralisée une mesure socle du droit applicable aux réseaux de communication électronique*».¹¹⁶

Ainsi, peu importe la source normative permettant d'imposer à un intermédiaire de prévenir ou faire cesser une atteinte à la propriété intellectuelle, une vigilance accrue s'impose pour que ces dispositifs ne puissent pas être qualifiés de surveillance générale, ce qui amène à s'intéresser aux contours de l'obligation particulière de surveillance.

B. Les contours de l'obligation particulière de surveillance

La spécificité de l'obligation particulière de surveillance est qu'elle s'oppose à l'obligation générale de surveillance, de sorte que pour savoir ce qu'elle est, il faut s'intéresser à ce qu'elle n'est pas, c'est-à-dire une obligation n'étant pas générale. On peut donc s'interroger quant à savoir ce que recoupe précisément le vocable «*général*» pour venir dresser une première esquisse de ce que pourrait être une obligation particulière de surveillance. Au delà de cette approche prospective (1), on verra que l'imprécision des termes conduit à une certaine insécurité juridique (2).

§1. La recherche d'une définition de la notion de généralité

La directive Commerce électronique reste avare quant à la notion de caractère général. La Commission européenne elle-même, dans un document de travail accompagnant sa communication «*Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et*

¹¹⁵ A l'heure du numérique.

¹¹⁶ BENABOU Valérie-Laure, «Chroniques», *Propriétés Intellectuelles*, Janvier 2012, n°42.

d'autres services en ligne» du 11 janvier 2012, a pu regretter ce manque de précisions quant à la différence entre l'obligation générale de surveillance et l'obligation particulière de surveillance.¹¹⁷

Ce manque de précision a donc amené les auteurs à s'interroger quant aux contours de l'obligation générale de surveillance et chercher à identifier quelle situation permet de considérer que l'on est en présence d'une obligation particulière de surveillance.

On peut appréhender cette notion de caractère général de plusieurs façons. Soit l'on considère que la généralité s'exprime par le fait que la mesure de surveillance, pour bloquer un contenu illicite, supposerait une recherche sur l'ensemble des contenus. Soit l'on considère que la généralité s'exprime du fait que l'on recherche tous les contenus potentiellement illicites.¹¹⁸

La première interprétation conduit à retenir que le caractère général d'une mesure de surveillance s'exprimerait en raison de l'étendue de la mesure de filtrage. Dit autrement, parce que la recherche d'un seul contenu illicite obligerait à filtrer l'ensemble des contenus, un tel dispositif serait assimilable à une surveillance générale. Une telle interprétation paraît quelque peu insensée, tant du point de vue juridique que du point de vue technique.

Juridiquement d'abord, nous sommes de ceux qui considérons que la possibilité laissée par la directive Commerce électronique d'imposer une obligation particulière s'inscrit en exception au principe d'interdiction d'imposer une obligation générale de surveillance. Pareille analyse n'est toutefois pas partagée par tous les auteurs. Ainsi Messieurs Étienne Montéro et Quentin Van Enis considèrent que *«l'affirmation d'un principe va souvent de paire avec la formulation d'autres principes qui, ayant leur domaine et leur justification propres, viennent compléter le premier, tempérer les effets, sans toutefois le contredire. Il faut voir en la possibilité d'imposer une obligation particulière de surveillance l'affirmation d'un tel principe correcteur qui vient compléter le principe d'interdiction des mesures générales de surveillance, sans le contrarier»*.¹¹⁹ Pour ces auteurs donc, *«il ne nous semble pas permis d'imposer une mesure générale de monitoring, fût-ce aux fins de détecter un contenu spécifique, au titre de la possibilité d'imposer une*

¹¹⁷ *«Yet what is a general monitoring obligation as opposed to a "specific" monitoring obligation, the second of which could be allowed in the meaning of recital 47 of the Directive? There remains uncertainty over what degree of monitoring is acceptable in the sense of Article 15.»* Nous traduisons : « Mais qu'est-ce qu'une obligation générale de surveillance, par opposition à une obligation de surveillance « spécifique », la seconde pouvant être autorisée au sens du considérant 47 de la directive ? », Commission Staff Working Document SEC(2011) 1641 final, 11 janvier 2012, plus particulièrement les pages 25 et 26. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1641:FIN:EN:PDF>.

¹¹⁸ Formulées différemment, ces questions sont posées par plusieurs auteurs. On peut citer Monsieur Ronan HARDOUIN, qui s'interroge ainsi : *«L'obligation est-elle générale du fait que les hébergeurs doivent filtrer l'ensemble des contenus pour en rechercher seulement un ? Ou la généralité s'exprime-t-elle par la seule recherche sur l'ensemble des contenus afin d'identifier les contenus illicites potentiels ?»*, Observations sur les nouvelles obligations prétoriennes des hébergeurs, <http://juriscom.net/wp-content/documents/resp20071108.pdf>. • Messieurs Étienne Montéro et Quentin Van Enis pose ainsi le problème : *«L'obligation de surveillance est-elle générale dès l'instant où elle implique une recherche sur l'ensemble des contenus, afin d'en bloquer un seul, supposé illicite, ou l'est-elle seulement s'il s'agit de surveiller l'ensemble des contenus afin d'en débusquer tous les contenus potentiellement illicites ?»*, Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'internet : la quadrature du cercle ?, RLDI 2010/60. • Madame Cécile Petit se questionne ainsi : *«Peut-on estimer que l'on tombe dans le cadre de l'obligation générale de surveillance dès l'instant où l'obligation implique une recherche sur l'ensemble des contenus afin d'en bloquer un seul ?»*, Google, une obligation de surveillance proportionnée ? Rec. Dalloz 2012, p. 2071.

¹¹⁹ Montéro et Q. Van Enis, Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'internet : la quadrature du cercle ?, RLDI 2010/60, plus particulièrement §31.

surveillance particulière». ¹²⁰ Cette position réduit toutefois l'obligation particulière en une peau de chagrin et semble rendre incertaine sa mise en place technique.

Techniquement parlant, il nous semble effectivement malaisé d'imaginer un système de surveillance visant la détection d'un contenu précis, sans que cette recherche soit étendue à l'ensemble des contenus. Cela supposerait que la recherche d'un contenu identifié comme illicite s'effectue, dans le cadre d'une obligation particulière de surveillance, de façon non générale (sic !) mais parcellaire. Une telle incohérence nous pousse à penser que cette interprétation du caractère général ne peut qu'être mauvaise.

Il nous semble en vérité que la seconde interprétation du caractère général soit la plus acceptable, à savoir que la généralité s'exprime du fait que l'on recherche tous les contenus potentiellement illicites. Dès lors, pour que l'on passe d'une surveillance générale à une surveillance particulière, il suffirait que le contenu faisant l'objet de la surveillance soit identifié. On se trouverait alors dans un cas *«spécifique clairement défini»*. ¹²¹ Ainsi que le note Ronan Hardouin, *«le critère discriminant pour que l'obligation spéciale de surveillance soit contraignante à l'égard de l'hébergeur est que les contenus à surveiller soient identifiées»*. ¹²²

§2. L'insécurité juridique née de l'absence de définition

L'absence de définition de l'obligation générale de surveillance et la difficulté à identifier les contours de l'obligation particulière de surveillance conduisent à une importante insécurité juridique. Elle vient d'une part semer le doute quant à l'interprétation que l'on peut donner à la directive Commerce électronique sur ces points. Cela a pour conséquence une profonde méconnaissance de ces mécanismes et leur faible utilisation par les justiciables devant les tribunaux. Par ailleurs, l'évolution de la jurisprudence, tant européenne que nationale, ses affinements et ses bouleversements rendent frileux les ayants droit à recourir à ces mécanismes pour protéger leurs droits de propriété intellectuelle.

L'appréciation par le juge vient en effet suppléer les lacunes d'une législation peu loquace et reste la meilleure grille d'appréciation des critères à retenir pour pouvoir imposer une obligation de surveillance aux intermédiaires techniques.

Section 2. L'appréciation par le juge des obligations de surveillance imposées aux intermédiaires techniques

L'étude de la jurisprudence tant européenne que française apporte des enseignements quant conditions pour qu'une obligation de surveillance imposée à un intermédiaire technique ne soit pas qualifiée de surveillance générale. A dire vrai, il semblerait que la récente jurisprudence de la Cour de Justice de l'Union Européenne (A) ait influencé la jurisprudence française en voie d'uniformisation (B).

¹²⁰ *Ibid.*

¹²¹ *«(...) l'article 15 n'empêche pas les autorités publiques des États membres d'imposer une obligation de surveillance dans un cas spécifique clairement défini»*, Premier rapport sur l'application de la directive 2000/31/CE sur le commerce électronique, 21 novembre 2003, p. 15. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:FR:PDF>.

¹²² HARDOUIN Ronan, «Fascicule 464 : La responsabilité des intermédiaires techniques de l'internet», *Lamy droit des médias et de la communication* 2012.

A. Les critères retenus par la CJUE

La Cour de Justice de l'Union Européenne, dans ses récents arrêts *Scarlet* et *Sabam* est venue justifier avec minutie les raisons selon lesquelles les filtrages litigieux à ces espèces devaient subir la qualification d'obligation générale de surveillance et partant être mis au ban.

Ainsi s'agissant de l'arrêt *Scarlet*, la Cour de Justice retenait que :

«Les directives (...) lues ensemble et interprétées au regard des exigences résultant de la protection des droits fondamentaux applicables, doivent être interprétées en ce sens qu'elles s'opposent à une injonction faite à un fournisseur d'accès à Internet de mettre en place un système de filtrage

- de toutes les communications électroniques transitant par ses services, notamment par l'emploi de logiciels «peer-to-peer»;*
- qui s'applique indistinctement à l'égard de toute sa clientèle;*
- à titre préventif;*
- à ses frais exclusifs, et*
- sans limitation dans le temps,*

capable d'identifier sur le réseau de ce fournisseur la circulation de fichiers électroniques contenant une œuvre musicale, cinématographique ou audiovisuelle sur laquelle le demandeur prétend détenir des droits de propriété intellectuelle, en vue de bloquer le transfert de fichiers dont l'échange porte atteinte au droit d'auteur.»

S'agissant de l'arrêt *Netlog*, la Cour de Justice motivait sa décision d'une manière quasi-identique en jugeant que :

«Les directives (...) lues ensemble et interprétées au regard des exigences résultant de la protection des droits fondamentaux applicables, doivent être interprétées en ce sens qu'elles s'opposent à une injonction faite par un juge national à un prestataire de services d'hébergement de mettre en place un système de filtrage:

- des informations stockées sur ses serveurs par les utilisateurs de ses services;*
- qui s'applique indistinctement à l'égard de l'ensemble de ces utilisateurs;*
- à titre préventif;*
- à ses frais exclusifs, et*

– sans limitation dans le temps,

capable d'identifier des fichiers électroniques contenant des œuvres musicales, cinématographiques ou audiovisuelles sur lesquelles le demandeur prétend détenir des droits de propriété intellectuelle, en vue de bloquer la mise à disposition du public desdites œuvres qui porte atteinte au droit d'auteur.»

On peut s'interroger quant à savoir si c'est la combinaison de l'ensemble de ces critères qui conduit la mesure de filtrage litigieuse à s'attirer les foudres des juges de l'Union européenne. Ou bien est-ce qu'un seul de ces critères apparaît à lui seul suffisant pour emporter la censure d'une telle mesure de surveillance ? Il nous semble qu'il faille retenir la première acception, en ce que c'est la combinaison d'un tout qui fait que la mesure apparaît disproportionnée. C'est donc la vérification d'un juste équilibre entre chacun de ces critères qui doit être menée par le juge pour apprécier la conformité de la mesure de filtrage sollicitée avec les exigences posées par le droit de l'Union européenne.

Quoique certains auteurs aient pu écrire qu'« (...) il est raisonnable d'avancer que la Cour n'accepterait pas non plus des mesures techniques qui ne seraient pas aussi larges que celle sollicitée en l'espèce»¹²³, la plupart des commentateurs optaient pour une interprétation plus nuancée, de sorte que la Cour « (...) réfute uniquement les filtrages préventifs, systématiques et illimités dans le temps qui est condamné».¹²⁴ Ainsi, le filtrage préventif n'est pas banni *per se*.¹²⁵

Aussi peut-on formuler ci-après pour chacun des points mis en lumière par la Cour de Justice de l'Union Européenne, à savoir la durée (§1), l'étendue (§2), le public visé (§3), le coût (§4) de la surveillance ainsi que son caractère préventif (§5) de brèves observations nous permettant de tracer les limites de l'obligation particulière de surveillance.

¹²³ Monsieur Cédric Manara répondait ici à la question suivante «*Est-ce la conjonction de sa complexité, de son coût et du fait que celui-ci est entièrement supporté par l'intermédiaire qui amène la Cour à qualifier la mesure de filtrage demandée d'«atteinte caractérisée à la liberté d'entreprise du FAI» ?*», «Le droit du commerce électronique après l'arrêt *Scarlet*», *RLDI* 2012/78, n°2612.

¹²⁴ CASTETS-RENARD Céline, «Protection du droit d'auteur confrontée aux droits fondamentaux : point trop n'en faut !», *RLDI* 2012/79, n°2622. On peut également citer d'autres auteurs : «*Ainsi, si tout système de filtrage généralisé est bien prohibé, il n'en est pas forcément de même pour des systèmes de filtrage plus ciblés*», COSTES Lionel, «Affaire *Sabam* : l'analyse de la CJUE», *RLDI* 2011/77, n°2541. • «*Le caractère excessif de la mesure demandée n'y est sans doute pas pour rien : sans limite dans le temps, aux frais du seul FAI, à titre préventif ... L'ouverture est donc étroite mais un recours plus mesuré au filtrage ne paraît pas totalement impossible*», BERNAULT Carine, «Coup d'arrêt pour le filtrage préventif sur les réseaux numériques», *L'ESSENTIEL Droit de la propriété intellectuelle*, 15 janvier 2012, n°1, p. 1. • «*La portée de l'arrêt est en effet circonscrite, la Cour, en interdisant, trace aussi les limites de ce qui est permis. Une lecture a contrario de l'arrêt conduit à accepter des filtrages limités, à titre curatif, qui ne sont pas seulement aux frais du réseau social et sont limités dans le temps*», MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 2 août 2012, n°215, p. 11.

¹²⁵ On peut relever la décision du juge britannique dans une affaire *Twentieth Century Fox v British Telecom* dans laquelle le juge, s'appuyant sur les conclusions de l'Avocat général dans l'affaire *Scarlet* (mais rendue antérieurement à l'arrêt *Scarlet*), ordonnait le filtrage du site Newsbin par l'opérateur BT. *Twentieth Century Fox and others v British Telecommunications plc* [2011] EWHC 1981 (Ch), 28 juillet 2011 http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/28_07_11_bt_newzbin_ruling.pdf.

§1. La durée de la surveillance

La Cour de Justice dans ses arrêts *Scarlet* et *Netlog* souligne que la mesure de filtrage est demandée «*sans limitation dans le temps*». On comprendrait effectivement mal pourquoi l'intermédiaire technique devrait être tenu à une obligation «*ad vitam aeternam*» au regard ne serait-ce que des principes civilistes de notre droit.

Plus encore, en ce qui concerne la propriété intellectuelle, on imagine mal pourquoi cette obligation viendrait être illimitée, de sorte qu'elle puisse dépasser le monopole légal de la protection des droits d'auteur, à savoir 70 ans *post-mortem*.

