Etude relative à la lutte contre les atteintes au droit d'auteur sur internet: rapport pour le SPF économie, P.M.E., classes moyennes et énergie : rapport final

Sandrine Hallemans, Caroline Colin

Etude relative à la lutte contre les atteintes au droit d'auteur sur internet

economie
SPF Economie, P.M.E., Classes moyennes et Energie

crids

.be

ETUDE RELATIVE A LA LUTTE CONTRE LES ATTEINTES AU DROIT D'AUTEUR SUR INTERNET

RAPPORT POUR LE SPF ECONOMIE, P.M.E., CLASSES MOYENNES ET ENERGIE

RAPPORT FINAL

24 septembre 2012

Sandrine HALLEMANS

(sous la supervision et avec la participation de Séverine DUSOLLIER et Caroline COLIN)

Centre de Recherche Information, Droit et Société (CRIDS)

Facultés Universitaires Notre-Dame de la Paix – Namur

economie
SPF Economie, P.M.E., Classes moyennes et Energie

crids

Le contenu de cette publication relève entièrement de la responsabilité du *Centre de Recherche Information, Droit et Société*

Service public fédéral Economie, P.M.E., Classes moyennes et Energie
Rue du Progrès 50
1210 BRUXELLES
N° d'entreprise : 0314.595.348
http://economie.fgov.be

tél. 02 277 51 11

Pour les appels en provenance de l'étranger :
tél. + 32 2 277 51 11

Editeur responsable : Jean-Marc Delporte
Président du Comité de direction
Rue du Progrès 50
1210 BRUXELLES

Version internet

S4-09-0000/0000

Table des matières

INTRODUCTION 9

CHAPITRE 1 – LE PHENOMENE DES ATTEINTES AU DROIT D'AUTEUR SUR INTERNET 12

Section 1. Panorama des moyens de téléchargement ou de partage sur internet d'œuvres protégées par le droit d'auteur 12

§1. Le peer-to-peer 12
- **I. Le peer-to-peer centralisé** 13
- **II. La décentralisation du *peer-to-peer*** 14
  - A. Le *peer-to-peer* décentralisé 14
  - B. Le *peer-to-peer* semi-décentralisé 14
- **III. Les torrents** 15

§2. Le téléchargement direct 16

§3. Le streaming 16
- **I. Les sites de streaming manifestement illicites** 17
- **II. Les sites de streaming manifestement licites** 18

§4. Les listes d'hyperliens et les moteurs de recherche traditionnels ou spécialisés 18

§5. Les réseaux sociaux ou réseaux privés d'échanges 19

§6. Cloud computing 19

Section 2. Solutions existantes ou en cours d'implémentation dans différents pays 20

§1. Les systèmes légaux de cessation des atteintes au droit d'auteur 21
- **I. Les mécanismes de réponse graduée** 21
  - A. Les pays dans lesquels le système est mis en œuvre 21
    1. La France - HADOPI 21
    2. Le Royaume-Uni 23
       a. Fonctionnement du système élaboré par le *Digital Economy Act* 24
       b. Obligations de l'OFCOM 25
    3. La Corée du Sud 26
    4. La Nouvelle-Zélande 28
    5. Les Etats-Unis 29
  - B. Les pays dans lesquels le mécanisme est en projet 29
    1. La Belgique 29
    2. L'Allemagne 30
- **II. Les systèmes d'avertissement** 30
  - A. La Norvège 31
  - B. La Finlande 32
  - C. Le Danemark 33
  - D. La Suède 33
- **III. Le blocage de sites internet** 34
  - A. Les pays dans lesquels le mécanisme est implémenté 34

1. L'Espagne – la Ley Sinde 34
2. Le blocage prévu dans de nombreux pays via l'action en cessation 36
B. Les pays dans lesquels le mécanisme est en projet 37
1. Les Etats-Unis 37
a. Le projet de loi SOPA 37
b. Le projet de loi PIPA 38
c. Qu'en est-il actuellement ? 39
2. L'Irlande 40
3. L'Italie 40
4. La Norvège 41
C. Le blocage de sites par la voie judiciaire 42
1. Belgique – L'article 87, §1er de la Loi sur le droit d'auteur 42
2. France – L'article L336-2 du Code de propriété intellectuelle 43
3. Autres cas de blocage (du site The Pirate Bay) 43
4. La fermeture de Megaupload 45

§2. La mise en place d'accords contractuels 46
I. L'Irlande 46
II. L'Australie 48

§3. Les systèmes d'autorisation 50
I. La licence non volontaire 50
A. La Belgique 50
B. L'Allemagne 51
II. La gestion collective obligatoire 51
III. La licence collective étendue 53

§4. Décision d'inaction 55
I. Les Pays-Bas 55
II. La Suisse 56

CHAPITRE 2 – ETUDE DU CADRE LEGAL DE LA LUTTE CONTRE LES ATTEINTES AU DROIT D'AUTEUR SUR INTERNET 58

Section 1. Les questions de droit d'auteur 58

§1. Qualification des actes de mise à disposition ou d'accès aux œuvres 58
I. La mise à disposition d'œuvres (*upload*) 58
II. Le téléchargement d'œuvres (*download*) 59
III. L'accès aux œuvres en *streaming* 63

§2. Légitimité des régimes d'autorisation 64
I. Question préliminaire : qualification de la gestion collective obligatoire et de la licence collective étendue 65
II. La liste fermée d'exceptions de la directive 2001/29 68
III. Le test des trois étapes 68
A. L'exigence d'un cas spécial 69
B. L'exigence d'une absence d'atteinte à l'exploitation normale de l'œuvre 70
C. L'exigence d'une absence de préjudice injustifié aux intérêts légitimes de l'auteur 72
IV. L'interdiction de formalités 73
V. L'étendue du répertoire 74

VI. Le mécanisme étranger de la licence collective étendue 76

Section 2. Les questions relatives à l'intervention des intermédiaires techniques 77

§1. Le régime de responsabilité 78
I. Cadre général 78
A. Objectifs de la directive 2000/31 sur le commerce électronique 78
B. Evolution du contexte 79
C. Définition des notions clés 80
II. Règles pour les différentes fonctions (simple transport, hébergement, cache) 81
A. Les fournisseurs d'accès à Internet et simples transporteurs 81
B. Les hébergeurs 83
C. Le *caching* 84
D. Conclusion : une approche fonctionnelle 85
III. Interprétation par la Cour de justice de l'Union européenne 86
A. Notion d'intermédiaire 86
B. Le critère de passivité 87

§2. Une obligation d'instaurer une procédure de notification et de retrait des contenus illicites 88
I. Cadre général de la procédure de notification et de retrait 88
II. La connaissance effective 91
III. Obligation d'agir promptement 92
IV. Pratiques des intermédiaires techniques 93

§3. Obligations d'intervention 94
I. Obligations de collaboration 95
II. Obligation de surveillance temporaire 97

§4. Actions en cessation à l'encontre des intermédiaires 97
I. Principe 97
II. Champ d'application 100
A. A l'encontre de quels intermédiaires ? 100
1. Les intermédiaires au sens de la directive 2000/31 100
2. Les moteurs de recherche 100
3. DNS.be 101
4. Les prestataires de paiement 101
B. Etendue des mesures sollicitées 102
1. Types de mesures 102
a. Le filtrage 102
b. Le blocage de sites 105
c. Autres types de mesures possibles 107
2. Dans le temps 108
3. Dans l'espace 111
C. Obligation de tenir compte d'autres droits et libertés 113

§5. Le droit d'information de l'article 86*ter* de la LDA 113

§6. Autre rôle des fournisseurs d'accès à internet 116
I. Dans le cadre du mécanisme de réponse graduée 116

B. La légitimité d'une autorité administrative 182

§3. Système de réponse graduée 183

I. Modalités pratiques 183

II. Questions juridiques 183

A. Protection des données personnelles 183

B. Droit fondamental d'accès à internet 185

C. Droit de la défense et procès équitable 185

III. Autres questions 186

A. Opportunité et popularité des mécanismes de réponse graduée 186

B. Coût 187

C. Les conséquences techniques et sociales d'une obligation de sécurisation des connexions internet 187

§4. Mesures additionnelles : mesures éducatives et promotion des offres légales 187

CONCLUSION 189

Remerciements

L'auteure tient à remercier pour leurs commentaires constructifs et leurs conseils judicieux A. Cruquenaire, E. Montero, J.-P. Moiny, D. Mougenot, C. de Terwangne, J.-N. Colin, J.-M. Van Gyseghem, Q. Van Ennis, M. Piron, N. Blaise, J. Gérard, D. Lemaire.

Avertissement

Les opinions exprimées dans ce rapport relèvent de la seule responsabilité de leur auteure et ne représentent en aucune manière la position officielle du SPF Economie.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Introduction

Les atteintes aux droits d'auteur sur Internet peuvent prendre différentes formes, qu'il s'agisse des échanges illégaux d'œuvres sur les réseaux *peer-to-peer*, du streaming illégal, de la diffusion d'œuvres sur les réseaux sociaux ou tout autre site ou blog sans l'autorisation de leur auteur… Toutes ces pratiques sont très difficiles à enrayer et jusqu'alors, malgré les multiples pistes de réponse explorées par les titulaires de droits (poursuites des utilisateurs individuels à des fins dissuasives, interdiction judiciaire de sites d'échange ou de fourniture de logiciels le permettant, imposition de filtrage aux fournisseurs d'accès…), les utilisateurs continuent à accéder en masse à de la musique, des films ou d'autres contenus par des sites et logiciels d'échange non autorisés, mettant en péril la rémunération légitime des créateurs et producteurs, ainsi que le développement d'offres légales respectueuses des droits.

Etant donné l'ampleur du phénomène et les difficultés juridiques rencontrées, un consensus mondial existe sur la nécessité d'agir pour protéger les droits d'auteur malmenés sur internet. Plusieurs projets politiques, actuellement en cours de discussion en Belgique et ailleurs en Europe et dans le monde, se positionnent en tentant d'apporter des solutions juridiques aux téléchargements illégaux d'œuvres et contenus protégés. La problématique des atteintes aux droits d'auteur sur Internet est devenue prioritaire à l'échelon européen. Les défis immédiats pour les droits d'auteur et droits voisins, en particulier dans le contexte numérique, ont été identifiés par des documents clés de la Commission européenne : la communication de 2008 sur les contenus créatifs en ligne (COM(2007) 836), la communication sur une stratégie numérique pour l'Europe (COM(2010) 245 final/2) et le document de réflexion d'octobre 2009 de la DG Société de l'Information et la DG Marché Intérieur[1]. Tous soulignent la nécessité d'accroître la sécurité juridique et économique pour encourager le développement de contenus en ligne et une efficacité du marché numérique européen. Disponibilité des contenus créatifs, licences multi-territoriales, distribution en ligne d'œuvres audiovisuelles, développement de l'offre légale et respect des droits ont été identifiés comme des défis majeurs appelant des mesures législatives dont notamment la révision de certaines directives.

De plus, le rapport de la Commission européenne sur l'application de la directive de 2004 relative au respect des droits d'auteur (COM(2010) 779 final) montre que celle-ci a eu pour effet de créer de fortes normes juridiques européennes afin de faire respecter le droit d'auteur. Cependant, il insiste aussi sur l'augmentation du volume des infractions au droit d'auteur sur Internet, point qui n'a pas été abordé par la directive car le partage de fichiers en *peer-to-peer* était seulement en train d'émerger. La directive ne concerne que les violations des droits de propriété intellectuelle commises à des fins commerciales ou causant des dommages significatifs aux ayants droit, ce qui soulève certaines questions quant à son éventuelle application au partage de fichiers par les utilisateurs à des fins non commerciales. Le rapport conclut que certaines clarifications sont requises pour assurer une protection plus efficace des droits de propriété intellectuelle et un meilleur fonctionnement du marché intérieur, portant sur la prévention de l'offre à la vente et du partage des

[1] Creative Content in a European Digital Single Market, A Reflection Document of DG INFSO and DG MARKT, 22 octobre 2009.

fichiers en violation des droits d'auteur, la notion d'intermédiaires et l'applicabilité des injonctions, et le juste équilibre entre le droit d'information et la législation sur la protection de la vie privée. Le 11 janvier 2011, une consultation sur ce rapport a été organisée. La synthèse des réponses, publiée le 8 juillet 2011[2], met en relief deux tendances opposées : l'une qui prône une modification de la directive dans le sens de règles plus strictes en matière de violation des droits d'auteur et d'une implication accrue des fournisseurs d'accès à Internet à cette fin, l'autre qui y est farouchement opposée en raison notamment de la préservation de la liberté d'expression et du libre-échange de l'information.

C'est que le respect des droits de propriété intellectuelle soulève également de nombreuses questions hors du droit d'auteur, relatives notamment à la protection des données à caractère personnel et à l'implication des fournisseurs d'accès. En effet, la poursuite des utilisateurs se heurte à l'obstacle de l'identification des internautes se livrant à ces échanges, ce qui a réduit les poursuites dans de nombreux pays, notamment en Belgique. Le 29 janvier 2008, la Cour de justice européenne a estimé que « les directives 2000/31, 2001/29, 2004/48 et 2002/58 n'imposent pas aux États membres de prévoir (…) l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile »[3]. En revanche, si le législateur admet une dérogation à la protection des données personnelles pour faciliter la poursuite de violations de droit d'auteur par les ayants droit, la Cour exige de rechercher un juste équilibre entre les différents droits fondamentaux tant par les législateurs au moment de la transposition des directives que par les juges lors des litiges[4].

De plus, le rôle des fournisseurs d'accès à Internet dans le respect des droits de propriété intellectuelle, bien que figé dans une position d'exonération de responsabilité sous conditions posé par la directive « e-commerce », est fortement remis en question. Le plan d'action de la Commission en matière de droits de propriété intellectuelle[5] entend lutter contre les atteintes aux droits de propriété intellectuelle sur Internet en réprimant les infractions à leur source. A cet effet, il préconise d'« encourager la coopération avec les intermédiaires, notamment les prestataires de services internet »[6]. La Commission indique qu'il ne s'agit pas de « porter atteinte aux objectifs des politiques en matière de haut débit ni aux intérêts des consommateurs »[7]. Elle précise d'ailleurs que ces modifications devront respecter tous les droits consacrés par la Charte des droits fondamentaux de l'Union européenne, à savoir notamment le droit au respect de la vie privée, à la protection des données à caractère personnel, à la liberté d'expression et à l'information[8]. Le commissaire de la DG Marché Intérieur, Michel Barnier, a déclaré, lors de la présentation du plan d'action, que son

[2] La synthèse des réponses est disponible sur http://ec.europa.eu/internal_market/consultations/docs/2011/intellectual_property_rights/summary_report_replies_consultation_en.pdf

[3] CJCE 29 janv. 2008, *Promusicae c/ Telefonica de Espana*, aff. C-275/06; se reporter aux commentaires de Ch. CARON, *CCE* mars 2008, comm. n° 32 ; voir également les conclusions de l'avocat général prononcées le 14 avril 2011 dans l'affaire *scarlet Extended c. Sabam,* C-70/10.