Peut-on en revanche considérer que la durée légale maximum de la protection des droits d'auteur puisse être une durée limitée ?¹²⁶ Quoique ainsi théoriquement limitée, la durée ne serait pour autant pas déterminée mais uniquement déterminable, le décès de l'auteur étant l'évènement permettant de calculer précisément la durée de la protection.

Aussi, il nous apparaît que la protection pour la durée du monopole légale du droit d'auteur ne doit pas être entendue comme une durée limitée, ce que la Cour de Justice semble poser comme une exigence. Des durées plus brèves et plus réduites devraient donc être proposées pour qu'une mesure de filtrage puisse être qualifiée de ciblée.¹²⁷ Ces durées pourraient être proposées en concertation avec les acteurs économiques de la propriété intellectuelle. Il nous semble en effet que le calcul de la durée de la protection relève moins d'une affaire d'espèce qu'un juge peut être amené à traiter que de considérations tenant à la nature de l'oeuvre. Ainsi, s'agissant des contenus audiovisuels, il nous semblerait utile et proportionnée que la durée du filtrage couvre, *a minima*, la durée de la chronologie des médias lorsque l'oeuvre en question est encore couverte par celle-ci.

§2. L'étendue de la surveillance

La Cour de Justice accorde également de l'importance à l'étendue de la surveillance qu'exige la mesure de filtrage, retenant dans l'affaire *Scarlet* que la mesure litigieuse visait à l'égard du fournisseur d'accès à internet à surveiller «*toutes les communications électroniques transitant par ses services, notamment par l'emploi de logiciels peer-to-peer*» et dans l'affaire *Netlog*, concernant un hébergeur, à surveiller «*des informations stockées sur ses serveurs par les utilisateurs de ses services*».

L'appréciation de l'étendue par la CJUE est quantitative, en ce sens que «*toutes*» les communications électroniques étaient visées par la mesure de surveillance. On peut s'interroger quant à la formulation quelque peu étrange employée ici qui ajoute «*notamment par l'emploi de logiciel peer-to-peer*». Est-ce à dire que la surveillance des seules communications électroniques transitant par le protocole *peer-*

¹²⁶ Sur cette question, voir les observations de Monsieur Ronan HARDOUIN : «*lorsque [l'activité de surveillance] porte sur un contenu protégé par un droit d'auteur, l'hébergeur sera lié au maximum jusqu'à la fin du monopole. On peut donc considérer qu'une telle obligation répond à la nécessité d'être « temporaire » tout en observant qu'il serait préférable de mentionner une durée de manière explicite*», Observations sur les nouvelles obligations prétoriennes des hébergeurs, 8 novembre 2007 <http://juriscom.net/2007/11/observations-sur-les-nouvelles-obligations-pretoriennes-des-hebergeurs/>.

¹²⁷ Pour un exemple de jurisprudence — ancienne ! — imposant un délai de 6 mois à un intermédiaire technique, en matière de concurrence déloyale. T. com. Paris, réf., 28 juillet 2007, « Vivastreet ». Voir Benoît Tabaka, « Vivastreet tenu à une obligation de filtrage a priori » <http://tabaka.blogspot.fr/2007/10/vivastreet-tenu-une-obligation-de.html>.

to-peer devrait être considérée comme une surveillance générale ? Répondre par la positive ne nous apparaîtrait pas pertinent. On a déjà pu faire observer que dès lors qu'un fichier à surveiller était identifié, l'obligation de surveillance devrait être considérée comme n'étant pas générale. Et d'ajouter qu'une mesure de filtrage ne portant pas sur l'intégralité des contenus circulant était par nature une mesure perméable. Si bien qu'une surveillance limitée sur les communications électroniques transitant par le protocole *peer-to-peer* nous apparaîtrait devoir être considérée comme ciblée.¹²⁸ Reste que la recherche d'un juste équilibre entre la protection des droits de la propriété intellectuelle et les autres droits fondamentaux apparaît plus complexe s'agissant d'un fournisseur d'accès à internet que d'un hébergeur, le trafic étant plus important, la nature des échanges et les types d'activités économiques reposant sur leur activité l'expliquant.

S'agissant de l'appréciation de l'étendue de la surveillance pour un hébergeur, l'arrêt *Netlog* retient que c'est en raison «des informations stockées sur ses serveurs par les utilisateurs de ses services» que celle-ci est notamment qualifiée de générale. Là encore la mesure de surveillance semble devoir être circonscrite à une étendue moindre que l'ensemble des contenus pouvant être stockés par l'intermédiaire. La possibilité technique de distinguer le type de contenu est ici plus aisée que pour le fournisseur d'accès à internet. En effet, alors que pour ce dernier, les communications électroniques transitent par paquet ne permettant pas de savoir la nature du contenu qu'ils transportent¹²⁹, l'hébergeur réceptionnant à l'arrivée les contenus et gérant lui-même ses services, peut mettre en bout de course un système de filtrage surveillant les seuls contenus vidéos ou audios.

En termes de juste équilibre, l'injonction adressée à un hébergeur pour protéger des droits de propriété intellectuelle nous apparaît plus apte à se concilier efficacement avec les libertés fondamentales.

§3. Le public visé par la surveillance

S'agissant du public visé par la mesure de filtrage, la CJUE pointait du doigt le fait que dans l'affaire *Scarlet*, cette mesure s'appliquait «*indistinctement à l'égard de toute sa clientèle*» et dans l'affaire *Netlog*, que la mesure s'appliquait «*indistinctement à l'égard de l'ensemble de ces utilisateurs*». En somme, la Cour de Justice vient dire qu'une mesure de surveillance qui concerne l'ensemble des internautes utilisant un service de communication électronique par un intermédiaire technique est un élément, combiné à d'autres, qui peut être jugée comme étant une surveillance générale. La question est donc de savoir comment est-il techniquement possible de retrancher un certain nombre d'internautes visés par la mesure de surveillance pour que celle-ci ne s'applique pas à tous. Dit autrement, la difficulté est de mettre en place une mesure de surveillance qui ne s'applique pas, selon les termes de la Cour elle-même, «*indistinctement*» à l'égard de tous.

¹²⁸ D'autant que l'usage de ce protocole s'avère servir, dans la majorité des cas, à la circulation de contenus protégés par la propriété intellectuelle. A tout le moins, ne transite pas par ce type de protocole des communications électroniques telles que de la correspondance privée, ce qui limite par principe les atteintes possibles aux droits des clients en cas de mise en place d'une mesure de filtrage.

¹²⁹ Sauf à mettre en place une technique de filtrage de type «Deep packet injection», permettant d'examiner chaque paquets afin d'identifier la nature du contenu qui est transporté. Cette technique est toutefois hautement intrusive en terme de secret des correspondances. Pour une présentation de cette technique, voir [Anglais] "Site Blocking" to reduce online copyright infringement», OFCOM, 27 May 2010, plus particulièrement p. 39 <http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf>.

Devant s'appliquer à un public moindre que l'ensemble, on peut se demander si la mesure de surveillance peut s'appliquer à un groupe d'individu ou doit s'appliquer à un seul individu, plus exactement l'auteur de la contrefaçon qui a conduit à mettre en place la surveillance ciblée.

Certain auteur défend effectivement cette deuxième acception, à savoir qu'une surveillance ciblée ne devrait concerner que la personne ayant mis en ligne l'oeuvre protégée par le droit d'auteur en ligne.¹³⁰ Pour étayer cette thèse, Alexandra Neri s'appuie sur le premier rapport sur l'application de la directive Commerce électronique qui, rappelant le considérant 47 de ladite directive, indique la possibilité pour les États membres d'imposer une obligation de surveillance dans un «*cas spécifique clairement défini*».¹³¹ Or, selon elle, la traduction de ce rapport dans la langue de Molière ne restituerait pas toute la précision contenue dans celle de Shakespeare, laquelle parle de «*specific, clearly defined individual case*». L'argument du manque de clarté n'est pas nouveau et s'appuie en l'espèce notamment sur le rapport du Sénat du 3 mars 2004¹³² lequel estimait que la version anglaise du rapport était plus précise que la traduction française. Si effectivement les sénateurs Herisson et Sido alertaient leurs collègues parlementaires sur cette différence de traduction, la correspondance avec la Commission européenne qu'ils apportent est de nature à écarter toute ambiguïté. La commission européenne écrivait au cabinet du Ministre de l'Industrie de l'époque qu'une obligation de surveillance dans un cas spécifique clairement défini : «*ne vise en aucun cas les obligations générales de surveillance pour lutter de manière générale et systématique contre certains types d'infractions, comme celles prévues dans le projet de loi, mais le cas où un hébergeur déterminé est soumis, dans le cadre d'une procédure judiciaire, à une obligation de surveillance précise, temporaire et encadrée concernant un site spécifique*».¹³³ Cette précision était la bienvenue, les sénateurs recherchant si l'on pouvait imposer des obligations de surveillance aux intermédiaires techniques en prévoyant des «*cas spécifiques clairement définis*» par la loi. La version anglaise du rapport, par l'ajout de l'adjectif «*individual*» n'a donc jamais eu pour but de venir rattacher l'obligation de surveillance à un individu. «*Individual case*» doit s'entendre en son sens commun et se traduire comme un «*cas particulier*», pour souligner d'avantage le caractère singulier - individuel - de la mesure.

En outre, notons que l'interprétation de la Commission européenne étant particulièrement claire, il ne convient pas d'étayer d'autres positions sur la base des débats parlementaires ayant amenés le Parlement français à transposer la directive Commerce électronique dans notre droit.¹³⁴

¹³⁰ Maître Alexandra Neri affirme que «*lorsque la directive fait obligation à un prestataire de stockage de retirer des informations dénoncées comme illicites ou de rendre l'accès à celles-ci impossible, cela ne peut concerner qu'un fait précisément défini, autrement dit un fichier reproduisant l'objet protégé en cause mis en ligne par un utilisateur en particulier, et non toute reproduction ultérieure de cette oeuvre par toute personne*», «L'injonction de filtrage rendue à l'égard d'un intermédiaire : une mesure controversée aux conséquences redoutables», *Communication Commerce Électronique*, n°1; janvier 2012, étude 3.

¹³¹ Premier rapport sur l'application de la 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 »), 21 nov. 2003, § 4.6.

¹³² Projet de loi pour la confiance dans l'économie numérique, rapport n° 232 (2003-2004) de MM. Pierre Hérisson et Bruno Sido, fait au nom de la commission des affaires économiques, déposé au Sénat le 3 mars 2004. Consultable en ligne http://www.senat.fr/rap/103-232/103-232_mono.html.

¹³³ Correspondance citée dans le rapport, *ibid*. Nous soulignons ici ce passage.

¹³⁴ On peut se référer aux écrits du doyen Carbonnier indiquant qu'il convient de rechercher l'intention du législateur parmi les travaux de celui qui a eu l'initiative du projet (not. l'exposé des motifs du projet de loi) plutôt que dans les débats parlementaires. *Droit civil*, vol. 1, PUF, 2004, n°154.

Par ailleurs, à bien regarder la jurisprudence antérieure de la CJUE, il semble que cette question avait déjà eu l'occasion d'être tranchée, de façon indirecte. En effet, dans l'affaire *L'Oréal c/ Ebay*¹³⁵, l'Avocat général M. Niilo Jääskinen avait, au sujet des injonctions pouvant être imposées à un intermédiaire technique et visant à empêcher la répétition d'une atteinte à un droit de marque, suggéré qu'il puisse «être institué une limite appropriée concernant l'objet des injonctions sous la forme d'une double condition d'identité. Cela signifie que, dans les affaires concernées, le tiers contrevenant devrait être la même personne et que les marques auxquelles il est porté atteinte devraient être les mêmes. Par conséquent, une injonction pourrait être prononcée à l'encontre d'un intermédiaire afin d'empêcher la poursuite ou la répétition d'une atteinte à une marque donnée par un utilisateur donné».¹³⁶ Monsieur Jääskinen n'a toutefois pas été suivi dans sa suggestion, si bien que l'objet d'une mesure de surveillance ciblée ne doit pas concerner l'objet contrefait par l'utilisateur contrefacteur.

Cette double condition d'identité, outre le fait qu'elle n'est prévue nulle part¹³⁷, serait techniquement illusoire. La double condition d'identité poserait en effet la question de l'identification de l'utilisateur contrefacteur. A supposer que l'identification repose sur l'adresse IP de l'utilisateur, rien n'empêche ce dernier d'en changer¹³⁸ ou de se connecter depuis un autre terminal. L'hypothèse ne semblait pas bien appréhendée par l'Avocat général qui, dans l'affaire *L'Oréal c/ Ebay* suggérait que l'intermédiaire technique puisse «se conformer à une injonction de ce type en clôturant tout simplement le compte client de l'utilisateur en question».¹³⁹ Pis encore, cette surveillance ciblée par identification de l'adresse IP ou par tout autre moyen poserait, à notre sens, de graves problématiques au regard de l'exigence de protection des données à caractère personnel voulue par la CJUE.

Ainsi, la surveillance ne devant pas concerner indistinctement tout les internautes, elle ne devrait pas *a priori* en concerner un seul, de sorte qu'il faut penser que la CJUE accepte qu'un groupe d'utilisateur puisse parfaitement faire l'objet d'une surveillance ciblée. Rappelons une fois de plus que la CJUE examine l'injonction sollicitée au regard de plusieurs critères, ce qui nous laisse à penser qu'une surveillance pourrait concerner un large public si les autres critères ne sont pas aussi absolus et permettent d'assurer un juste équilibre avec les droits et libertés fondamentales.

On pourrait ainsi imaginer, s'agissant d'une injonction adressée à un fournisseur d'accès à internet, qu'une mesure de surveillance ne concernant que les communications échangées sur le réseau *peer-to-peer* puisse s'étendre à l'ensemble des utilisateurs. Les clients du fournisseur d'accès n'utilisant pas tous le réseau *peer-to-peer*, les personnes l'utilisant constituent nécessairement un public distinct de l'ensemble de la clientèle. Ces observations demeurent toutefois purement hypothétiques.

¹³⁵ CJUE 12 juillet 2011, C-324/09 *L'Oréal c/ Ebay*, Consultable en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=57196>.

¹³⁶ Point 182 des Conclusions de l'Avocat général M. Niilo Jääskinen présentées le 9 décembre 2010 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83750&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=57317>.

¹³⁷ Que ce soit dans la directive 2004/48 dont il était question dans l'arrêt *L'Oréal c/ Ebay* ou que ce soit dans la directive 2001/31.

¹³⁸ En passant par exemple par un réseau privé virtuel (Virtual Private Network) ou par un serveur proxy, permettant de naviguer sur internet avec une adresse IP autre que celle fournie par le fournisseur d'accès.

¹³⁹ Point 182, *ibid.*

§4. Le coût de la surveillance

La CJUE retient également le critère du coût de la surveillance et fait grief, dans les arrêts *Scarlet* et *Netlog*, que celui-ci soit supporté par l'intermédiaire technique «à ses frais exclusifs». On sait que les considérations économiques justifient pour partie l'interdiction par la directive Commerce électronique d'imposer aux intermédiaires une obligation générale de surveillance¹⁴⁰ et la Cour de Justice ne fait ici qu'une exacte application de ce texte.

Pour autant, l'attention doit se porter sur l'adjectif «*exclusif*» employé, source possible de plusieurs interprétations. Quant à savoir si l'intermédiaire technique doit être intégralement ou partiellement déchargé de la charge financière, la Cour semble venir dire qu'un filtrage dont le coût ne serait pas supporté exclusivement par lui pourrait être validé. Effectivement, si la Cour avait voulu dire que l'intermédiaire technique n'avait pas à supporter, même partiellement, les frais liés à la mise en place d'un système de filtrage, elle se serait abstenue d'utiliser cette précision.

Reste à savoir qui doit supporter la charge financière du système de filtrage. Naturellement, les regards se tournent vers les titulaires des droits de propriété intellectuelle qui réclament la mise en place de mesures de filtrage.¹⁴¹ Ces derniers arguent toutefois que dans certains domaines, c'est l'État qui supporte la charge de compenser les coûts engagés par les intermédiaires techniques. On peut notamment citer le décret 30 décembre 2011¹⁴² qui en matière de sites de paris et de jeux d'argent vient préciser, à son article 2, que «*les éventuels surcoûts résultant des obligations mises à la charge des [fournisseurs d'accès] font l'objet d'une compensation financière prise en charge par l'Autorité de régulation des jeux en ligne*». De même, le décret du 25 février 2011¹⁴³ relatif à la conservation des données d'identification prévoit, à son article 10, que «*les surcoûts identifiables et spécifiques supportées par [les fournisseurs d'accès et les hébergeurs] font l'objet d'un remboursement par l'État...*». Ces remboursements ne sont toutefois possibles que dans le cadre de la lutte contre le terrorisme et ne s'applique pas aux autres demandes d'identification que peuvent recevoir ces intermédiaires techniques.¹⁴⁴ La prise en charge par l'État des coûts supportés par les intermédiaires techniques est en effet circonscrite aux cas de sauvegarde de l'ordre public. La jurisprudence du Conseil constitutionnel en la matière est intéressante. Amené à examiner la loi de finances rectificative pour 2001¹⁴⁵, les Sages censurèrent l'article 48 mettant à la charge des opérateurs de réseaux

¹⁴⁰ Nous renvoyons à nos développements ci-avant (Chapitre 1, Section 1).

¹⁴¹ Citons à ce propos Messieurs Jean-Pierre GASNIER et Olivier ROUX «*Chacun est responsable de sa propriété, fût-elle immatérielle. D'où vient qu'il faudrait en rendre un tiers responsable en faisant peser sur lui une obligation de surveillance générale et a priori de la chose ainsi détenue ?*» Libres propos autour des conclusions de l'Avocat général de la CJUE dans l'affaire eBay contre l'Oréal : *RLDI* févr. 2011/68, n° 2220.

¹⁴² Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025062583&dateTexte&categorieLien=id>.

¹⁴³ Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id>.

¹⁴⁴ Voir, pour plus de précisions, CASTETS-RENARD Céline, «Protection du droit d'auteur confrontée aux droits fondamentaux : point trop n'en faut !», *RLDI* 2012/79, n°2622.

¹⁴⁵ Cons. const., déc. n° 2000-441 DC, 28 déc. 2000 sur la loi de finances rectificative pour 2001 <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2000/2000-441-dc/decision-n-2000-441-dc-du-28-decembre-2000.460.html>.

de télécommunications le coût d'investissement ainsi qu'une partie du coût de fonctionnement des dispositifs d'interception de sécurité. Ils jugèrent que *«s'il est loisible au législateur, dans le respect des libertés constitutionnellement garanties, d'imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est étranger à l'exploitation des réseaux de télécommunications ; que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs»*.¹⁴⁶

La protection de la propriété intellectuelle ne semble pas relever de la sauvegarde de l'ordre public mais vise à protéger des intérêts privés, de sorte qu'il faut exclure l'intervention financière de l'État quant à la charge des dispositifs de surveillance étrangers à l'activité des intermédiaires techniques. Les titulaires des droits de propriété intellectuelle sont donc les acteurs à qui il doit incomber le coût de la surveillance.

Cette participation financière peut prendre en réalité diverses formes, tant sur les modalités que sur le partage des coûts avec l'intermédiaire technique. Elle reste à être définie au cas par cas ou suivant des recommandations que chaque acteur pourrait préconiser. En tout état de cause, cette question suppose une saine collaboration entre les titulaires des droits de propriété intellectuelle et les intermédiaires techniques.

Soulignons une nouvelle fois que dans les affaires *Scarlet* et *Netlog*, la Cour de Justice examine l'injonction litigieuse dans son ensemble, si bien qu'il n'est pas impossible qu'il soit demandé à un intermédiaire technique, dans certaines conditions, de supporter intégralement le coût de la surveillance, tant que l'équilibre avec les libertés fondamentales n'est pas rompu. Comme le dit justement Madame Castets-Renard, *«il n'est pas certain non plus que, face à des opérations de filtrage ponctuelles et limitées dans le temps, contrairement au cas d'espèce (...) la CJUE estime que les coûts engendrés soient réduits et ne constituent pas une réelle atteinte à cette liberté fondamentale»*.¹⁴⁷

§5. La surveillance préventive

La CJUE invalide en outre les injonctions litigieuses dans les affaires *Scarlet* et *Netlog* en ce qu'elles seraient prononcées *«à titre préventif»*. Il faut ici comprendre non pas que la Cour de Justice entend ne pas permettre la prévention de réitération d'un dommage mais la prévention de la réalisation hypothétique d'un dommage. En effet, la SABAM dans ces deux affaires avaient demandé au juge belge d'enjoindre au fournisseur d'accès à internet *Scarlet* et à l'hébergeur *Netlog* de procéder au filtrage et au blocage l'ensemble des oeuvres contenus dans le répertoire que cette société d'auteur gère. Une telle demande ne pouvait qu'aboutir à la censure de la CJUE et être assimilée, comme cette dernière le fait, à une obligation générale de surveillance. C'est donc ici une critère qui nous apparaît être de nature à invalider n'importe quelle demande d'injonction de filtrage.

Les arrêts *Scarlet* et *Netlog*, de part leur importance, eurent un écho favorable sur les juridictions nationales et notamment sur la Cour de Cassation.

¹⁴⁶ Considérant 41 de la décision précitée.

¹⁴⁷ CASTETS-RENARD Céline, *ibid.*

B. Les critères retenus par la Cour de Cassation

A regarder la récente jurisprudence de la Cour de Cassation, plus particulièrement ses arrêts du 12 juillet 2012, on peut s'apercevoir que la Cour régulatrice a pris acte de la jurisprudence de la CJUE. Alors que la jurisprudence des juges du fond en matière de prévention de réitération des contenus illicites était divergente voire audacieuse (§1), la Cour de Cassation est venue redonner une juste interprétation des textes permettant d'imposer une obligation particulière de surveillance (§2).

§1. L'état de la jurisprudence avant les arrêts du 12 juillet 2012

Face au problème de la réapparition de contenus illicites déjà signalés comme tels, les juges du fond ont été tentés d'imposer aux intermédiaires techniques une obligation de suppression définitive.

Ce développement du mécanisme de *notice and stay down*¹⁴⁸ fut initié dès 2007, par le TGI de Paris.¹⁴⁹ En l'espèce, les juges du fond reprochèrent à la société Google de ne pas avoir empêché la réapparition d'un contenu déjà signalé au motif qu'«*informée du caractère illicite du contenu en cause par la première notification, il lui appartenait de mettre en oeuvre tous les moyens nécessaires en vue d'éviter une nouvelle diffusion*» jugeant en outre que «*l'argumentation selon laquelle chaque remise en ligne constitue un fait nouveau nécessitant une nouvelle notification doit être écartée dans la mesure où, si les diffusions successives imputables à des utilisateurs différents, leur contenu et les droits de propriété intellectuelle y afférents sont identiques*». Ainsi, les ayants droit étaient dispensés de devoir effectuer une nouvelle notification si le contenu réapparaissait et pouvaient engager la responsabilité de l'hébergeur, à condition qu'il n'ait rien fait pour rendre son contenu à nouveau impossible. Cette même obligation incombant à l'hébergeur fut rappelée par le TGI de Paris¹⁵⁰, la Cour d'appel de Paris¹⁵¹, et d'autres juridictions.¹⁵²

Toutefois, l'obligation pour l'hébergeur était de mettre en oeuvre tous les moyens nécessaires en vue d'éviter une nouvelle réapparition, de sorte que celui-ci n'était pas tenu d'une obligation de résultat.¹⁵³ Certains juges refusèrent alors d'engager la responsabilité d'un hébergeur pour la réapparition de contenus déjà notifiés au motif que les ayants droit n'avaient pas souhaité fournir les empreintes numériques de leurs oeuvres pour que l'outil mis en place par l'hébergeur puisse les filtrer et les bloquer.¹⁵⁴

Reste que cette construction jurisprudentielle ne reposait sur aucun texte et était même *contra legem*. En effet, obliger les hébergeurs à empêcher la réapparition d'un contenu illicite revenait à court-

¹⁴⁸ L'expression s'inspire du modèle américain dans lequel l'intermédiaire qui reçoit la notification doit retirer le contenu notifier et empêcher sa réapparition.

¹⁴⁹ TGI Paris, 3ème chambre, 2ème section, 19 octobre 2007, n°06/11874.

¹⁵⁰ TGI Paris, 11 juin 2010, La Chauve-Souris et 120 Films c/ Dailymotion ; TGI Paris, 13 janv. 2011, Calt Production c/ Dailymotion ; TGI Paris, 3ème Chambre, 4ème section, 28 avril 2011.

¹⁵¹ CA Paris, 9 avr. 2010, Google c/ Flach Films et autres ; CA Paris, 3 déc. 2010, Dailymotion c/ Zadig Production ; CA Paris, 14 janv. 2011, Google Inc. c/ Bac Films et autres 09/11 729 et 09/11 779.

¹⁵² TGI Créteil, 14 déc. 2010, INA c/ YouTube.

¹⁵³ La Cour d'appel de Paris l'a ainsi jugé en ce sens dans diverses affaires. CA Paris, Pôle 5, chambre 2, 3 décembre 2010, n°06/12315 ; CA Paris, Pôle 5, chambre 2, 4 février 2011, Google Inc. et Aufeminin.com et autres c/ André Rau, H & K., n°09/21941 ; CA Paris Pôle 5, chambre 1, 9 mai 2012, n°10/12711.

¹⁵⁴ TGI Paris 3ème chambre, 4ème section, 28 avril 2011, SPFF c/ Youtube.

circuiter le mécanisme de notification préalable permettant de porter à l'hébergeur la connaissance d'un fait illicite et qui est au coeur du régime de responsabilité des intermédiaires techniques. Ainsi, cela revenait à imposer à ces hébergeurs une obligation générale de surveillance. Ce courant jurisprudentiel était aussi *contra legem* par rapport aux textes de la LCEN permettant d'imposer aux hébergeurs une surveillance ciblée afin que des contenus illicites déjà signalés réapparaissent.

Les arrêts de la Cour de Cassation du 12 juillet 2012 sont venus stopper cette oeuvre prétorienne pour revenir à une juste lecture des textes qui permettent d'imposer une surveillance ciblée aux intermédiaires techniques.

§2. L'apport des arrêts du 12 juillet 2012

Par trois arrêts intéressants cette question du *notice and stay down*, la Cour de Cassation vint mettre *knock down* l'élan jurisprudentiel présenté ci-avant.¹⁵⁵ La Cour régulatrice, dans des attendus similaires pour les trois décisions, casse les arrêts de la Cour d'appel de Paris.

La Haute juridiction retient, dans l'affaire *Google et Aufeminin.com c/ André Rau* qu'«*en se prononçant ainsi, quand la prévention et l'interdiction imposées à la société Aufeminin.com, en tant qu'hébergeur, et aux sociétés Google, en tant que prestataires de services de référencement, pour empêcher toute nouvelle mise en ligne de l'image contrefaisante, sans même qu'elles en aient été avisées par une autre notification régulière pourtant requise pour qu'elles aient effectivement connaissance de son caractère illicite et soient alors tenues d'agir promptement pour la retirer ou en rendre l'accès impossible, aboutit à les soumettre, au-delà de la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause, à une obligation générale de surveillance des images qu'elles stockent et de recherche des reproductions illicites et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps, la cour d'appel a violé les dispositions susvisées*».

Dans les deux affaires *Google c/ Bac Films*, la Cour de Cassation retient qu'«*en se prononçant ainsi, quand la prévention imposée aux sociétés Google pour empêcher toute nouvelle mise en ligne des vidéos contrefaisantes, sans même qu'elles en aient été avisées par une autre notification régulière pourtant requise pour qu'elles aient effectivement connaissance de son caractère illicite et de sa localisation et soient alors tenues d'agir promptement pour la retirer ou en rendre l'accès impossible, aboutit à les soumettre, au-delà de la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause, à une obligation générale de surveillance des images qu'elles stockent et de recherche des mises en ligne illicites et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps, la cour d'appel a violé les dispositions susvisées*».

¹⁵⁵ L'arrêt Cass. 1 Civ. 12 juillet 2012 pourvois n° **11-15.165** et **11.15.188** vient casser l'arrêt CA Paris, Pôle 5, chambre 2, 4 février 2011, Google Inc. et Aufeminin.com et autres c/ André Rau, H & K., n°09/2194 • L'arrêt Cass. 1 Civ. 12 juillet 2012 pourvoi n°**11-13.669** vient casser CA Paris, 14 janv. 2011, Google Inc. c/ Bac Films et autres. • L'arrêt Cass. 1 Civ. 12 juillet 2012 pourvoi n°**11-13.666** vient casser un autre arrêt du 14 janvier rendu par la Cour d'appel de Paris. (CA Paris, 14 janv. 2011, Google Inc. c/ Bac Films et autres).

La Cour de Cassation vient casser ces arrêts de Cour d'appel au visa des articles 6 I 2, 6 I 5 et 6 I 7 de la LCEN. Elle rappelle dans cet attendu l'économie de la LCEN, à savoir que la responsabilité de l'hébergeur ne peut être engagée qu'après une notification régulière, «*requisse pour qu'elles aient effectivement connaissance de son caractère illicite et soient alors tenues d'agir promptement pour la retirer ou en rendre l'accès impossible*». A défaut de suivre ces prescriptions, cela reviendrait à soumettre ces hébergeurs «*à une obligation générale de surveillance [des contenus qu'ils] stockent*», interdit en tant que tel par l'alinéa premier de l'article 6 I 7 de la LCEN.

Pour autant, la Cour de Cassation en profite pour préciser que ces obligations en l'espèce vont «*au-delà de la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause*». Elle rappelle ici, et c'est important, la possibilité offerte à l'alinéa 2 de l'article 6 I 7 de la LCEN pour l'autorité judiciaire d'imposer une activité de surveillance ciblée et temporaire.

En outre, les obligations de prévention litigieuses reviennent à prescrire aux hébergeurs, «*de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps*». Monsieur Cédric Manara fait remarquer que «*là où la juridiction européenne avait envisagé cinq critères pour rejeter une mesure de blocage, sans dire si l'un d'eux pouvait avoir plus d'importance qu'un autre, la Cour de Cassation considère que la seule circonstance qu'une demande de blocage ne soit pas limitée dans le temps suffit pour qualifier cette demande de disproportionnée par rapport au but poursuivi*». ¹⁵⁶ On peut toutefois penser que la Cour de Cassation se livre moins à une appréciation jurisprudentielle qu'à une stricte application de l'article 6 I 7, au visa duquel sont rendus ces arrêts, et qui exige à son alinéa 2 que ces mesures soient notamment temporaires.

La Cour de Cassation souligne également le fait que le filtrage doit être ciblé, lorsqu'elle rappelle la possibilité d' «*ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause*». La référence au «*contenu actuel du site*» implique que la surveillance doit concerner des fichiers identifiés. Elle implique en outre, et la référence faite au dommage le souligne aussi, que la mesure de surveillance doit concerner des contenus ayant déjà été contrefaits. Elle exclue ainsi la surveillance préventive au sens de la CJUE, à savoir la surveillance de répertoires entiers dont les oeuvres n'ont pas forcément fait l'objet d'une contrefaçon.