[4] L'arrêt de la CJCE du 19 févr. 2009 (ord., *LSG-Gesellschaft zur Wahrrnehmung von Leistungsschutzrechten GmbH c/ Tele 2 Telecommunication GmbH,* aff. C.557-07,) s'inscrit dans la même tendance : voir L. COSTES, *CCE* avr. 2009, comm. 1567, p. 22.

[5] Cf. *supra*.

[6] *Ibid*.

[7] *Ibid*.

[8] *Ibid*.

intention, « s'agissant de l'éradication des sites de piratage, est d'agir plus directement à la source, c'est-à-dire vers et avec les fournisseurs d'accès à internet »[9]. Pour l'heure, cette coopération avec les fournisseurs d'accès n'a pas été définie. Mais force est de constater que l'Europe envisage désormais de se tourner vers ces intermédiaires pour lutter plus efficacement contre les comportements enfreignant le droit d'auteur.

Parallèlement à cette dynamique européenne, plusieurs projets politiques, actuellement en cours de discussion en Belgique et ailleurs en Europe, se positionnent en tentant d'apporter des solutions juridiques aux atteintes portées aux droits d'auteur sur Internet et notamment aux échanges illégaux d'œuvres sur les réseaux *peer-to-peer*. Certains pays de l'Union Européenne ont adopté une approche en trois étapes appelée « réponse graduée » (ex: France, Royaume-Uni...) pour dissuader les utilisateurs de partager la musique protégée et des films, solution également discutée lors des négociations de l'Accord commercial anti-contrefaçon (ACTA). En Belgique, une proposition de loi, rédigée par le groupe MR, d'abord par le sénateur Monfils le 21 avril 2010 puis par le sénateur Miller le 28 janvier 2011[10], s'inscrit dans cette tendance en instaurant, notamment, une réponse graduée s'inspirant de la solution dite HADOPI française. De leur côté, les groupes Ecolo et Groen ont élaboré une autre proposition de loi, déposée une première fois le 2 mars 2010 par les sénateurs Hellings et Piryns puis une seconde fois le 9 décembre 2010 par les sénateurs Morael et Piryns[11], destinée à régulariser ces échanges dans le cadre d'une licence dite globale. Deux principales tendances destinées à lutter contre les atteintes aux droits d'auteur sur Internet émergent: l'une répressive, l'autre davantage permissive mais dans un contexte de respect du droit d'auteur. Une dernière proposition de loi émanant des socialistes francophones insiste plutôt sur le rôle de certains intermédiaires et élargit la possibilité d'intenter une action en cessation contre les intermédiaires dont les services sont utilisés pour commettre des violations de droit d'auteur, aux intermédiaires proposant des services de paiement[12].

Cette effervescence législative démontre que la diversité des solutions offertes aux pouvoirs publics et aux ayants droit pour renforcer la lutte contre l'accès non autorisé aux œuvres sur les réseaux numériques. La présente étude a pour objectif de présenter l'état des lieux dans divers pays européens et non européens et d'analyser les enjeux et obstacles juridiques que les systèmes proposés comportent.

L'étude appréhendera, au sein d'un premier chapitre, les atteintes au droit d'auteur sur internet. Un descriptif de ces atteintes sera proposé ainsi que les systèmes mis en place ou en cours d'implémentation par différents pays afin de lutter contre ces atteintes au droit d'auteur sur internet. Un deuxième chapitre sera consacré à l'analyse du cadre légal de la lutte contre les atteintes au droit d'auteur sur internet et abordera tant les questions de droit d'auteur, que de

[9] S. ESTIENNE, « L'Europe relance le débat sur les droits d'auteur à l'heure d'internet », dépêche AFP, 24 mai 2011.
[10] Proposition de loi favorisant la protection de la création culturelle sur Internet, *Doc. Parl.*, Sénat, 2010-2011, n° 5-741/1.
[11] Proposition de loi visant à adapter la perception du droit d'auteur à l'évolution technologique tout en préservant le droit à la vie privée des usagers d'Internet, *Doc. Parl.*, Sénat, 2010-2011, n° 5-590/1.
[12] Proposition de loi modifiant l'article 87 de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins en ce qui concerne la responsabilité des intermédiaires lors d'atteintes au droit d'auteur et aux droits voisins, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1084.

responsabilité des intermédiaires, de données personnelles ou de droits fondamentaux. Enfin l'analyse des options envisageables pour lutter contre les atteintes au droit d'auteur sur internet, qu'il s'agisse des systèmes d'autorisation des échanges, des systèmes de réponse graduée ou des mesures de neutralisation des contenus illicites, fera l'objet du troisième chapitre.

Chapitre 1. Le phénomène des atteintes au droit d'auteur sur Internet

Ce chapitre de la présente étude a pour objectif de dresser une comparaison des approches nationales en matière de lutte contre le piratage en ligne (section 2), après avoir procédé à la description du phénomène des atteintes au droit d'auteur sur Internet (section 1).

Section 1. Panorama des moyens de téléchargement ou de partage sur internet d'œuvres protégées par le droit d'auteur

Le piratage en ligne est le fruit du perfectionnement des technologies permettant cet accès rapide, facile et gratuit à du contenu protégé par le droit d'auteur. En effet, les consommateurs ne doivent plus rien payer, ni le support physique, ni le contenu, tout étant disponible en ligne gratuitement[13]. Un rapport anglais de 2009 a trouvé 29 possibilités de télécharger et partager du contenu digital non-autorisé[14]. Nous analyserons ici les aspects techniques des méthodes les plus courantes, du *peer-to-peer* (§1.), au téléchargement direct (§2.), au streaming (§3.), aux moteurs de recherche et listes d'hyperliens menant à du contenu contrefait (§4.) et partage de fichiers protégés sur les réseaux sociaux (§5.), tous étant la cible des ayants droit, qui sont parvenus avec plus ou moins de réussite à en éradiquer certains. Nous ferons également un bref point sur l'utilisation du *cloud computing* pour stocker des fichiers acquis illégalement et les partager (§6.).

§1. Le peer-to-peer

La technologie du *peer-to-peer* – ou pair à pair – permet à plusieurs ordinateurs reliés entre eux de communiquer via un réseau commun et de partager des fichiers sur ce réseau. Il ne s'agit pas ici de téléchargement direct – c'est-à-dire le téléchargement via un serveur – mais plutôt d'échange entre utilisateurs, qui jouent alors chacun à la fois le rôle de client et de serveur. Les réseaux *peer-to-peer* fournissent une architecture stable, bon marché et de partage global de toutes sortes d'informations numérisées, que ce soit de la musique, des films, des logiciels, des *e-books*, *etc*[15]. Les caractéristiques principales de ce système sont donc la décentralisation et le fonctionnement sans l'intervention d'un

[13] *Media Consulting Group*, « Le 'forfait sur le contenu' : une solution au partage illégal de fichiers ? », Etude pour le Parlement européen, juillet 2011, pp. 45-46, disponible sur http://www.europarl.europa.eu/studies

[14] SABIP CIBER Report, « Copycats? Digital consumers in the online age », A CIBER report for the Strategy Advisory Board on Intellectual Property, mai 2009, Annexe 4, p. 85 (Rapport téléchargeable sur : http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCYQFjAA&url=http%3A%2F%2Fwww.kennisland.nl%2Fuploads%2Ffckconnector%2Fa8ea9001-9376-4478-9506-6bc889065215&ei=Tu1ETfoKIfv8QOikdXiBA&usg=AFQjCNEKz1JAmGLKjPZt-LOv0f02jC7pEw&sig2=_sjWXbqhOHypaIzLGYSNLg)

[15] A. PEUKERT, « A Bipolar Copyright System for the Digital Network Environnement », in *Peer-to-peer file-sharing and secondary liability in Copyright law,* Edward Elgar, Cheltenham, 2009, pp. 148-151.

serveur. Chaque logiciel installé sur des ordinateurs, et donc finalement les utilisateurs, peuvent être qualifiés de *nœud*, et c'est entre les nœuds que se passent les échanges. Le système fonctionnant sur un modèle communautaire, au plus le nombre de nœuds possédant un même fichier est important, au plus grande est la chance d'obtenir rapidement ce fichier. En effet, il est possible de télécharger le même fichier auprès de plusieurs sources à la fois, ce qui augmente considérablement la vitesse de téléchargement des fichiers les plus populaires.

Les échanges d'œuvres sur les réseaux *peer-to-peer* mettent en jeu une opération de *download,* ou téléchargement descendant et une opération d'*upload,* ou téléchargement ascendant. De manière générale, dès que l'on se connecte au réseau *peer-to-peer* pour télécharger un contenu, on devient automatiquement « fournisseur » de ce contenu, il y a un *upload* automatique.

Il existe plusieurs types de *peer-to-peer*. Tout d'abord le *peer-to-peer* centralisé (I), qui a pour caractéristique principale un système d'indexation centralisé, une sorte de serveur gérant les requêtes et les partages de fichiers, mais qui ne contient pas les fichiers eux-mêmes. Le passage par un tel serveur n'empêche dès lors pas la qualification d'un tel système de *peer-to-peer,* du fait qu'il revient aux utilisateurs, les pairs, de transférer les fichiers entre eux, sans passer par le serveur central. Vient ensuite le *peer-to-peer* totalement décentralisé (II.A.), sans intervention de serveur d'indexation centralisé. Pour pallier les difficultés émanant de ces deux mécanismes, un troisième modèle est apparu : le *peer-to-peer* semi-décentralisé (II.B.).

I. Le peer-to-peer centralisé

C'est en 1999 avec le lancement de Napster que le *peer-to-peer* centralisé a fait son apparition. Dans ce système, l'information permettant de localiser les fichiers à télécharger est listée sur des serveurs, sous forme de système d'indexation centralisé, généralement répartis sur des zones géographiques précises. Les utilisateurs souhaitant télécharger un fichier donné vont soumettre une requête au serveur pour ce fichier, ce dernier possédant la liste des adresses IP des utilisateurs ayant le fichier. Le serveur renvoie cette liste à l'utilisateur qui prend alors contact directement avec les personnes identifiées sur la liste et commence à télécharger le fichier désiré. Concernant l'*uploading*, il s'agit juste d'insérer dans la liste des serveurs le nom des fichiers que l'on souhaite partager, couplé aux utilisateurs possédant ce fichier – à ce moment, uniquement l'*uploadeur.*

Le point central de fonctionnement de ce système est un groupement de serveurs qui contient le listing de tous les utilisateurs connectés et les fichiers, et fait donc office d'index centralisé. Ce point central était également son point faible. En effet, il suffisait de s'attaquer aux serveurs pour détruire le système entier. C'est d'ailleurs cela qui a couté la perte de Napster, transformé depuis lors en service de musique légal.

Comme exemples de logiciels *peer-to-peer* centralisés nous pouvons retenir les plus connus, Napster et Morpheus.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

II. La décentralisation du *peer-to-peer*

Pour faire face aux attaques des autorités à l'encontre des serveurs centralisant toutes les informations, s'est mis en place un *peer-to-peer* plus décentralisé, travaillant de manière communautaire.

A. Le *peer-to-peer* décentralisé

Dans un système de *peer-to-peer* décentralisé, on se passe des serveurs centralisés, chaque utilisateur jouant alors ce rôle de serveur. Ici, les utilisateurs doivent explorer le réseau par eux-mêmes pour trouver le fichier qu'ils souhaitent télécharger.

Par ce système d'exploration, que l'on peut appeler *query floading*, l'utilisateur « inonde » littéralement le réseau de requêtes, multipliant ainsi les sources de téléchargement. Les pairs possédant le fichier recherché répondent à la requête, la réponse remontant alors jusqu'au demandeur initial. Ce dernier va ensuite choisir les fichiers à télécharger en envoyant directement une requête de téléchargement aux pairs identifiés comme disposant du fichier.

Le système a pour défaut de saturer le réseau, car il est très coûteux en bande passante, et les recherches sont beaucoup plus lentes que dans les systèmes centralisés. L'augmentation du nombre d'utilisateurs alourdit fortement le réseau et le sature également. De plus, la requête peut éventuellement ne pas atteindre une surface de réseau suffisante, en raison des nombreux sauts qu'elle doit effectuer. L'avantage d'un tel mécanisme où chaque utilisateur est serveur réside dans l'absence de point unique de défaillance – *single point of failure.*

Un exemple de ce système est le logiciel Kazaa.

B. Le *peer-to-peer* semi-décentralisé

Pour ne pas subir ces inconvénients d'inondation du réseau, des systèmes basés sur des interconnexions entre des « serveurs » stables ont été conçus. Les réseaux utilisent un processus décentralisé appelé *Fast Track*, qui assigne des fonctions d'indexation aux ordinateurs connectés au réseau, appelés « supers nœuds », quand cela est nécessaire – chaque ordinateur pouvant virtuellement être un super nœud[16]. Ici, chaque utilisateur explore une partie de son environnement rapproché, plusieurs utilisateurs étant connectés à un super nœud proche. Ce que l'utilisateur partage y est alors enregistré, contenu sous forme de *listings*, et lorsqu'il effectue une recherche, il interroge ce même serveur, qui se charge de lancer la recherche parmi les autres utilisateurs qui lui sont connectés. Personne n'a le fichier dans son entièreté, le fonctionnement s'opérant par téléchargement de petits morceaux du fichier (*chunks*), qui seront alors reconstitués après réception

[16] A. STROWEL, « Introduction: peer-to-peer file sharing and secondary liability in copyright law », in *Peer-to-peer file-sharing and secondary liability in Copyright law*, *op. cti.*, p. 2.

de tous les morceaux. Dans ce genre de système, au plus il y a de nœuds dans son environnement proche, au plus il y aura de chance d'avoir une requête aboutie.