Dès lors que l'activité de surveillance, demandée par l'autorité judiciaire, est ciblée et temporaire et qu'elle est proportionnée au but poursuivi, celle-ci ne saurait être assimilée à une obligation de surveillance générale. La Cour d'appel de Paris semble avoir récemment fait un juste retour à cette règle. ¹⁵⁷

¹⁵⁶ MANARA Cédric, «La Cour de cassation fait obstruction au blocage de contenus par les hébergeurs», Dalloz Actualité, 18 juillet 2012.

¹⁵⁷ Cour d'appel de Paris, 21 juin 2013, SPPF c. Youtube <http://juriscom.net/wp-content/uploads/2013/06/caparis20130621.pdf>.

CONCLUSION DU TITRE I

Les intermédiaires techniques peuvent donc jouer un rôle central dans la lutte contre les atteintes répétées aux droits de propriété intellectuelle. Les mesures de surveillance qu'il est possible de leur imposer pour éviter la réapparition d'un contenu illicite ne sauraient toutefois être absolues. Elles devront ne pas être générales mais ciblées, temporaires et proportionnées au but poursuivi. En outre, les ayants droit les sollicitant à l'autorité judiciaire devront veiller à ce qu'elles ne portent pas atteintes aux droits et libertés fondamentales. Il leur appartiendra donc de limiter leurs prétentions afin qu'un juste équilibre soit trouvé et validé par le juge. Les intermédiaires techniques astreints à ces mesures de surveillance particulière pourront toutefois trouver des craintes légitimes quant à la nature et l'engagement de leur responsabilité suite à la mise en place de ces mesures techniques.

TITRE II. LA RESPONSABILITE DE L'INTERMEDIAIRE TECHNIQUE SUITE A LA MISE EN PLACE DE MESURES TECHNIQUES DESTINEES A PREVENIR ET FAIRE CESSER UNE ATTEINTE A DES DROITS DE PROPRIETE INTELLECTUELLE

La mise en place d'une mesure technique destinée à prévenir et faire cesser une atteinte à des droits de propriété intellectuelle pose la question de la responsabilité de l'intermédiaire technique, d'une part sur la compatibilité de ces mesures avec le bénéfice du régime de responsabilité attaché aux intermédiaires techniques (Chapitre 1) et d'autre part en cas de défaillance de ces dispositifs de filtrage (Chapitre 2).

Chapitre 1. La compatibilité des mesures de surveillance ciblée avec le régime de responsabilité des intermédiaires techniques

La mise en place de mesures de surveillance ciblée, quelle soit forcée ou volontaire, suscite des interrogations quant à savoir si ces mesures, en raison de leur nature, ne risquent pas de priver les intermédiaires techniques du bénéfice du régime spécial de responsabilité qui leur est reconnu par la directive Commerce électronique (Section 1). Ces doutes observés, il conviendra de reconnaître que ces mesures de surveillance ciblée doivent être nécessairement compatibles avec le régime de la responsabilité des intermédiaires techniques (Section 2).

Section 1. Les risques de la mise en place de mesures de filtrage sur le bénéfice du régime de responsabilité des intermédiaires

La mise en place de mesures de filtrage semble pouvoir remettre en cause à la fois l'activité des intermédiaires techniques, au regard de la définition donnée par les textes des services de la société de l'information (A) mais également la neutralité de ces intermédiaires techniques (B) ce qui aurait pour effet potentiel de priver ces derniers du régime favorable de responsabilité qui est censé leur être reconnu.

A. La mesure de filtrage au regard de la définition du service de la société de l'information

Les mesures de filtrage, entendues au sens large, ont pour objet d'identifier des contenus et de déterminer s'il y a lieu ou non de les bloquer, c'est-à-dire empêcher leur circulation ou leur accessibilité.

Les intermédiaires techniques sont, au sens de la directive Commerce électronique, les personnes qui réalisent les activités décrites aux articles 12, 13 et 14. Ces activités, si elles prennent des modalités différentes (fourniture d'accès, fourniture de cache, hébergement), consistent à fournir un service de la société de l'information. Il faut entendre par service de la société de l'information «*tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services*». ¹⁵⁸ Monsieur Cédric MANARA ¹⁵⁹, s'appuyant sur cette définition et celle donnée du terme «*voie électronique*» ¹⁶⁰ tire la conséquence que cette définition exclue par hypothèse les mesures de filtrage et de blocage. Pour cet auteur, un service de la société de l'information nécessite donc qu'il soit,

¹⁵⁸ Directive 98/48/CE du Parlement européen et du Conseil du 20 juillet 1998 portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques - Journal officiel n° L 217 du 05/08/1998 p. 0018 - 0026 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0048:FR:HTML>.

¹⁵⁹ MANARA Cédric, «Bloquer le filtrage ! Une approche critique des affaires Sabam», RLDI 2011/76, n°2533.

¹⁶⁰ «un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques», Directive 98/48/CE.

«envoyé à l'origine et reçu» et «entièrement transmis acheminé et reçu» comme l'indique la définition de voie électronique.

Dès lors, une mesure de filtrage-blocage ayant pour raison d'être d'analyser et éventuellement de bloquer, ne répondrait pas parfaitement à la définition du service de la société de l'information donnée par le législateur communautaire. Partant, ne délivrant pas véritablement un service de la société de l'information, ces prestataires ne pourraient être qualifiés d'hébergeur, de fournisseur d'accès ou de fournisseur de cache. Monsieur MANARA en tire cette conclusion : «*le régime découlant de la qualification, l'activité ainsi définie paraît exclusive de toute possibilité de blocage*».

Les mesures de filtrage suscitent également des interrogations, certainement plus pertinentes, quant à la neutralité de l'intermédiaire technique.

B. La mesure de filtrage au regard de la neutralité de l'intermédiaire technique

Une autre interrogation subsiste quant à savoir si les mesures de filtrage-blocage ne porteraient pas atteinte à la neutralité de l'intermédiaire technique et partant priveraient ce dernier du bénéfice du régime de responsabilité qui lui est attaché.

Le critère de neutralité est le fruit d'une construction jurisprudentielle, initiée par la CJUE et reprise depuis par les juridictions nationales, notamment françaises. Dans une décision du 23 mars 2010 «*Vuitton c/ Google Adwords*»¹⁶¹, les juges communautaires sont venus ajouter un nouveau critère pour bénéficier du régime de responsabilité des intermédiaires techniques. Outre le fait de devoir fournir un service de la société de l'information répondant aux activités définies aux articles 12 à 14 de la directive Commerce électronique, ces intermédiaires doivent également veiller à conserver un rôle neutre ou passif quant aux contenus qui transitent par leurs services. Les juges fondent leur décision en s'appuyant sur le considérant 42 de la directive Commerce électronique, lequel dispose que «*les dérogations en matière de responsabilité prévues par la présente directive ne couvrent que les cas où l'activité du prestataire de services dans le cadre de la société de l'information est limitée au processus technique d'exploitation et de fourniture d'un accès à un réseau de communication sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission. Cette activité revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées*».¹⁶²

La CJUE vient alors dire que «*l'article 14 de la directive 2000/31 doit être interprété en ce sens que la règle y énoncée s'applique au prestataire d'un service de référencement sur Internet lorsque ce prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées. S'il n'a pas joué un tel rôle, ledit prestataire ne peut être tenu responsable (...)*».¹⁶³ Quoique

¹⁶¹ CJUE 23 mars 2010, aff. C-236/08 à C-238/08, «Vuitton c/ Google AdWords» <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008J0236:FR:HTML>.

¹⁶² Nous soulignons.

¹⁶³ Point 120 de la décision. Nous soulignons.

critiquée par plusieurs commentateurs¹⁶⁴, la CJUE est venu conforter sa jurisprudence dans une affaire «Oréal c/ Ebay». ¹⁶⁵.

On peut s'interroger quant à savoir si la mise en place d'une mesure de filtrage est de nature à conférer un rôle actif à l'intermédiaire technique. Il s'avère bien difficile d'y répondre dans la mesure où les juges n'ont pas entendu apporter plus de précisions quant au sens à donner à ce rôle passif ou neutre. Le commentateur ne peut que se tourner vers la lettre du considérant 42 et y découvrir diverses interprétations aux conséquences multiples.

Le considérant 42 commence par venir caractériser l'activité du prestataire technique, laquelle doit revêtir un «*caractère purement technique, automatique et passif*». L'intermédiaire doit donc se borner à faire circuler les contenus et rester inerte. Les vocables employés semblent contredire sérieusement la possibilité de mettre en place des mesures de filtrage-blocage. En effet, ces mesures supposent un comportement alerte et non pas inerte pour intercepter les contenus. Soulignons d'ores et déjà que ce comportement alerte peut tout à fait être technique et automatique, dans la mesure où c'est un programme informatique qui vient identifier et bloquer les contenus reconnus. Malgré cela le législateur communautaire, avec ces termes, semble marteler l'idée d'un rôle «*purement*» neutre limitant les possibilités de recourir aux mesures de filtrage-blocage en faisant de l'intermédiaire un simple tuyau de communication.

Toutefois, la suite du considérant 42 donne plus de sens à ce rôle neutre que doit adopter l'intermédiaire technique car celui-ci doit permettre qu'il n'ait «*pas la connaissance ni le contrôle des informations transmises ou stockées*». Il faut d'abord faire remarquer que cette formule, en ce qu'elle serait récurrente, n'a pas voulu exprimer la même vision restrictive formulée ci-avant. Précisant que le rôle neutre devait conduire à ce que l'intermédiaire technique n'ait pas la connaissance ni le contrôle des informations, elle a nécessairement voulu distinguer deux interprétations que l'on peut donner de la neutralité. La première est celle déjà présentée, à savoir la thèse d'une neutralité absolue qui viendrait interdire tout contrôle et toute intervention. La seconde, est celle d'une neutralité relative, à savoir une neutralité qui n'interdirait pas qu'un contrôle technique soit mis en place, dès lors que la connaissance des contenus n'est pas intellectuelle. C'est la distinction qu'opère Monsieur Ronan HARDOUIN, distinguant la neutralité technique de la neutralité intellectuelle, celle-ci permettant «*de considérer que la neutralité ne découle pas nécessairement d'une inertie totale du prestataire mais de l'absence d'une 'influence intellectuelle' sur le contenu*». ¹⁶⁶ Partant, une mesure de filtrage-blocage ne serait qu'une vanne ajoutée sur le tuyau, permettant «*'une connaissance technique' mais excluant tout contrôle intellectuel*». ¹⁶⁷

Quoique les doutes ici présentés trouvent une certaine pertinence, il nous apparaît que les mesures de filtrage sont nécessairement compatibles avec le régime de la responsabilité des intermédiaires techniques.

¹⁶⁴ ROUHETTE Thomas et GATEAU Charles, «Le statut d'hébergeur en Europe, une insécurité juridique née de la difficile adaptation du droit à l'évolution technologique» : *RLDI* juin 2011/72, n° 2399. ; HARDOUIN Ronan, Du copulatif au passif ou comment la conjonction "et" ajoute une condition pour jouir du régime de l'hébergeur <http://juriscom.net/wp-content/documents/resp20100408.pdf>.

¹⁶⁵ CJUE, 12 juillet 2011, aff C-324/09 L'Oréal et a. c/ eBay et a. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009J0324:FR:HTML>.

¹⁶⁶ HARDOUIN Ronan, «Fascicule 464 : La responsabilité des intermédiaires techniques de l'internet», *Lamy droit des médias et de la communication* 2012.

¹⁶⁷ HARDOUIN Ronan, *ibid.*

Section 2. La nécessaire compatibilité des mesures de filtrage avec le régime de responsabilité des intermédiaires techniques

Les mesures de filtrage nous apparaissent effectivement compatibles avec le régime de responsabilité des intermédiaires techniques, que ces mesures soient ordonnées par le juge (A) ou qu'elles soient le fait volontaire des intermédiaires techniques eux-mêmes (B).

A. Le filtrage imposé par le juge : une possibilité conforme à la directive

Il semble évident que les mesures de filtrage sont compatibles avec la directive, nonobstant le fait que la définition des services de la société de l'information semble l'exclure. Le considérant 47 de la directive Commerce électronique, prévoit expressément la possibilité pour les autorités nationales de mettre en place des obligations de surveillance applicables à un cas spécifique.

En outre, les activités des fournisseurs d'accès à internet, des fournisseurs de cache et des hébergeurs, tels que définis aux articles 12 à 14 de la directive, n'excluent pas la possibilité pour ces derniers de se voir imposer une obligation de prévention de la réitération d'un fait illicite. En effet, ces mesures sont sans préjudice de l'activité des intermédiaires techniques, comme le précise la directive, respectivement pour les fournisseurs d'accès, les fournisseurs de cache et les hébergeurs, aux articles 12§3¹⁶⁸, 13§2¹⁶⁹, 14§3.¹⁷⁰

Toutefois, on peut s'interroger quant à savoir si la solution serait la même lorsque ces mesures de filtrage sont mises en place de la propre initiative des intermédiaires techniques.

B. Le filtrage volontaire : une possibilité laissée par la directive

La mise en place d'un dispositif de filtrage et de blocage à l'initiative d'un intermédiaire technique n'est pas rare. A dire vrai, c'est même l'accroissement de la mise en place volontaire de ces outils qui a conduit les juges à imposer de plus en plus des mesures de *notice and stay down* à leur égard.¹⁷¹

Face à la mise en place volontaire de mesures de filtrage par certains intermédiaires techniques, on peut s'interroger quant au sort de leur responsabilité. La directive Commerce électronique semble dans son considérant 40 encourager ces initiatives, affirmant qu' « *il est dans l'intérêt de toutes les parties qui participent à la fourniture de services de la société de l'information d'adopter et d'appliquer* » des « *mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci*

¹⁶⁸ Article 12§3 de la directive Commerce électronique : «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».

¹⁶⁹ Article 13§2 de la directive Commerce électronique : «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 fin à une violation ou qu'il prévienne une violation».

¹⁷⁰ Article 14§3 de la directive Commerce électronique : «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».

¹⁷¹ «*Il est impossible d'ignorer que la pratique s'est développée spontanément, preuve qu'elle n'est pas hors d'atteinte d'un prestataire diligent*», SIRINELLI Pierre, Chronique de jurisprudence, RIDA, oct. 2012, p. 465.

impossible». Elle ajoute que «*les dispositions de la présente directive sur la responsabilité ne doivent pas faire obstacle au développement et à la mise en oeuvre 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, dans le respect des limites établies par les directives 95/46/CE et 97/66/CE*».

D'après le législateur européen, les règles relatives à la responsabilité des intermédiaires techniques ne sauraient donc «*faire obstacle*» au développement des «*instruments techniques de surveillance*». Ces précisions plaident en faveur de la neutralité intellectuelle, en considérant que la communication au public d'un contenu ayant fait l'objet d'un contrôle technique *a priori* ne fait pas perdre le régime de responsabilité des intermédiaires techniques. Le bon sens commande effectivement qu'en présence d'intermédiaires techniques de bonne foi, le bénéfice de cette responsabilité atténuée leur soit reconnu. Ne pas reconnaître le rôle de bon père de famille que peuvent jouer ces acteurs de l'Internet serait contre-productif pour la lutte contre les atteintes aux droits de propriété intellectuelle. Chacun y trouve son compte, tant les titulaires de droits intellectuels que les intermédiaires techniques qui préservent ainsi leur image de marque.¹⁷² Aussi, la diligence de l'intermédiaire doit lui profiter ce que reconnaît par exemple la Cour d'appel de Californie qui considère qu'un hébergeur ne doit pas voir sa responsabilité engagée s'il met en oeuvre des mesures proactives pour lutter contre la contrefaçon.¹⁷³

En outre, ces mesures volontaires ne semblent pas contredire l'exigence de se comporter en opérateur diligent, standard dégagé par la CJUE¹⁷⁴ et présenté par certains auteurs comme l'équivalent du bon père de famille.¹⁷⁵ La Cour de Justice vient en effet reconnaître une certaine obligation de vigilance en affirmant qu'un intermédiaire technique n'ayant pas joué de rôle actif ne peut se prévaloir de son exonération de responsabilité «*s'il a eu connaissance de faits ou de circonstances sur la base desquels un opérateur économique diligent aurait dû constater l'illicéité des offres à la vente en cause et, dans l'hypothèse d'une telle connaissance, n'a pas promptement agi*».¹⁷⁶

S'il convient de considérer que la nature des mesures de filtrage que peut mettre en place, de gré ou de force, un intermédiaire technique ne remet pas en cause la nature de ses activités et partant ne le prive pas du bénéfice du régime de responsabilité qui lui est favorable, reste à voir les hypothèses multiples de responsabilité qui peuvent se présenter à lui en cas de défaillance d'une mesure de filtrage.

¹⁷² MONTERO Etienne, «La responsabilité des prestataires intermédiaires sur les réseaux», in *Le commerce électronique européen sur les rails ? Analyse et propositions de mise en oeuvre de la directive sur le commerce électronique*, Bruxelles, Bruylant, 2001, p. 279.

¹⁷³ Cour d'appel de Californie, *Lars Gentry c/eBay Inc.*, 26 juin 2002.

¹⁷⁴ CJUE, 12 juillet 2011, aff C-324/09 *L'Oréal et a. c/ eBay et a.*

¹⁷⁵ C'est pour le Professeur Pierre-Yves GAUTIER le «traditionnel bon père de famille du Code civil», De l'éventuel « rôle actif » des **opérateurs** internet dans la réalisation du dommage (qualification de responsabilité civile), D. 2011, point de vue p. 2054, n° 3 ; Madame Céline CASTETS-RENARD présente l'opérateur diligent comme une sorte de «*bon père de famille de l'économie numérique*», «Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet», *Recueil Dalloz* 2012, p. 827.

¹⁷⁶ Point 124 de l'arrêt.

Chapitre 2. La responsabilité de l'intermédiaire technique en cas de défaillance des mesures de filtrage

Une fois mises en place, les mesures de filtrage peuvent s'avérer défaillantes, que ce soit à l'égard d'un contenu qu'elles auraient dû bloquer ou que ce soit à l'égard d'un contenu qu'elles n'auraient pas dû bloquer. Ces défaillances posent alors la question de la responsabilité de l'intermédiaire technique tant à l'égard des ayants droit, mécontents de constater une violation de leurs droits de propriété intellectuelle (Section 1) que des internautes, mécontents de constater qu'une de leur communication en ligne ait fait l'objet d'un blocage (Section 2).

Section 1. La responsabilité de l'intermédiaire technique à l'égard des ayants droit

Confrontés à une défaillance du système de filtrage ne bloquant pas un contenu violant des droits de la propriété intellectuelle, les ayants droit pourraient chercher à engager la responsabilité de l'intermédiaire technique. Si cette responsabilité de l'intermédiaire technique apparaît possible (A), il faut relever que dans la recherche d'une lutte conjointe contre les atteintes aux droits de la propriété intellectuelle, celle-ci s'avère contre-productive (B).

A. Une responsabilité de l'intermédiaire technique possible

Ayant obtenu d'un juge qu'un intermédiaire technique mette en place une mesure technique destinée à prévenir une atteinte à ses droits de propriété intellectuelle, l'ayant droit qui constaterait la défaillance de la mesure technique par la réapparition en ligne du même contenu pourrait engager la responsabilité de cet intermédiaire. Cette responsabilité apparaît toutefois draconienne pour l'intermédiaire technique (§1) et conduit à lui conférer un rôle dépassant ses compétences (§2).

§1. Une responsabilité draconienne pour l'intermédiaire technique

La responsabilité de l'intermédiaire technique apparaît draconienne dans la mesure où il est impossible de garantir l'efficacité d'un système de filtrage (a) et qu'en outre il s'avère impossible de déterminer un niveau de filtrage acceptable (b).

a. L'impossibilité de mettre en place un filtrage parfait

Faire peser la charge à l'intermédiaire technique d'empêcher toute remise en ligne d'un contenu déjà signalé comme illicite revient à considérer que les dispositifs de filtrage sont efficaces à 100%. Or, l'efficacité prêtée à ces dispositifs de filtrage est loin d'être absolue et cela de l'avis même de certaines juridictions.¹⁷⁷

S'il est difficile de filtrer des personnes, il est encore plus difficile de filtrer des contenus. Or, les applications de filtrage proposées sur le marché ne se valent pas toutes. Ainsi, dans l'arrêt *Scarlet*, l'Avocat général Monsieur Pedro Cruz Villalón citait le rapport d'expertise au sujet des dispositifs de filtrage, lequel

¹⁷⁷ Au sujet des seules mesures de filtrage destinées à restreindre l'accès à des contenus à certains visiteurs, on peut citer, telles que rapportées par Monsieur MANARA («Bloquer le filtrage ! Une approche critique des affaires *Sabam*», *RLDI* 2011/76, n°2533.), les décisions suivantes : En France, TGI Paris, référé 20 novembre 2000 ; En Allemagne, Bayerischer Verwaltungsgerichtshof, 7 mai 2007, 24 CS 07.10 ; En Hollande, Rechtbank Zwolle-Lelystad, 3 mai 2006 N°AW6288, Stokke c/ Maarkplats.

soulignait qu' «à l'exception de la solution proposée par Audible Magic, toutes les solutions tentent d'empêcher l'utilisation des réseaux peer-to-peer, indépendamment du contenu qui y est véhiculé». ¹⁷⁸ Pis encore, le même expert ajoutait que «la pérennité des solutions de filtrage d'application peer-to-peer est loin d'être assurée sur le moyen terme (2-3 ans)». ¹⁷⁹ Ainsi, les intermédiaires techniques seraient liés dans leur choix du fournisseur d'application de filtrage, en raison des capacités inégales mais ils ne seraient pas garantis à 100% de leur efficacité, les techniques de contournement s'améliorant. ¹⁸⁰ La Commission européenne, dans son premier rapport sur l'application de la directive Commerce électronique soulignait ce fait : «il est important de noter que les rapports et études sur l'efficacité des logiciels de blocage et de filtrage semblent indiquer qu'il n'existe pas encore, à l'heure actuelle, de technologies qui ne puissent être contournées et qui permettent de bloquer ou de filtrer de façon tout à fait efficace les informations illicites et préjudiciables, tout en évitant de bloquer des informations tout à fait légales, ce qui porterait atteinte à la liberté d'expression». ¹⁸¹ Malgré tout, les intermédiaires seraient tenus de leur efficacité à l'égard des ayants droit ! Il semblerait qu'ainsi l'adage qui veut qu'à l'impossible nul ne soit tenu ne s'applique pas pour les intermédiaires techniques. Comme le relève Monsieur Cédric MANARA : «À rebours du principe *lex cogit ad non impossibilia*, cela revient à devenir responsable du fait qu'il n'existe pas de système efficace». ¹⁸²

L'autre difficulté que pose la question de la responsabilité des intermédiaires techniques est de savoir avec quel degré de tolérance ils doivent filtrer des contenus identifiés.

b. L'impossibilité de déterminer un filtrage acceptable

La mise en place d'un dispositif de filtrage-blocage comporte deux étapes. L'étape de filtrage consiste en une phase d'identification de contenus correspondant à des occurrences contenues dans la base de données des empreintes numériques. En fonction de la précision que permet le dispositif ou que va choisir l'intermédiaire, les résultats remontant seront différents. Il sera par exemple possible, non seulement de détecter une oeuvre reproduite en entier, mais aussi un extrait de cette oeuvre.

L'intermédiaire technique va-t-il devoir bloquer seulement les fichiers reproduisant l'oeuvre en son intégralité ou devra-t'il s'assurer que des extraits de celle-ci ne puissent pas circuler ou être stockés ? Que l'oeuvre soit reproduite en entier ou de façon partielle, c'est bien l'oeuvre qui est contrefaite de nouveau, quoique d'une façon différente. Dès lors, l'intermédiaire technique devrait bloquer également la réapparition de simples extraits de l'oeuvre. Imaginer que la règle juridique soit moins contraignante reviendrait en outre à laisser la possibilité pour les contrefacteurs de remettre en ligne un contenu, par exemple une vidéo, sous forme d'extraits multiples qui, ensemble, reconstitueraient l'oeuvre en son intégralité.

¹⁷⁸ Conclusions de l'Avocat Général M. Pedro Cruz Villalón dans l'affaire C-70/10, CJUE 24 novembre 2011, «Scarlet / S A B A M», point 21 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=81776&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=364346>.

¹⁷⁹ *Ibid.*

¹⁸⁰ Parfois même avant la mise en place d'un dispositif de filtrage, on évoque les possibilités qu'auront les internautes les plus avertis de les contourner, comme dans l'affaire *Twentieth Century Fox v British Telecom* EWHC 1981 (Ch), 28 juillet 2011 http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/28_07_11_bt_newzbin_ruling.pdf.

¹⁸¹ Premier rapport sur l'application de la 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 »), 21 nov. 2003, page 15.

¹⁸² MANARA Cédric, précité.

Reste à savoir quel filtrage acceptable doit adopter l'intermédiaire technique. Que doit-il décider s'il détecte qu'un nouveau contenu reprend une infime quantité de l'oeuvre marquée, par exemple 5 secondes ou 5% d'un contenu audio ou vidéo ? Il apparaît bien difficile de savoir où commence et où s'arrête la contrefaçon. Comme le note le Professeur Valérie-Laure BENABOU, «*sur le plan théorique, il est extrêmement difficile de déterminer à partir de quand une oeuvre devient telle ou encore, à l'inverse, jusqu'où il est loisible de la dépecer pour tomber en deçà du seuil permettant d'aboutir à une telle qualification*». ¹⁸³

Sur le plan pratique, cette responsabilité de l'intermédiaire revient à lui conférer un rôle dépassant ses compétences.

§2. Une responsabilité dépassant les compétences de l'intermédiaire technique

Confronté dans le cadre d'une injonction à prévenir toute réapparition d'un contenu déjà signalé comme illicite, l'intermédiaire technique se retrouve à déterminer si un contenu reprenant peu ou prou celui déjà signalé doit être bloqué ou non.

La réaction de l'intermédiaire devrait être celle de s'interroger quant à savoir si le contenu est manifestement illicite ¹⁸⁴ et, en cas de réponse par la positive, le retirer. Toutefois, la jurisprudence tend à faire de l'intermédiaire technique un juge de la certitude ¹⁸⁵, l'obligeant à retirer quand bien même l'illicéité n'est pas manifestement apparente, poussant celui-ci à une réaction d'autodéfense conduisant le plus souvent à retirer le contenu signalé. Ce phénomène n'est pas seulement propre aux intermédiaires français mais s'observe aussi dans d'autres pays de l'Union européenne. ¹⁸⁶ Transposé à notre situation, à savoir celle d'un intermédiaire ayant reçu une injonction d'empêcher qu'un contenu signalé comme illicite réapparaisse, il semble peu probable que celui-ci s'attache à jouer son rôle de gardien de la liberté d'expression. ¹⁸⁷

Cette situation de fait a pour conséquence de créer un risque de censure privée ¹⁸⁸ réalisée par les intermédiaires techniques, préférant ne pas prendre le risque de voir leur responsabilité engagée par les ayants droit quitte à porter atteinte aux droits des internautes, clients ou utilisateurs.

¹⁸³ BENABOU Valérie-Laure, «L'oeuvre poulpe», *RDTI*, 2009, n° spécial 32.

¹⁸⁴ THOUMYRE Lionel, "Comment les hébergeurs français sont devenus juges du manifestement illicite", *Juriscom*, 28 juillet 2004 <http://juriscom.net/2004/07/comment-les-hebergeurs-francais-sont-devenus-juges-du-manifestement-illicite/>.

¹⁸⁵ Nous renvoyons ici à l'étude de Monsieur Ronan HARDOUIN, «La connaissance de l'illicéité par les hébergeurs ou quand être notifié ne signifie pas nécessairement devoir retirer», *RDTI* N12/2, Juillet 2012.

¹⁸⁶ A titre d'exemple, Bits of Freedom demanda en 2004 à 10 intermédiaires techniques de retirer un texte d'un auteur tombé dans le domaine public (connu comme tel) en se faisant passer pour le représentant légal dudit auteur. 70% des intermédiaires techniques sollicités retirèrent le contenu suite à la notification reçue par l'e-mail. <http://www.bof.nl/docs/researchpaperSANE.pdf>.

¹⁸⁷ TABAKA Benoît, «L'hébergeur, gardien de la liberté d'expression. La preuve par l'exemple», <http://tabaka.blogspot.fr/2011/08/lhebergeur-gardien-de-la-liberte.html>.

¹⁸⁸ Monsieur Cédric MANARA relève que «L'évacuation de toute possibilité d'appréciation sur le sort de la circulation d'une oeuvre a pour effet de transformer l'intermédiaire en censeur de fait», MANARA Cédric, «Bloquer le filtrage ! Une approche critique des affaires *Sabam*», *RLDI* 2011/76, n°2533.

Dangereuse pour les intermédiaires techniques, cette responsabilité est en outre contre-productive dans la lutte contre les atteintes aux droits de propriété intellectuelle sur Internet.

B. Une responsabilité de l'intermédiaire technique contre-productive

L'engagement de la responsabilité de l'intermédiaire technique en cas de réapparition d'un contenu illicite, nonobstant la mise en place d'un dispositif de filtrage, ne serait qu'une mesure sanctionnatrice stérile. L'intermédiaire technique ne devrait être tenu qu'à une obligation de moyen dans la mise en place d'un système de filtrage (1) et ce d'autant plus qu'une collaboration avec les ayants droit se révèle nécessaire (2).

§1. Une responsabilité de l'intermédiaire devant être limitée à une obligation de moyen

L'intermédiaire technique qui met en place, à la suite d'une injonction judiciaire, une mesure de filtrage afin de prévenir et empêcher la réitération de l'illicite ne devrait pas se voir imposer une obligation de résultat. Le caractère approximatif des solutions de filtrage et leurs caractéristiques différentes ne devraient effectivement pas rendre responsable l'intermédiaire de leur hypothétique défaillance intrinsèque. Partant, une obligation de moyen à la charge de l'intermédiaire technique, l'obligeant à faire tout son possible pour empêcher la réitération de l'illicite ne serait qu'en cas d'irrespect que la seule cause permettant d'engager sa responsabilité. Cette obligation de moyen aurait pour but de s'assurer que l'intermédiaire technique mette tous les moyens en oeuvre pour implanter correctement le dispositif de filtrage et le faire fonctionner efficacement. Les juges du fond qui reconnaissent une obligation de *notice and stay down* aux intermédiaires techniques précisent d'ailleurs qu'ils n'étaient pas tenus d'une obligation de résultat.¹⁸⁹

Ajoutons en outre qu'au regard des jurisprudences *Scarlet* et *Netlog*, l'intermédiaire technique n'a pas à supporter exclusivement les frais liés à la mise en place ou au fonctionnement de la mesure de filtrage. Sans savoir exactement ce qu'entend ici la CJUE, l'on sait que l'ayant droit devra, à tout le moins supporter une partie ou la totalité de ces frais. Dans les deux hypothèses, il semble que l'ayant droit ait un pouvoir d'appréciation sur la solution technique retenue, le choix de telle ou telle mesure de filtrage impactant sur les frais financiers engagés.