Concernant l'*upload* de fichiers, il suffit de déposer le fichier que l'on veut partager dans un dossier particulier, avec un nom bien défini, et le logiciel, une fois lancé, considèrera que tout ce qui y est contenu peut être partagé.

L'avantage du *peer-to-peer* semi-décentralisé est que l'on assiste à une moins forte saturation du réseau. De plus, les recherches sont beaucoup plus rapides, on retrouve plus vite l'information demandée car elle se localise dans des listings situés sur des serveurs proches. L'augmentation du nombre de serveurs, par rapport à un système de *peer-to-peer* centralisé, a pour conséquence qu'il n'y a pas de point unique de défaillance. Deux logiciels bien connus de *peer-to-peer* semi-décentralisé sont Emule et Limewire. Tous deux n'appartiennent pas à une entreprise, ce qui les rend moins vulnérables juridiquement[17].

III. Les torrents

Le système des *torrents* fonctionne sur le même modèle que le *peer-to-peer* semi-décentralisé mais avec des caractéristiques bien particulières. Il s'agit d'un protocole d'échange qui utilise des *trackers* et des *metafiles* pour coordonner la distribution de fichiers.

On retrouve également ici une découpe en segments de l'information à partager, et ensuite une distribution des segments différents à des interlocuteurs différents afin qu'ils aient eux-mêmes quelque chose à échanger[18]. Ce qui varie par rapport à d'autres mécanisme de *peer-to-peer* c'est la méthode originale de mise en route d'un téléchargement : il faut aller chercher sur un site spécialisé la signature du fichier que l'on souhaite télécharger – service que propose le site bien connu *The Pirate Bay* – ces sites étant appelés des annuaires de liens. Une fois cette signature obtenue (tout petit fichier en .torrent), il suffit de l'ouvrir dans un logiciel de type BitTorrent et le téléchargement est lancé, qui fonctionne alors dans un modèle *peer-to-peer* semi-décentralisé. C'est la signature qui permet ici de retrouver le fichier souhaité sur le réseau.

Le moyen d'uploader un fichier est très simple : il suffit de créer une signature pour le fichier. Une fois la signature partagée sur un site, tout le monde peut télécharger ce fichier.

Juridiquement, BitTorrent n'est pas en soi illégal. Dès lors, plutôt que de s'attaquer à BitTorrent lui-même, les ayants droit visent les annuaires de liens ainsi que les utilisateurs, le fonctionnement du protocole rendant aisé la collecte des adresses IP ayant téléchargé des fichiers[19].

Des exemples de sites proposant de tels torrents sont : *IsoHunt*, *Torrentz, IP Torrents,* etc.

[17] « De Napster à Megaupload, le long affrontement entre la justice et les services de téléchargement », *Le Monde*, 25 janvier 2012, disponible sur http://www.lemonde.fr/technologies/article/2012/01/23/de-napster-a-megaupload-le-long-affrontement-entre-la-justice-et-les-services-de-telechargement_1633482_651865.html
[18] http://fr.wikipedia.org/wiki/BitTorrent_(protocole)
[19] « De Napster à Megaupload (…), *op. cit.*

§2. Le téléchargement direct

Dans ce cas de figure, le contact s'opère directement entre l'ordinateur client et le serveur via l'URL du fichier, l'ordinateur lui envoyant sa requête et le serveur répondant en lui transmettant le fichier. Les sites dédiés hébergent les fichiers sur leurs serveurs et les mettent à disposition sur leurs sites internet. Ce système a été popularisé par le développement du haut débit, sous l'égide de Rapidshare[20].

La plupart de ces sites retirent, sur demande des ayants droit, les fichiers contrefaits qui leur sont signalés. Mais on peut leur reprocher le fait qu'ils proposent des services d'abonnement payant et que certains récompensent les meilleurs *uploaders*, en sachant très bien que les fichiers qui « marchent » le mieux sont les fichiers illégaux… Ces abonnements payants – ou abonnements *premium* – permettent un plus grand débit et une augmentation de la rapidité de téléchargement, et peuvent insinuer un doute dans l'esprit des utilisateurs, ceux-ci pensant que parce qu'ils payent ce service, celui-ci en devient légal, alors qu'aucune contrepartie n'est en réalité reversée aux ayants droit.

Néanmoins, ces sites ne proposent pas que du contenu illégal, des particuliers ou des entreprises pouvant payer un service pour un stockage sur les serveurs mis à disposition. Mais cela n'a pas empêché les autorités, essentiellement américaines, dans le cadre de leur opération « In Our Sites »[21], de saisir les noms de domaines des sites proposant de tels services ainsi que la saisie et la fermeture de leurs serveurs – nous pensons bien évidemment directement à Megaupload.

L'*upload* dans ce système est très facile à réaliser : il suffit de mettre à disposition le fichier sur le serveur, qui va alors lui donner une URL qu'il suffira d'introduire sur le site pour retrouver le fichier et le télécharger à sa guise.

Nous pouvons relever que certains sites proposent un service de *multi-upload*, qui offre la possibilité d'*uploader* les fichiers sur tous les sites d'hébergement connus, ce qui permet de faire face à la fermeture éventuelle de l'un d'eux, afin que le fichier soit toujours disponible.

Des exemples de sites proposant des fichiers en téléchargement direct sont Megaupload et Rapidshare.

§3. Le streaming

Il s'agit ici d'une diffusion des fichiers en flux continu, sans téléchargement de ces fichiers. A l'instar du téléchargement direct, un contact est opéré directement entre l'ordinateur de l'utilisateur et le serveur possédant le fichier souhaité, par requête envoyée par l'utilisateur. Le fichier arrive alors dans le serveur de l'ordinateur client dans une séquence ordonnée permettant une lecture immédiate. Il ne faut pas attendre que le fichier soit téléchargé dans son intégralité pour pouvoir le consulter, ce qui en fait un des avantages majeurs de ce système, spécialement pour les fichiers qui ne nécessitent qu'un visionnage unique, sans nécessité de le revoir par la suite (par exemple les

[20] « De Napster à Megaupload (…) », *op. cit.*
[21] Voir supra.

séries télévisées, une des applications les plus courantes dans le téléchargement illégal d'œuvres protégées par le droit d'auteur).

Au sens strict du terme il y a bien téléchargement, car un échange de données s'opère entre un utilisateur et un serveur, mais avec un stockage provisoire dans la mémoire vive de l'ordinateur. Une fois le visionnage terminé, le fichier est retiré automatiquement du cache où il était stocké. Il est toujours possible d'intercepter cette copie cache via son flux, ce qui permet la conservation du fichier : la copie à durée déterminée devient indéterminée.

I. Les sites de streaming manifestement illicites

A partir de 2003 avec *Radio.blog.club*, apparaît une nouvelle manière d'écouter de la musique en ligne : la diffusion à la demande[22]. Les *radioblogs* sont des programmes permettant d'écouter de la musique gratuitement sur internet, et sont indexés sur le site de Radioblogclub.com. Il est possible avec ce site d'insérer un lecteur de musique sur une page personnelle ou un blog, ce qui en a été l'utilisation la plus importante. Les fichiers musicaux ne sont pas stockés par Radioblog mais sur les serveurs des membres, les fichiers étant ensuite lus en streaming. Il apparaît donc que ce n'est pas le site lui-même qui est responsable des infractions au droit d'auteur mais les utilisateurs du service. En mars 2011, la Sacem est malgré tout parvenue à faire condamner les créateurs du site pour « mise à disposition du public d'un logiciel conduisant à l'écoute et au partage non autorisé d'œuvres musicales protégées »[23].

Un autre type de site de diffusion à la demande manifestement illégal est Grooveshark, un service illimité et gratuit d'écoute de musique en ligne. Les utilisateurs ayant un compte sur ce site fournissent la musique, qui profite alors à tous. Il existe des comptes payants, et pour les autres, une publicité visuelle apparaît dans le lecteur d'écoute. Faute d'accords de diffusion, les ayants droit ont attaqué Grooveshark, dont les créateurs sont accusés d'avoir chargé, en connaissance de cause, des milliers de morceaux protégés par le droit d'auteur[24]. Fin janvier 2012, en Allemagne, le site a été fermé suite à de nombreuses plaintes de la GEMA. En février 2012, c'est au Danemark que le site a été rendu inaccessible[25].

Spotify et Deezer sont des services similaires à Grooveshark mais ceux-ci ne proposent que des fichiers musicaux pour lesquels ils ont obtenus des accords de la part des ayants droit, qui sont rémunérés par le biais des recettes publicitaires ou par les abonnements.

Le secteur de l'audiovisuel n'est pas non plus épargné par le streaming. Les films et les séries télévisées sont téléchargés en masse sur des sites de mise à disposition en ligne de type Megavideo, Mixture Vidéo, *etc.*

[22] « De Napster à Megaupload (…) », *op. cit.*
[23] Paris (12e ch.), 22 mars 2011, *Sppf, Scpp / Mubility et autres.*
[24] « De Napster à Megaupload (…) », *op. cit.*
[25] O. ROBILLART, « Une coalition d'ayants droit obtient le blocage de Grooveshark au Danemark », *Clubic*, 21 février 2012, disponible sur http://pro.clubic.com/legislation-loi-internet/telechargement-illegal/actualite-477164-ayants-droit-blocage-grooveshark-danemark.html

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

II. Les sites de streaming manifestement licites

Il existe des sites de visualisation et de partage de vidéos en streaming qui ne sont pas destinés à être illégaux mais qui peuvent être détournés dans ce but. Youtube et Dailymotion, deux sites du genre, s'attèlent à supprimer les contenus contrefaisant lorsqu'ils leurs sont signalés, mais en tant qu'intermédiaires techniques, ils n'ont aucune obligation de surveillance généralisée sur leur plateforme[26]. La part de contenus postés sur ces sites sans autorisation est assez importante, ce qui permet de les ranger dans la présente étude.

§4. Les listes d'hyperliens et les moteurs de recherche traditionnels ou spécialisés

Il existe un grand nombre de moteurs de recherche spécialisés, de plateformes de recherche ou encore de sites regroupant des listes d'hyperliens menant vers des contenus illégaux – l'un des plus connu étant le site *The Pirate Bay*, le plus gros site référenceur de fichiers BitTorrent du monde. D'autres exemples de tels sites sont Torrents.to, www.filesdrop.com, dpstream.net, *etc.* Ces sites de référencement sont la cible des ayants droit, la tendance actuelle étant d'intenter des actions en justice pour faire fermer ces sites, plutôt que d'attaquer les contrevenants individuellement.

Les moteurs de recherche traditionnels, comme Google, permettent également de trouver des liens menant vers des contenus piratés. Google est à l'origine d'une grande part de téléchargements illégaux, le simple fait de taper dans la barre de recherche le nom d'un film renvoie fréquemment à un lien de téléchargement, souvent en BitTorrent. Mais il est difficile de rendre cet intermédiaire responsable, car il n'héberge aucun contenu. Les ayants droit font depuis longtemps pression sur Google pour que celui-ci déréférence certains mots menant à du contenu piraté, tels que *The Pirate Bay*, Torrent, Rapidshare, *etc.*[27] Dernièrement, l'IFPI a fait savoir qu'elle souhaite que Google filtre les liens menant vers des contenus piratés « en amont », dans le but de faire remonter les liens légaux[28]. La fédération de l'industrie du disque a la volonté de déposer une plainte contre Google pour abus de position dominante dans la recherche en ligne, car selon elle, la position dominante de Google dans ce secteur lui confère des responsabilités supplémentaires[29]. Ce filtrage en amont est irréalisable selon Google, celui-ci estimant ne pouvoir répondre qu'à des demandes précises[30]. L'IFPI a demandé à Google de retirer pas moins de 460 000 liens sur la période des six derniers mois de

[26] T.G.I. Paris (3e ch.), 15 avril 2008, *Omar et Fred et autres c. Dailymotion.*
[27] Julien L., « Google Instant filtre BitTorrent, RapidShare et Megaupload », *Numerama*, 27 janvier 2011, disponible sur : http://www.numerama.com/magazine/17902-google-instant-filtre-bittorrent-rapidshare-et-megaupload.html ; Julien L., « Google filtre The Pirate Bay, IsoHunt, BT Junkie et 4Shared », *Numerama*, 24 novembre 2011, disponible sur : http://www.numerama.com/magazine/20692-google-filtre-the-pirate-bay-isohunt-btjunkie-et-4 shared.html
[28] Julien L., « L'IFPI veut que Google filtre le piratage 'en amont' », *Numerama*, 16 février 2012, disponible sur : http://www.numerama.com/magazine/21686-l-ifpi-veut-que-google-filtre-le-piratage-en-amont.html
[29] « L'IFPI envisage de déposer plainte contre Google », *L'Express*, 15 février 2012, disponible sur : http://lexpansion.lexpress.fr/high-tech/l-ifpi-envisage-de-deposer-plainte-contre-google_283037.html
[30] Julien L., « L'IFPI veut que Google filtre le piratage 'en amont' », *op. cit.*

l'année 2011, le moteur de recherche affirmant en avoir supprimé cinq millions sur toute l'année 2011, sur requête des ayants droit[31].

§5. Les réseaux sociaux ou réseaux privés d'échanges

Le réseau social peut être défini comme étant un site internet dont le principal objet est d'agir comme un connecteur entre les utilisateurs, et via lequel ils échangent entre eux tous types d'information, à partir de profils individualisés – l'information et son échange étant donc la base du réseau social[32].

Il est très fréquent que l'on publie sur sa page Facebook, ou tout autre réseau social, des images protégées par le droit d'auteur, le clip de la chanson que l'on aime, *etc.* Or, pour héberger une œuvre sur sa page Facebook, il faut obtenir le droit de reproduction du titulaire du droit, ce qui est rarement le cas. Mais comment lutter contre cette pratique qui est entrée dans les mœurs…?

Les conditions d'utilisation de réseaux sociaux tels Facebook[33], Twitter, Instagram, *etc.* comprennent une clause par laquelle ils insistent sur le respect des droits de propriété intellectuelle et se réservent le droit de retirer tout contenu violant ces droits.

§6. Cloud computing

Le *cloud computing* consiste dans le stockage de contenus divers sur des serveurs distants, dont l'utilisateur ne connait pas l'emplacement exact, au lieu d'un stockage sur des serveurs locaux. Les contenus se situant dans ce *cloud* sont accessibles à distance par l'utilisateur, de n'importe quelle machine. L'utilisation de son *cloud* est *a priori* personnelle, ce qui pourrait faire pencher en faveur de la légalité des contenus qui y stockés sur base de l'exception de copie privée, mais il est évidemment très facile de rendre son utilisation publique, moyennant le partage du mot de passe qui permet d'y accéder, et d'en faire par là un outil de partage illégal de fichiers protégés par le droit d'auteur.