On se rend donc compte que les ayants droit seront amenés inévitablement à collaborer avec les intermédiaires techniques pour mettre en place le système de filtrage désiré.

§2. Une collaboration nécessaire des ayants droit pour la mise en place d'un système de filtrage

La mise en place d'un système de filtrage nécessite la collaboration des ayants droit avec les intermédiaires, pour la mise en oeuvre technique de ces dispositifs (a). Ces collaborations sont en outre vivement encouragées pour être prises sous la forme de charte (b).

¹⁸⁹ CA Paris, Pôle 5, chambre 2, 3 décembre 2010, n°06/12315 ; CA Paris, Pôle 5, chambre 2, 4 février 2011, Google Inc. et Aufeminin.com et autres c/ André Rau, H & K., n°09/21941 ; CA Paris Pôle 5, chambre 1, 9 mai 2012, n°10/12711.

a. Une collaboration technique nécessaire

La collaboration entre les ayants droit et les intermédiaires techniques est nécessaire d'abord pour des raisons techniques. L'ayant droit se plaignant d'un contenu violant ses droits de propriété intellectuelle doit apporter matériellement à l'intermédiaire technique une copie de cette oeuvre pour qu'il puisse ajouter à sa base de données des oeuvres à identifier l'empreinte numérique de celle-ci. Le TGI de Paris a eu l'occasion de refuser de reconnaître responsable l'intermédiaire technique qui n'avait pas empêché la réapparition d'un contenu violant des droits de propriété intellectuelle déjà notifié, au motif que l'ayant droit n'avait pas accepté d'utiliser l'outil de signalement que l'hébergeur mettait à sa disposition.¹⁹⁰ Dans un commentaire de cette décision, Madame Anne DEBET¹⁹¹ relève que si l'hébergeur en question, YouTube, exige que les ayants droit lui fournissent une empreinte numérique du fichier, Dailymotion réalise quant à lui une empreinte directement sur son site des contenus qui lui sont signalés. Si la solution technique est possible, il faut toutefois préférer attendre de l'ayant droit la communication de l'empreinte numérique de l'oeuvre contrefaite. Elle permet de s'assurer que le fichier soit de qualité et ne soit pas modifié, assurant ainsi de meilleures conditions techniques pour qu'un contenu contrefaisant soit identifié. La Cour d'appel de Paris vient récemment de confirmer la décision des juges du fonds, retenant que *«s'agissant, par ailleurs, de la contestation du jugement en ce qu'il fait grief à la SPPF de n'avoir pas souscrit à la proposition que lui faisait la société Youtube et qui portait sur un outil permettant la reconnaissance de contenus à partir d'empreintes, c'est par motifs pertinents que la cour adopte que les premiers juges ont considéré que cette abstention pouvait lui être imputée à faute»*.¹⁹²

Ce type de collaboration est également imaginable de façon préventive, alors qu'aucun agissement de contrefaçon n'a été constaté. Comme le note le Professeur Christophe CARON, l'intermédiaire technique *«peut tout à fait s'engager dans la voie d'une saine collaboration avec les titulaires de droits qu'il convient d'encourager car tout le monde a intérêt à ce que la concorde l'emporte sur la discorde»*.¹⁹³ Ces initiatives sont d'ailleurs de plus en plus encouragées par les institutions.

b. Une collaboration pouvant prendre la forme de charte

La concorde entre les ayants droit et les intermédiaires techniques aurait des vertus que vantent bon nombre d'institutions. Leurs encouragements à la *soft law* ne tarissent pas, appelant aux dialogues entre les

¹⁹⁰ TGI Paris, 3ème Chambre, 4ème section, 28 avril 2011, SPPF c/ Youtube.

¹⁹¹ DEBET Anne, «Responsabilité des sites de partage de vidéos : les représentants des ayants droit doivent coopérer», *Communication Commerce Électronique*, n°7, Juillet 2011, comm. 67.

¹⁹² Cour d'appel de Paris, 21 juin 2013, SPPF c. Youtube
<http://juriscom.net/wp-content/uploads/2013/06/caparis20130621.pdf>.

¹⁹³ CARON Christophe, «Responsabilité des hébergeurs : requiem pour le «take down, stay down», *Communication Commerce Électronique*, n°9, Septembre 2012, comm. 91.

intéressés¹⁹⁴ ou à la coopération.¹⁹⁵ Les professionnels appellent de leurs vœux l'élaboration de chartes¹⁹⁶ et la doctrine ne voit pas cela d'un mauvais œil.¹⁹⁷ Rappelons que la directive Commerce électronique, tant dans ses considérants¹⁹⁸ que dans ses articles¹⁹⁹, n'empêche pas d'y recourir. On peut citer à cet égard l'initiative d'acteurs du commerce électronique et de titulaire de droits de la propriété intellectuelle de signer un *Memorandum of Understanding*²⁰⁰ pour collaborer afin de lutter contre la vente de produits contrefaits en ligne. Cette initiative est citée en exemple par la Commission européenne²⁰¹, laquelle considère que «*la collaboration entre parties prenantes, en particulier les prestataires de l'Internet, les ayant-droit et les services de paiements, engagée dans l'Union européenne et aux Etats-Unis, peut aussi permettre de lutter contre les contenus illégaux*».²⁰²

Ces chartes ne visent d'ailleurs pas exclusivement à lutter contre les actes de contrefaçon mais permettent aussi pour les ayants droit de trouver un financement sur leurs contenus publiés à leur insu. La solution ContentID²⁰³ de Youtube permet ainsi pour les intermédiaires techniques de demander le blocage de leurs oeuvres ou d'obtenir une monétisation sur ces contenus, en récoltant les revenus publicitaires découlant de leur visionnage. Les ayants droit y trouvent un intérêt certain, passant des accords avec la plateforme de vidéo Youtube et préférant dans la majorité monétiser leurs contenus plutôt que de les bloquer.²⁰⁴ Dailymotion a également passé des accords avec les principaux ayants droit qui utilisent sa technologie de filtrage Audible Magic : «*Dailymotion a signé des accords historiques avec les principales*

¹⁹⁴ Communication de la commission, « Renforcer l'application des droits de propriété intellectuelle sur le marché intérieur » (COM(2009) 467 final), 11 septembre 2009, page 10, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0467:FIN:FR:PDF>.

¹⁹⁵ Communication de la Commission, Doper la créativité et l'innovation pour permettre à l'Europe de créer de la croissance économique, des emplois de qualité et des produits et services de premier choix, COM(2011) 287 final, 24 mai 2011, pages 22 et 23 http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_fr.pdf.

¹⁹⁶ SIRINELLI Pierre, «Propriété littéraire et artistique - Chronique», *Recueil Dalloz* 2011 p.2164.

¹⁹⁷ «*La soft law pourrait être d'un grand secours : l'idée d'élaborer des chartes ou des codes de bonne conduite est excellente. La négociation contractuelle serait encore plus fructueuse, y compris au sens financier du terme : rêvons à la conclusion d'accords entre les ayants droit et les hébergeurs*», MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 18 octobre 2012, n°292, p. 12.

¹⁹⁸ Considérant 40 «*(...) La présente directive doit constituer la base adéquate pour l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible. Il conviendrait que de tels mécanismes soient élaborés sur la base d'accords volontaires négociés entre toutes les parties concernées et qu'ils soient encouragés par les Etats membres. Il est dans l'intérêt de toutes les parties qui participent à la fourniture de services de la société de l'information d'adopter et d'appliquer de tels mécanismes. 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, dans le respect des limites établies par les directives 95/46/CE et 97/66/CE*».

¹⁹⁹ Article 16 «*1. Les États membres et la Commission encouragent: a.) l'élaboration, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs, de codes de conduite au niveau communautaire, destinés à contribuer à la bonne application des articles 5 à 15*».

²⁰⁰ Memorandum of Understanding, 4 may 2011, http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf.

²⁰¹ Communication de la commission 2011-942 «Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne», page 14.

²⁰² Communication de la commission, *ibid.* page 15.

²⁰³ La solution ContentID est présenté comme permettant de «[Bloquer] et [monétiser]» ses contenus <http://www.youtube.com/t/contentid>.

²⁰⁴ Content ID : le watermark de YouTube adopté par six studios français, NUMERAMA, 24 juin 2009 <http://www.numerama.com/magazine/13264-content-id-le-watermark-de-youtube-adopte-par-six-studios-francais.html>.

sociétés d'auteurs : l'ADAGP, la SACD, la SCAM, la SACEM-SDRM-SESAM et la SAIF. En vertu de ces différents accords, ces sociétés d'auteurs perçoivent des droits d'auteurs auprès de Dailymotion pour les œuvres de leur répertoire proposées sur le site. Ces accords sont les premiers du genre négociés entre sociétés d'auteurs et une plateforme de partage de vidéos et illustrent parfaitement la coexistence bénéfique entre le légitime respect des droits des auteurs et la formidable opportunité de circulation des œuvres et d'accès à la connaissance qu'offre Internet». ²⁰⁵

Reste à savoir quelle est la valeur normative de tels engagements. Les parties les veulent bien souvent dépourvus de toute force contraignante ²⁰⁶, mais comme le note Madame Céline CASTETS-RENARD «rien n'empêcherait un juge d'imposer le respect des engagements pris, en raison de la confiance légitime qu'ils ont fait naître». ²⁰⁷ La Cour de Cassation a en effet déjà pu retenir qu'un engagement même moral pouvait être qualifié d'obligation civile : «Mais attendu qu'en s'engageant, fût-ce moralement, "à ne pas copier" les produits commercialisés par la société Créations Nelson, la société Camaieu International avait exprimé la volonté non équivoque et délibérée de s'obliger envers la société concurrente ; que la cour d'appel, qui n'encourt aucun des griefs du moyen, en a donc exactement déduit que cette clause avait une valeur contraignante pour l'intéressée et qu'elle lui était juridiquement opposable ; que le moyen n'est pas fondé». ²⁰⁸ Mesdames Alexandra BENSAMOUN et Célia ZOLYNSKY relèvent à propos de cet arrêt que «l'affirmation rappelle que l'intention des parties n'est pas le seul critère de juridicité : celle-ci peut être admise, même en cas de volonté contraire des parties à l'acte. Elle rappelle encore que la qualification n'est pas la chose des parties, mais bien celle du juge.»

Quoiqu'en disent les parties donc, les accords et chartes de conduite pourraient se révéler contraignants. Ce faisant, ils donnent de l'intérêt à recourir à la *soft law*, lui donnant une certaine réalité juridique et renforçant la confiance que peuvent avoir chaque parties prenantes. Toutefois, la collaboration suppose de prendre également en compte les intérêts et droits des internautes, au risque pour l'intermédiaire technique de voir sa responsabilité engagée par eux.

Section 2. La responsabilité de l'intermédiaire technique à l'égard des internautes

L'intermédiaire technique doit également veiller lors de la mise en place d'une mesure de filtrage à ne pas venir porter atteinte aux droits et libertés des internautes, qu'ils soient à son égard clients ou simplement utilisateurs. Dans le cas contraire, ces derniers pourraient fort bien engager la responsabilité de l'intermédiaire technique (A) d'où la nécessité d'intégrer les internautes dans le processus de filtrage-blocage afin de leur permettre de formuler des observations (B).

²⁰⁵ Dailymotion <http://www.dailymotion.com/fr/legal/contentprotection>.

²⁰⁶ Citons ainsi le Memorandum of Understanding qui dans son préambule précise «*This MoU is limited to each signatory to the extent that it provides services in the Member States of the European Union / European Economic Area. It is not legally binding and does not now nor in the future create any contractual or pre-contractual obligations under any law or legal system*».

²⁰⁷ CASTETS-RENARD Céline, «Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet», *Recueil Dalloz* 2012, p. 827.

²⁰⁸ Cass. com., 23 janv. 2007, n° 05-13.189, Bull. IV, n° 12.

A. Une responsabilité de l'intermédiaire technique possible

La responsabilité de l'intermédiaire technique à l'égard des internautes peut se voir engager en cas de défaillance du système de filtrage, c'est-à-dire lorsque un contenu licite n'est pas reconnu comme tel et est alors bloqué. Ce risque de «faux positif» est bien réel en matière de protection de la propriété intellectuelle (§1) et conduit à restreindre la liberté d'expression et de communication des internautes (§2).

§1. Le risque de «faux positif»

La défaillance du dispositif de filtrage-blocage dans la détection de véritables contenus illicites est bien réelle. Elle est même la conséquence du perfectionnement de ces dispositifs qui, venant de mieux en mieux détecter les oeuvres contrefaites, détectent des contenus qui ne contrefont pas des oeuvres. Les exemples de ces «faux positifs» trouvent un large écho auprès des internautes. Parmi les plus ubuesques, on peut citer la mésaventure d'un vidéaste champêtre qui eu la surprise de constater que YouTube avait détecté que les chants d'oiseaux que l'on entendait sur sa vidéo violaient des droits d'auteur.²⁰⁹ Ou bien le retrait de la vidéo de la NASA montrant l'amarsissage de Curiosity qui aurait violé les droits de propriété intellectuelle d'une chaîne de télévision qui ne faisait que réutiliser les images de la NASA.²¹⁰ Ces illustrations montrent bien que ces dispositifs de filtrage jouent un rôle automatique et purement technique.

A dire vrai, la difficulté relève moins de la complexité technique que de la complexité juridique propre à la propriété intellectuelle. Pareille problématique avait été relevée par la CJUE dans son arrêt *Scarlet* lorsqu'elle affirmait que *«la licéité d'une transmission dépend également de l'application d'exceptions légales au droit d'auteur qui varient d'un État membre à l'autre. En outre, certaines œuvres peuvent relever, dans certains États membres, du domaine public ou elles peuvent faire l'objet d'une mise en ligne à titre gratuit de la part des auteurs concernés»*.²¹¹ Les dispositifs de filtrage ne distingueront pas non plus les réutilisations d'oeuvre autorisées par leurs auteurs ou les contenus relevant du genre de la pastiche, de la parodie ou de la caricature et qui bénéficient d'une exception légale.²¹² Pire encore, une oeuvre marquée dans le système d'empreintes, qui utiliserait un élément du domaine public, pourrait empêcher une autre oeuvre de l'utiliser, croyant que ce «tout» qu'est l'oeuvre est entièrement protégé.

Pour se rendre compte de l'ampleur de ces méandres, Monsieur Cédric MANARA, s'appuyant sur les travaux de Monsieur Smári McCarthy²¹³, livre ce chiffre : 10 460 353 203. *«Il s'agit du nombre minimal de combinaisons différentes auxquelles pouvait donner lieu la transposition de la directive «droit d'auteur dans la société de l'information. (...) Pour parvenir à ce chiffre, il faut d'abord tenir compte des 21 exceptions optionnelles au droit de reproduction du texte : les États pouvaient choisir ou non de les transposer, ce qui*

²⁰⁹ Sur YouTube, les chants d'oiseaux sont protégés par le droit d'auteur, NUMERAMA, 27 février 2012 www.numerama.com/magazine/21823-sur-youtube-les-chants-d-oiseaux-sont-proteges-par-le-droit-d-auteur.html.

²¹⁰ La NASA censurée sur YouTube pour piratage de sa propre vidéo, NUMERAMA, 7 août 2007, www.numerama.com/magazine/23351-la-nasa-censuree-sur-youtube-pour-piratage-de-sa-propre-video.html.