Une autre application du *cloud computing* pouvant conduire à des échanges d'oeuvres est l'application iTunes Match d'Apple. L'iCloud d'Apple permet de stocker la musique que l'on a achetée via iTunes, et de la partager sur tous ses supports Apple. Cela concerne donc uniquement les contenus téléchargés légalement sur la plateforme iTunes. Pour les fichiers musicaux éventuellement acquis illégalement par les utilisateurs, Apple a développé iTunes Match, un service payant qui permet de mettre dans le nuage d'Apple l'ensemble de notre collection, ce qui inclut donc les éventuels fichiers téléchargés illégalement, et qui offre même d'améliorer la qualité initiale des fichiers originaux…[34] On pourrait presque parler de « blanchiment » de contenus piratés.

---

[31] « L'IFPI envisage de déposer plainte contre Google », *op. cit.*
[32] J.-P. MOINY, « Contracter dans les réseaux sociaux : un geste inadéquat pour contracter sa vie privée – Quelques réflexions en droit américain », *Revue de la Faculté de droit de l'Université de Liège 2010/2*, p. 135.
[33] https://www.facebook.com/legal/terms
[34] http://www.apple.com/fr/icloud/features/

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Section 2. Solutions existantes ou en cours d'implémentation dans différents pays

De nombreuses solutions différentes sont adoptées ou sont en cours de mise en œuvre dans un certain nombre de pays pour faire face au partage et au téléchargement illégaux d'œuvres protégées sur internet. Nous pouvons diviser les solutions en différentes catégories : les systèmes de cessation des atteintes au droit d'auteur (§1), les mécanismes basés sur la mise en place d'accords contractuels (§2), les systèmes d'autorisation ou de légitimation des échanges (§3) et enfin l'autorégulation développée par le marché lui-même (§4). Nous aurons l'occasion de remarquer, et nous pouvons déjà le soulever à ce stade, que c'est la difficulté à identifier les individus qui téléchargent et partagent illégalement les contenus protégés qui constitue l'obstacle principal dans la lutte contre le piratage sur internet.

Quoi qu'il en soit, toutes ces lois et projets de lois s'inscrivent dans un mouvement plus large soutenu et poussé par certains titulaires de droits qui souhaitent une condamnation sévère des téléchargements illégaux d'œuvres. Le traité ACTA (*Anti-Counterfeiting Trade Agreement*), négocié par une dizaine de pays[35], demandait un renforcement des moyens de lutte contre des violations de droit d'auteur sur internet dans une Section 5 dédiée à l'*Enforcement of Intellectual Property Rights in the Digital Environment*, ce qui aurait pu encourager les Etats à instaurer des dispositifs de réponse graduée. Le 4 juillet 2012, le Parlement européen a rejeté le traité en séance plénière par 478 voix contre, 39 pour et 165 abstentions. Mais le Traité a été ratifié par la plupart des autres pays l'ayant négocié.

Par ailleurs, à l'échelon européen, le Parlement a adopté, le 22 septembre 2010, le rapport de l'eurodéputée PPE/UMP (France) Marielle Gallo[36] sur le renforcement de l'application des droits de propriété intellectuelle sur le marché intérieur. Le rapport met l'accent sur la nécessité de sensibiliser le grand public, la promotion de l'offre légale et la lutte contre les échanges non autorisés d'œuvres sur internet en trouvant des solutions appropriées et urgentes en fonction du secteur concerné.

Parallèlement à ce mouvement visant à enrayer les échanges d'œuvres sur les réseaux *peer-to-peer*, une autre tendance se dessine qui a pour objectif d'autoriser ces échanges. Il ne s'agirait donc plus de contenir ou réprimander des comportements mais de les encadrer par des mécanismes légaux. Mais nous le verrons, cette solution est de moins en moins proposée, la tendance étant à la cessation des atteintes, par le blocage de site ou la riposte graduée.

[35] Le texte adopté le 3 décembre 2010 est disponible sur http://trade.ec.europa.eu/doclib/html/147079.htm.
[36] Rapport sur l'application des droits de propriété intellectuelle sur le marché intérieur, (2009/2178(INI)) de Marielle GALLO, Commission des Affaires juridiques du Parlement Européen, disponible sur http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2010-0175+0+DOC+XML+V0//FR.

§1. Les systèmes légaux de cessation des atteintes au droit d'auteur

Il existe différents systèmes répressifs tendant à lutter contre le piratage d'œuvres en ligne, allant de la réponse graduée (I), à des systèmes d'avertissements (II) que l'on peut rapprocher d'un mécanisme de réponse graduée « atténuée », en passant par le blocage pur et simple des sites internet pirates (III).

I. Les mécanismes de réponse graduée

L'une des tendances actuelles pour lutter contre les téléchargements illégaux des œuvres sur les réseaux *peer-to-peer* consiste à élaborer des mécanismes dits de « réponse graduée » – ou *three-strikes*. Certains pays ont décidé d'emprunter cette voie (A), comme la France, le Royaume-Uni, la Corée du Sud ou la Nouvelle-Zélande, d'autres sont en train de la prendre en considération pour éventuellement l'intégrer dans leur droit national (B), comme en Belgique, au Danemark et en Allemagne, avec plus ou moins d'avancée… En Europe, la France a été la première à emprunter cette voie (1), suivie par le Royaume-Uni (2), mais c'est la Corée du Sud (3) qui a été la première à introduire un tel mécanisme dans sa réglementation interne, la Nouvelle-Zélande (4) étant le dernier des pays examinés à l'avoir fait.

A. Les pays dans lesquels le système est mis en œuvre

1. La France - HADOPI

La France a choisi de s'orienter vers un mécanisme de réponse graduée destiné à lutter contre les pratiques illégales de téléchargement d'œuvres protégées par le droit d'auteur. Elle est le premier pays européen à s'être lancé dans l'implémentation d'un tel mécanisme.

Une disposition du code de propriété intellectuelle, issue de la loi de transposition de 2006 de la directive « société de l'information », prévoyait déjà l'obligation de l'abonné internet de veiller à ce que sa connexion ne soit pas utilisée à des fins de contrefaçon, par lui ou par un autre. Mais cette obligation n'était pas assortie de sanctions. C'est ce que pallient notamment les « lois HADOPI ». Adoptées les 12 juin et 28 octobre 2009, ces lois sont la concrétisation de la dynamique originale choisie par la France[37]. Une obligation de sécurisation de la connexion internet incombe désormais à l'abonné ; celui-ci sera informé par son fournisseur d'accès à internet, qui est quant à lui obligé de livrer ces informations. Une nouvelle autorité est créée, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI). Elle a trois missions principales : la régulation des mesures techniques de protection, l'encouragement de l'offre légale sur internet et la protection des œuvres diffusées sur internet avec la mise en place de réponses dites graduées.

[37] Parmi une littérature foisonnante, voir Ch. CARON, « La lutte contre la contrefaçon sur Internet dans les lois HADOPI I et II », *CCE* janv. 2010, comm. n° 1, p. 24 et s. ; V.-L. BENABOU, « La riposte graduée contre la contrefaçon de masse : de l'alibi pédagogique à la tentation sécuritaire », *A&M*, 2010, p. 438.