²¹¹ Point 52 de l'arrêt *Scarlet*.

²¹² Article L122-5 4° du Code de la propriété intellectuelle.

²¹³ Mc CARTHY Smári, «Copyright Combinatorics – Exercises in the banal mathematics of EU policy», 11 août 2011, www.smarimccarthy.com/2011/08/copyright-combinatorics/.

faisait 221 possibilités (soit 2 097 152), qu'il faut ensuite combiner avec les exceptions prévues pour le droit de distribution, pour aboutir au nombre de 10 460 353 203». ²¹⁴

Le risque d'atteinte à la liberté d'expression et de communication des internautes est donc parfaitement probable et préjudiciable.

§2. Le risque d'atteinte à la liberté d'expression et de la communication

Le risque d'atteinte à la liberté d'expression et de communication des internautes n'est pas à mésestimer. Il ne faudrait en outre pas imaginer que le préjudice résultant de l'impossibilité d'exercer une exception du droit d'auteur soit faible. D'abord certaines exceptions comme l'exception de parodie participent efficacement à la liberté d'expression dans une société démocratique. Ensuite, ces exceptions peuvent jouer un rôle économique crucial. A titre d'exemple, l'industrie américaine dégagait en 2010 environ 20 milliards de chiffre d'affaires grâce au *fair use*. ²¹⁵

L'intermédiaire technique qui bloque un contenu qu'il n'aurait pas dû créer nécessairement un préjudice à l'internaute relevant de l'atteinte à la liberté d'expression et de la communication. Le risque juridique pourrait être minimisé, en considérant qu'il s'agit là de simple utilisateurs, au pire de clients. Il ne faut toutefois pas perdre de vue qu'un internaute n'est pas nécessairement un particulier et qu'un professionnel, personne physique ou moral, peut subir un important préjudice. Les exemples de «faux positif» rattrapent l'imagination et l'on peut citer ce clip de campagne d'Obama, chantonnant une chanson du domaine public bloqué par YouTube ²¹⁶ ou l'interruption de la retransmission en direct d'une convention démocrate utilisant des oeuvres musicales. ²¹⁷

Ces exemples montrent donc la nécessité pour les intermédiaires techniques de concevoir la mise en place des dispositifs de filtrage-blocage en prenant en compte les intérêts des internautes.

B. La nécessité d'intégrer l'internaute dans la décision de blocage

La collaboration de l'intermédiaire technique devrait également se faire avec l'internaute à qui l'on reproche un acte de contrefaçon. L'idée n'est pas saugrenue dans la mesure où précisément celui-ci n'est pas forcément contrefacteur (§1). En outre, elle renforcerait la neutralité que doit jouer l'intermédiaire technique, en remettant face à face l'ayant droit et l'internaute (§2).

²¹⁴ MANARA Cédric, «Le droit du commerce électronique après l'arrêt *Scarlet*», *RLDI* 2012/78, n°2612.

²¹⁵ Economic Contribution of Industries Relying on Fair Use, Computer & Communications Industry Association, 2010, www.cciainet.org/CCIA/files/cclibraryFiles/Filename/000000000354/fair-use-study-final.pdf.

²¹⁶ YouTube restores Obama videos, refuses to explain takedown policies, *ARS TECHNICA*, 20 juillet 2012 <http://arstechnica.com/tech-policy/2012/07/youtube-restores-obama-videos-refuses-to-explain-takedown-policies/>.

²¹⁷ YouTube Flags Democrats' Convention Video on Copyright Grounds, *WIRED*, 9 mai 2012 <http://www.wired.com/threatlevel/2012/09/youtube-flags-democrats-convention-video-on-copyright-grounds/>.

§1. Un droit de réponse pour l'internaute

L'image négative véhiculée par les mesures de filtrage s'explique pour partie à cause de l'aspect arbitraire que celles-ci prennent. Y ajouter un droit de réponse à l'internaute qui prétend les subir apparaît être en mesure de redorer cette image ternie en permettant à celui-ci de faire valoir ses observations.

Les intermédiaires techniques pourraient s'inspirer de ce que propose déjà YouTube pour son système ContentID²¹⁸ qui intègre ce qu'il présente comme une sorte de droit d'appel.²¹⁹ L'intérêt vaut tant pour les intermédiaires techniques que les ayants droit, qui peuvent avec un système équilibré trouver un compromis financier et pouvant être à même de ne pas faire fuir les internautes vers des réseaux moins contrôlés.²²⁰

§2. Un renforcement du rôle neutre de l'intermédiaire technique

En prévoyant une concertation de l'ayant droit avec l'internaute présumé contrefacteur ou, à tout le moins, en permettant ce dernier de faire valoir ses observations au premier, l'intermédiaire technique verrait son rôle neutre renforcé. Ce dialogue inspire d'ailleurs certains auteurs outre-Atlantique à la recherche d'un système pour lutter contre les atteintes aux droits de la propriété intellectuelle autre que celui du filtrage et inspiré des procédures de résolution des litiges UDRP pour les noms de domaine.²²¹ Du côté de l'Europe, la Commission européenne a lancé le 4 juin 2012 une consultation publique sur les procédures de notification à l'encontre des contenus illicites.²²² Clôturé le 11 septembre 2012 et non encore publié, la consultation devrait donner des bases de réflexion sur la place de l'internaute présumé contrefacteur dans ces procédures de notification puisqu'elle posait expressément la question.²²³ Parmi les contributeurs, certains proposent que l'internaute présumé contrefacteur soit averti, afin notamment de prévenir toute désactivation ou retrait d'un contenu légal.²²⁴ Ils ajoutent que pourrait être imaginé une procédure rapide par laquelle le

²¹⁸ Appealing Rejected Content ID Disputes <https://support.google.com/youtube/answer/2770411?hl=fr&rd=1>.

²¹⁹ «Prior to today, if a content owner rejected that dispute, the user was left with no recourse for certain types of Content ID claims (e.g., monetize claims). Based upon feedback from our community, today we're introducing an appeals process that gives eligible users a new choice when dealing with a rejected dispute. When the user files an appeal, a content owner has two options: release the claim or file a formal DMCA notification», Improving Content ID, 3 octobre 2012 <http://youtubecreator.blogspot.fr/2012/10/improving-content-id.html>.

²²⁰ CHEMLA Laurent, [BBS] L'Internet caché du monde de l'ombre, 15 mai 2013, <http://www.ecrans.fr/BBS-L-Internet-cache-du-monde-de-l-1,16367.html>.

²²¹ LEMLEY Marc & REESE Anthony, A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes, *Cardozo Arts & Entertainment Law Journal*, 2005, Vol. 23, n° 1, p 1-20. http://www.law.uci.edu/pdf/treese/reese_copyrightdisputes.pdf.

²²² A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm.

²²³ «Question 16 Should hosting service providers consult the providers of alleged illegal content ?», *ibid*.

²²⁴ « Upon reception of a notice, and before any action on the alleged illegal content is taken. That will prevent the disabling of legal content or its removal.», RESPONSE PRESENTED BY TRANS EUROPE EXPERTS TO THE CONSULTATION "A CLEAN AND OPEN INTERNET" ON PROCEDURES NOTIFYING AND ACTING ON ILLEGAL CONTENT HOSTED BY ONLINE INTERMEDIARIES, BÉNABOU Valérie-Laure, CASTETS-RENARD Céline, HARDOUIN Ronan, MANARA Cédric, VOSS Grégory, ZOLYNSKY Célia, <http://www.transeuropexperts.eu/documents/TEE%20-%20A%20CLEAN%20AND%20OPEN%20INTERNET.pdf?PHPSESSID=b8ccaeeb109b02b448af5c5c622a2bcd>.

fournisseur du contenu aurait seulement quelques jours (par exemple 2) pour exercer son droit de réponse et qu'en cas de non-réponse, l'hébergeur pourrait alors retirer le contenu dénoncé.²²⁵

CONCLUSION DU TITRE II

La mise en place d'une mesure de filtrage pose de multiples interrogations non résolues quant à la responsabilité de l'intermédiaire technique. La directive Commerce électronique ne traite que trop vaguement de la possibilité de recourir à ces mécanismes et met dans l'incertitude les intermédiaires techniques sur le sort qui leur est réservé. Face à ces incertitudes juridiques, les institutions européennes incitent à la conclusion de charte scellant la collaboration des intermédiaires techniques et des ayants droit. Gageons que cette réponse imparfaite précède une révision des directives permettant d'assurer une sécurité juridique pour les intermédiaires techniques.

²²⁵ «Nevertheless, we can imagine a short procedure in which the content provider should have just some days (2 for example) to exercise his adversarial right. If it didn't, the hosting provider will be able to remove the content denounced.», *ibid.*

CONCLUSION GÉNÉRALE

Notifier et devoir sans cesse recommencer à notifier, «*Ce serait l'histoire de l'hydre de Lerne*» comme l'écrivait Charles de Bernard que nous reprenions en épitaphe. Les mesures de filtrage imposées aux intermédiaires techniques peuvent s'avérer être des dispositifs efficaces pour prévenir et faire cesser les atteintes à la propriété intellectuelle sur Internet. Mais les textes qui permettent aux ayants droit de les solliciter restent trop abstraits face à l'interdiction de faire peser sur les intermédiaires une obligation générale de surveillance. Par ailleurs, la recherche d'un juste équilibre entre la protection de la propriété intellectuelle et les libertés fondamentales pouvant être affectées par la mise en place de ces dispositifs est complexe à évaluer. Si les juges dégagent des critères généraux permettant cette conciliation, reste que les ayants droit sollicitant ces injonctions de filtrage se retrouvent dans une insécurité juridique quant à savoir si l'équilibre sera respecté et la mesure avalisée par le juge.

S'agissant des intermédiaires techniques, les incertitudes quant au sort de leur responsabilité suite à la mise en place d'une mesure de filtrage ne permettent pas à ces acteurs de l'internet de les envisager sereinement. Parallèlement, la jurisprudence a aujourd'hui dégagé de manière claire, conformément aux textes, les régimes de responsabilité de ces intermédiaires. S'agissant des hébergeurs, on sait qu'ils :

- ne sont pas tenus à une obligation générale de surveillance,
- ne sont pas responsables des contenus qu'ils hébergent,
- ne peuvent être reconnus responsables que s'ils ont eu connaissance d'un contenu manifestement illicite et qu'ils n'ont alors rien fait pour le retirer.

La crainte de perdre le bénéfice de ce régime de responsabilité favorable qui leur est accordé ou la possibilité de les poursuivre en cas de défaillance de la mesure technique de surveillance font peser chez les intermédiaires techniques des risques latents.

Comme nous l'avons vu, la mise en place d'une obligation particulière de surveillance pour prévenir et faire cesser des atteintes aux droits de propriété intellectuelle suppose qu'elle soit :

- ordonnée par une autorité judiciaire,
- ciblée et temporaire,
- proportionnée au but poursuivi.

La jurisprudence communautaire s'avère être sur ce dernier point une indispensable grille d'analyse de l'équilibre nécessaire entre la protection de la propriété intellectuelle (le but poursuivi) et les autres libertés fondamentales.

La contribution des intermédiaires techniques à la lutte contre les atteintes à la propriété intellectuelle, couplée à la nécessité de ne pas porter atteintes aux libertés fondamentales des internautes les mettent donc dans le rôle d'un équilibriste qui nécessiterait plus de considérations au regard du rôle central de ces acteurs dans le fonctionnement de l'Internet. L'impossibilité de mettre en place un dispositif de filtrage parfait et le risque de porter atteinte à la liberté d'expression et de communication des internautes appellent à une révision des textes relatifs à la responsabilité des intermédiaires techniques.

Continuons à citer l'auteur de *La Chasse aux amants* : «*Croyez-moi, les expédients pacifiques sont les meilleurs ; mettez de côté toute humeur sanguinaire, et laissez-moi continuer mon rôle de gardien officieux*». Voilà ce qui pourrait bien être un cri du coeur des intermédiaires techniques. Des solutions nouvelles pour lutter contre les atteintes à la propriété intellectuelle appellent à être trouvées afin de parvenir à l'équilibre des intérêts de tous les protagonistes.

BIBLIOGRAPHIE

I. Sources doctrinales

• Ouvrages

- CARBONNIER Jean, *Droit civil*, vol. 1, PUF, 2004, n°154
- MARINO Laure, *Droit de la Propriété Intellectuelle*, PUF, Thémis Droit, 2013
- LUCAS A. et H.-J., *Traité de la propriété littéraire et artistique*, LITEC, 3e éd. 2006
- ZOLYNSKY Célia, Méthode de transposition des directives communautaires. Etude à partir de l'exemple du droit d'auteur et des droits voisins, *Dalloz Nouvelle Bibliothèque de Thèses*, 2007.

• Commentaires, études et chroniques

- BENABOU Valérie-Laure, «L'oeuvre poulpe», *RDTI*, 2009, n° spécial 32
- BENABOU Valérie-Laure, «Chroniques», *Propriétés Intellectuelles*, Janvier 2012, n°42, p. 47.
- BENSAMOUN Alexandra & ZOLYNSKI Célia, Lutte contre la contrefaçon sur internet : les sources de l'implication des prestataires techniques », *RLDI* 2011/75, n°2494, pp. 59-65
- BERBETT Katharina & PRUD'HOMME Mathieu, «Contenus illicites : l'obligation de suppression pesant sur l'hébergeur», *Gaz. Pal.* 15 octobre 2011, n°288, p.15.
- BERGEL Jean-Louis, «La découverte du sens en droit par la finalité», in *La découverte du sens en droit, Association française de Philosophie du droit*, 1991, p. 67
- BERNAULT Carine, «Coup d'arrêt pour le filtrage préventif sur les réseaux numériques», *L'ESSENTIEL Droit de la propriété intellectuelle*, 15 janvier 2012, n°1, p. 1.
- BRUGUIERE Jean-Michel, «Liens hypertextes, notice and stay down», *Semaine Juridique Entreprise & Affaires*, n°42, 18 octobre 2012, 1627
- CALMES Dominique, «Difficile consensus autour de la responsabilité des hébergeurs», *Revue Lamy Droit Civil*, 2012/92, page 59.
- CARON Christophe, «Responsabilité des hébergeurs : requiem pour le «take down, stay down», *Communication Commerce Électronique*, n°9, Septembre 2012, comm. 91.
- CASANOVA Antoine, «La Cour de Cassation préfère le «notice and take down» au «notice and stay down», au risque de voir les ayants droit «knocked down»», *Lexbase*, Hebdo Edition Affaires n°307, 6 septembre 2012.
- CASTETS-RENARD Céline, «Protection du droit d'auteur confrontée aux droits fondamentaux : point trop n'en faut !», *RLDI* 2012/79, n°2622.
- CASTETS-RENARD Céline, «Un nouvel intermédiaire irresponsable : le distributeur de presse en ligne», *RLDI* 2012/81, n°2700.
- CASTETS-RENARD Céline, «Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet», *Recueil Dalloz* 2012, p. 827.
- CASTETS-RENARD Céline, «Hébergement et contrefaçon en ligne : clarification du droit de la responsabilité sur l'internet», *Recueil Dalloz* 2012 p. 2075.
- COSTES Lionel, «Affaire *Sabam* : l'analyse de la CJUE», *RLDI* 2011/77, n°2541.
- COSTES Lionel, «Absence d'obligation générale de surveillance pesant sur les prestataires d'hébergement pour la Cour de Cassation», *RLDI* 2012/85, n°2866.
- COSTES Lionel, «TF1 c/ Dailymotion : manquement à son obligation de prompt retrait», *RLDI* 2012/86, n°2895.

- DE BEER Jeremy & CLEMMER Christopher, Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?, *Jurimetrics*, Vol. 49, No. 4, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1529722
- DEBET Anne, «Responsabilité des sites de partage de vidéos : les représentants des ayants droit doivent coopérer», *Communication Commerce Électronique*, n°7, Juillet 2011, comm. 67.
- DEBET Anne, «Des limites strictes posées au filtrage des contenus sur Internet par la CJUE», *Communication Commerce Électronique*, n°6, Juin 2012, comm. 63.
- DEBET Anne, «Dailymotion condamné à payer 200 000€ de dommages et intérêts à TF1 pour manquement à son obligation de retirer promptement des contenus», *Communication Commerce Électronique*, n°11, novembre 2012, comm. 122.
- DERIEUX Emmanuel, «Neutralité : liberté ou surveillance Fondements et éléments du droit de l'internet», *RLDI* 2011/74, n° 2464.
- DERIEUX Emmanuel, «Filtrage par les FAI - Opposition aux obligations générales de filtrage imposées aux fournisseurs d'accès à internet», *RLDI* 2012/78, n°2611.
- DERIEUX Emmanuel, «Fournisseurs d'hébergement - Impossible obligation générale mais possibles obligations particulières de surveillance et de filtrage», *RLDI* 2012/81, N°2699.
- FRANCILLON Jacques, «Téléchargement illégal d'oeuvres protégées par un droit d'auteur. Appréciation de la validité au regard du droit européen des mesures générales de filtrage et de blocage par les fournisseurs d'accès à internet (non)», *Revue de science criminelle*, 2012 p. 163.
- GATEAU Christine & COSLIN Christelle, «La Cour de Cassation a tranché : les prestataires d'hébergement n'ont pas à rechercher d'éventuelles remises en ligne des contenus notifiés après les avoir retirés», *RLDI* 2012/86, n°2889.
- GAUTIER Pierre-Yves, D. 2011, *De l'éventuel « rôle actif » des opérateurs internet dans la réalisation du dommage (qualification de responsabilité civile)*, point de vue p. 2054, n° 3
- GASNIER Jean-Pierre et ROUX Olivier, «Libres propos autour des conclusions de l'Avocat général de la CJUE dans l'affaire eBay contre l'Oréal» : *RLDI* févr. 2011/68, n° 2220
- GUTHFREUND-ROLAND Florence & MARRACHE Élisabeth, «Arrêt *Sabam* : requiem pour "Hadopi 3" ?», *RLDI* 2012/78, n°2614.
- HARDOUIN Ronan, «Observations sur les nouvelles obligations prétorienne des hébergeurs», *Juriscom.net*, 8 novembre 2007, <http://www.juriscom.net/documents/resp20071108.pdf>
- HARDOUIN Ronan, «Du copulatif au passif ou comment la conjonction «et» ajoute une condition pour jouir du régime de l'hébergeur», *Juriscom.net*, <http://juriscom.net/wp-content/documents/resp20100408.pdf>
- HARDOUIN Ronan, «La connaissance de l'illicéité par les hébergeurs ou quand être notifié ne signifie pas nécessairement devoir retirer», *RDTI* N12/2, Juillet 2012.
- HARDOUIN Ronan, «Fascicule 464 : La responsabilité des intermédiaires techniques de l'internet», *Lamy droit des médias et de la communication* 2012
- LEMLEY Marc & REESE Anthony, A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes, *Cardozo Arts & Entertainment Law Journal*, 2005, Vol. 23, n° 1, p 1-20. http://www.law.uci.edu/pdf/treese/reese_copyrightdisputes.pdf
- MANARA Cédric, «Bloquer le filtrage ! Une approche critique des affaires *Sabam*», *RLDI* 2011/76, n°2533.
- MANARA Cédric, «Le droit du commerce électronique après l'arrêt *Scarlet*», *RLDI* 2012/78, n°2612
- MANARA Cédric, «La Cour de cassation fait obstruction au blocage de contenus par les hébergeurs», *Dalloz Actualité*, 18 juillet 2012
- MARINO Laure, «Le fabuleux destin de la responsabilité des hébergeurs, à propos des arrêts Dailymotion et autres», *Resp. civ. et assur.* n°6, Juin 2011, étude 8
- MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 16 février 2012, n°47, p. 14

- MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 2 août 2012, n°215, p. 11
- MARINO Laure, «Chronique de jurisprudence», *Gaz. Pal.* 18 octobre 2012, n°292, p. 12
- MONTERO Étienne «La responsabilité des prestataires intermédiaires sur les réseaux», *in* Le commerce électronique européen sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique, Bruxelles, Bruylant, 2001, p. 279
- MONTERO Étienne & VAN ENIS Quentin, «Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'internet : la quadrature du cercle ?», *RLDI* 2010/61, n°2028
- NERI Alexandra, «L'injonction de filtrage rendue à l'égard d'un intermédiaire : une mesure controversée aux conséquences redoutables», *Communication Commerce Électronique*, n°1; janvier 2012, étude 3.
- ROUX Olivier, «Être ou ne pas être hébergeur, une question toujours aussi difficile», *RLDI*, 2012/81, n°2701.
- PETIT Cécile, «Google, une obligation de surveillance proportionnée ?», *Recueil Dalloz*, 2012, p. 2071.
- POIDEVIN Blandine, «Responsabilité de l'hébergeur - Chronique d'une année mouvementée», *Expertises*, Octobre 2012.
- POLLAUD-DULIAN Frédéric, «TPI Bruxelles, 29 juin 2007, *Sabam c/ Scarlet*, RIPIA 2007/3, n°229, p. 46», *RTD. Com.* 2008, p. 306
- ROUHETTE Thomas et GATEAU Christine, «Le statut d'hébergeur en Europe, une insécurité juridique née de la difficile adaptation du droit à l'évolution technologique» : *RLDI* juin 2011/72, n° 2399.
- SAINT MARTIN (de) Axel, «Blocage de contenus illicites et fournisseurs d'accès - Précisions sur le principe de subsidiarité», *RLDI* 2012/82, n°2745.
- SIRINELLI Pierre, «Propriété littéraire et artistique - Chronique», *Recueil Dalloz* 2011 p.2164
- SIRINELLI Pierre, Chronique de jurisprudence, *RIDA*, oct. 2012, p. 465
- TABAKA Benoît, «Les hébergeurs protègent-ils encore la liberté d'expression sur internet ?», <http://tabaka.blogspot.fr/2011/07/les-hebergeurs-protigent-ils-encore-la.html>
- TABAKA Benoît, «L'hébergeur, gardien de la liberté d'expression. La preuve par l'exemple», <http://tabaka.blogspot.fr/2011/08/lhebergeur-gardien-de-la-liberte.html>
- TABAKA Benoît, «Vivastreet tenu à une obligation de filtrage a priori», 24 octobre 2007, <http://tabaka.blogspot.fr/2007/10/vivastreet-tenu-une-obligation-de.html>
- TERRÉ François, «Etre ou ne pas être... responsable : à propos des prestataires de services par internet», *JCP* 2011. I. 1175
- THOUMYRE Lionel, «Le mannequin et l'hébergeur», 25 février 1999 <http://lthoumyre.chez.com/pro/1/resp19990225.htm>
- THOUMYRE Lionel, "Comment les hébergeurs français sont devenus juges du manifestement illicite", *Juriscom*, 28 juillet 2004 <http://juriscom.net/2004/07/comment-les-hebergeurs-francais-sont-devenus-juges-du-manifestement-illicite/>
- TREFIGNY Pascale, «Droit du numérique : août 2011 - août 2012», *Recueil Dalloz*, 2012 p. 2343.
- TROIANIELLO Antonino, «La CJUE s'oppose au filtrage généralisé de l'internet», *RLDI* 2012/78, n°2613.
- VALETTE MATHIEU, «Détection et interprétation automatique de contenus illicites et préjudiciables sur Internet» : http://faculty.arts.ubc.ca/winder/me/linguistique_du_corpus/Valette_PRINCIP.html
- WU Tim, «Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863#%23

II. Textes

• Directives et autres textes communautaires

- Directive 98/48/CE du Parlement européen et du Conseil du 20 juillet 1998 portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques - Journal officiel n° L 217 du 05/08/1998 p. 0018 - 0026 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0048:FR:HTML>
- 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 (JO L 178, p. 1) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML>
- 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 (JO L 167, p. 10)
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:FR:NOT>
- Directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle (JO L 157, p. 45, et rectificatif JO L 195, p. 16)
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:01:FR:HTML>
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, p. 31) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>
- Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JO L 201, p. 37) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML>
- Premier rapport sur l'application de la 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 »), 21 nov. 2003
- Rapport sur l'application de la directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, COM(2010) 779 final, 22 décembre 2010
- Communication de la commission 2011-942 «Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne»
- Communication de la commission, « Renforcer l'application des droits de propriété intellectuelle sur le marché intérieur » (COM(2009) 467 final), 11 septembre 2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0467:FIN:FR:PDF>
- Communication de la Commission, Doper la créativité et l'innovation pour permettre à l'Europe de créer de la croissance économique, des emplois de qualité et des produits et services de premier choix, COM(2011) 287 final, 24 mai 2011, pages 22 et 23 http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_fr.pdf
- COMMISSION STAFF WORKING DOCUMENT «Online services, including e-commerce, in the Single Market», SEC(2011) 1641 final, http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf
- A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services», 11 janvier 2012, SEC(2011) 1641 final, http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf
- Charte des droits fondamentaux de l'Union européenne (2000/C 364/01) www.europarl.europa.eu/charter/pdf/text_fr.pdf
- Memorandum of Understanding, 4 mai 2011 http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf

- A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, 4 juin 2012, http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm

• **Lois, décrets et autres textes parlementaires**

- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

- Rapport d'information n°627 du 23 janvier 2008 sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

- Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

- Projet de loi pour la confiance dans l'économie numérique, rapport n° 232 (2003-2004) de MM. Pierre Hérisson et Bruno Sido, fait au nom de la commission des affaires économiques, déposé au Sénat le 3 mars 2004, http://www.senat.fr/rap/l03-232/l03-232_mono.html

- Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée

- Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne`

• **Lois étrangères**

- Digital Millenium Copyright Act (DMCA), 28 octobre 1998, consultable en ligne <http://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf>

III. Jurisprudence

• Cour de Justice de l'Union européenne

- CJCE 2 septembre 2006, C-479/04, «Laserdisken»
- CJCE, 29 janv. 2008, aff. C-275/06 «Promusicae»
- CJUE 23 mars 2010, aff. C-236/08 à C-238/08, «Vuitton c/ Google AdWords»
- CJUE, 21 octobre 2010, aff. C-467/08, «Padawan»
- CJUE 12 juillet 2011, aff. C-324/0 «L'Oréal c/ Ebay»
- Conclusions de l'Avocat général M. Niilo Jääskinen dans l'affaire C-324/0 présentées le 9 décembre 2010
- CJUE 24 novembre 2011, affaire C-70/10 «SABAM / Scarlet»
- Conclusions de l'Avocat Général M. Pedro Cruz Villalón dans l'affaire C-70/10 présentées le 14 avril 2011
- CJUE 16 février 2012, affaire C-360/10 «SABAM / Netlog»

• Conseil constitutionnel

- Conseil constitutionnel, décision n°2004-496 DC du 10 juin 2004

• Cour de Cassation

- Cass. Crim. 13 janvier 2009 «*Sacem et autres / Cyrille S.*»
- Cass. com., 23 janv. 2007, n° 05-13.189, Bull. IV, n° 12
- Cass. 1ère Civ. 12 juillet 2012, n°11-15.165 et n°11.15.188
- Cass. 1ère Civ. 12 juillet 2012, n°11-13.666
- Cass. 1ère Civ. 12 juillet 2012, n°11-13.669

• Juridictions du fond

- CA Paris 10 février 1999 Estelle H. c/ Valentin L.
- CA Paris, 9 avr. 2010, Google c/ Flach Films et autres
- CA Paris, 3 déc. 2010, n°06/12315, Dailymotion c/ Zadig Production n°06/12315
- CA Paris, 14 janv. 2011, Google Inc. c/ Bac Films et autres 09/11 729
- CA Paris, 14 janv. 2011, Google Inc. c/ Bac Films et autres 09/11 779
- CA Paris, Pôle 5, chambre 2, 4 février 2011, Google Inc. et Aufeminin.com et autres c/ André Rau, H & K., n°09/21941 ;
- CA Paris Pôle 5, chambre 1, 9 mai 2012, n°10/12711.
- CA Paris, 21 juin 2013, SPPF c. Youtube
- TGI Paris, référé 20 novembre 2000
- TGI Paris, 3ème chambre, 2ème section, 19 octobre 2007, n°06/11874
- TGI Paris, 11 juin 2010, La Chauve-Souris et 120 Films c/ Dailymotion
- TGI Créteil, 14 déc. 2010, INA c/ YouTube.
- TGI Paris, 13 janv. 2011, Calt Production c/ Dailymotion
- TGI Paris, 3ème Chambre, 4ème section, 28 avril 2011, SPPF c/ Youtube

- **Jurisprudences étrangères**

- Royal Court of Justice, [2011] EWHC 1981 (Ch), 28 juillet 2011 *Twentieth Century Fox v British Telecom* http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/28_07_11_bt_newzbin_ruling.pdf
- Cour d'appel de Californie, *Lars Gentry c/eBay Inc.*, 26 juin 2002
- Bayerischer Verwaltungsgerichtshof, 7 mai 2007, 24 CS 07.1
- Rechtbank Zwolle-Lelystad, 3 mai 2006 N°AW6288, *Stokke c/ Maarkplats*.

- **Avis**

- Conseil National du Numérique, Avis «Net Neutralité», n°2013-1 du 1er mars 2013 <http://www.cnumerique.fr/wp-content/uploads/2013/03/130311-avis-net-neutralite-VFINALE.pdf>
- Groupe «G29», avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel, consultable en ligne
- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf

IV. Rapports

- CSPLA, Commission spécialisée sur les prestataires de l'Internet, rapport du 4 juillet 2008
- Le rôle économique et social des intermédiaires techniques, OCDE, 30 juin 2010 <http://www.oecd.org/fr/internet/ieconomie/45847774.pdf>
- "Site Blocking" to reduce online copyright infringement», OFCOM, 27 May 2010 <http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf>
- CALLANAN C., GERCKE M., DE MARCO E., DRIES-ZIEKENHEINER H., «*Rapport Filtrage d'Internet : Equilibrer les réponses à la cybercriminalité dans une société démocratique*», Octobre 2009, <http://www.juriscom.net/documents/lib20100520.pdf>
- RESPONSE PRESENTED BY TRANS EUROPE EXPERTS TO THE CONSULTATION "A CLEAN AND OPEN INTERNET" ON PROCEDURES NOTIFYING AND ACTING ON ILLEGAL CONTENT HOSTED BY ONLINE INTERMEDIARIES, BÉNABOU Valérie-Laure, CASTETS-RENARD Céline, HARDOUIN Ronan, MANARA Cédric, VOSS Grégory, ZOLYNSKY Célia, <http://www.transeuropexperts.eu/documents/TEE%20-%20A%20CLEAN%20AND%20OPEN%20INTERNET.pdf?PHPSESSID=b8ccaeeb109b02b448af5c5c622a2bcd>
- Economic Contribution of Industries Relying on Fair Use, Computer & Communications Industry Association, 2010, <http://www.cciainet.org/CCIA/files/ccLibraryFiles/Filename/000000000354/fair-use-study-final.pdf>