Le mécanisme se déroule en plusieurs étapes. Tout d'abord, l'abonné doit être identifié par un agent assermenté grâce à son adresse IP. L'HADOPI, saisie, s'adresse ensuite au fournisseur d'accès à internet pour lever l'anonymat. Une fois les coordonnées dévoilées, l'HADOPI envoie une première recommandation à l'abonné via email qui a pour objet de l'informer sur son obligation de surveillance de l'accès internet, l'existence d'offres légales, les dangers de la contrefaçon et les moyens de sécurisation. Si rien ne change dans les six mois, l'HADOPI envoie une seconde recommandation du même type. A l'origine, l'HADOPI avait le pouvoir de suspendre la connexion internet de l'usager, ce qui a été censuré par le Conseil constitutionnel qui a qualifié le droit d'accéder à internet, qui fait partie de la liberté de communiquer et recevoir des informations, de droit fondamental[38]. Il s'ensuit que la coupure de l'accès internet ne peut désormais résulter que de la décision d'un juge judiciaire. Après deux rappels infructueux, l'HADOPI peut décider d'envoyer le dossier de l'internaute récidiviste au Ministère public qui décidera des poursuites éventuelles. La seconde loi HADOPI prévoit une nouvelle contravention de 5ème classe pour « négligence caractérisée » si l'abonné, après la seconde recommandation, n'a pas sécurisé son accès internet et a donc laissé faire les téléchargements illégaux. Par le biais d'une ordonnance pénale simplifiée qui permet une sanction plus rapide, le juge peut alors prononcer une peine qui peut aller jusqu'à la suspension de l'accès internet.

Au-delà du mécanisme de réponse graduée, les lois HADOPI ont instauré un nouvel article L. 336-2 du Code de la propriété intellectuelle qui sanctionne 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 juge du tribunal de grande instance peut ordonner toute mesure strictement nécessaire destinée à prévenir ou à faire cesser ces atteintes. Comme nous le verrons *infra*, ce nouvel article est la porte ouverte au blocage de sites internet par le juge français. Depuis l'adoption des lois, plusieurs textes réglementaires relatifs aux lois HADOPI ont été adoptés[39].

Fin février 2012, la Haute Autorité s'est enfin lancée dans la troisième phase de la réponse graduée[40], en envoyant au Procureur de la République la première série de dossiers des utilisateurs internet suspectés de téléchargement illégal. C'est maintenant au Parquet de décider s'il engagera des poursuites à l'encontre de ces récidivistes, qui risquent alors une amende de 1 500 euros et une

[38] Décision n° 2009-580 DC du 10 juin 2009, disponible sur le site du Conseil Constitutionnel (http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html).

[39] Le décret n° 2010-695 du 25 juin 2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur internet ; le décret n° 2010-872 du 26 juillet 2010 relatif à la procédure devant la commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet ; le décret n° 2010-994 du 26 août 2010 relatif à la commission prévue à l'article L. 132-44 du code de la propriété intellectuelle ; le décret n° 2010-1057 du 3 septembre 2010 modifiant le décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » ; la circulaire du 6 août 2010 relative à la présentation des lois n° 2009-669 du 12 juin 2009, favorisant la diffusion et la protection de la création sur Internet, et n° 2009-1311 du 28 octobre 2009, relative à la protection pénale de la propriété littéraire et artistique sur Internet, ainsi que de leurs décrets d'application ; le décret n° 2011-264 du 11 mars 2011 (HADOPI) relatif au traitement automatisé de données à caractère personnel, JORF n°0061 du 13 mars 2011

[40] « HADOPI enters first round of the 'third strike' phase », *The 1709 Blog,* 21 février 2012, disponible sur http://the1709blog.blogspot.com/2012/02/HADOPI-enters-first-round-of-third.html

première suspension de leur connexion internet pour une période pouvant aller jusqu'à un mois. Seulement 134 cas seraient concernés, et encore aucun internaute n'a vu sa connexion suspendue[41].

Depuis l'élection de François Hollande comme président de la République, qui s'était engagé à remplacer le système HADOPI, le gouvernement français a dernièrement chargé Pierre Lescure, ancien PDG de Canal+ et directeur du théâtre Marigny, de la mission de statuer sur l'avenir de l'HADOPI. Il y a déjà une volonté de la Ministre de la culture française Aurélie Filippetti de réduire le budget octroyé à la haute autorité, mais rien n'indique une volonté de sa part de mettre fin au mécanisme de la réponse graduée, bien qu'elle ait estimé disproportionnée la sanction de la coupure de l'accès à internet[42].

A la mi-septembre, un internaute a pour la première fois été condamné dans le cadre de la loi HADOPI, mais la sanction n'a pas été jusqu'à une limitation ou une coupure de sa connexion internet. Il a été condamné par le tribunal de police de Belfort à une amende de 150€ pour défaut de sécurisation de sa connexion, la sanction se voulant pédagogique.[43]

2. *Le Royaume-Uni*

En Europe, la deuxième loi intégrant un système de réponse graduée a été mise en place au Royaume-Uni en 2010, par l'adoption par la Chambre des Communes le 8 avril 2010 du *Digital Economy Act*[44] régulant les médias numériques. Ses articles 3 à 18 sont consacrés à la violation du droit d'auteur sur Internet. Il est prévu la possibilité pour les ayants droit, sous le contrôle du régulateur des télécommunications – l'OFCOM – d'obliger les fournisseurs d'accès à internet de restreindre ou couper l'accès à internet des internautes se livrant à des échanges en ligne non autorisés d'œuvres protégées par le droit d'auteur, et ce malgré la réception d'une lettre d'avertissement. Un mécanisme de réponse graduée intégral[45] est donc prévu.

La législation anglaise contenait déjà un arsenal législatif assez développé en matière de lutte contre la contrefaçon[46]. Mais même si des moyens légaux existent déjà, le problème n'est pas résolu pour autant en vertu de la difficulté pratique de mettre en œuvre ces dispositions, au niveau des preuves à rapporter ou des coûts consécutifs à chaque action[47].

---

[41] « HADOPI "failure" a warning for the UK? », *The1709 Blog*, 8 août 2012, disponible sur http://the1709blog.blogspot.be /2012/08/hadopi-failure-warning-for-uk.html

[42] B. MANENTI, « Aurélie Filippetti : 'Je vais réduire les crédits de l'HADOPI », *Le Nouvel Observateur*, 1er août 2012, disponible sur http://obsession.nouvelobs.com/high-tech/20120801.OBS8587/aurelie-filippetti-je-vais-reduire-les-credits-de-l-hadopi.html

[43] O. ROBILLART, « HADOPI : un premier internaute condamné à 150 euros d'amende », *Clubic*, 13 septembre 2012, disponible sur http://pro.clubic.com/legislation-loi-internet/hadopi/actualite-510745-hadopi-premier-internaute-condamne.html

[44] *Digital Economy Act 2010* (c.24), 18 avril 2010, disponible en ligne sur : http://www.legislation.gov.uk /ukpga/2010/24/contents.

[45] Il existe des mécanismes de réponse graduée « atténuée » consistant en l'envoi de lettres d'avertissement, sans l'étape ultime de la sanction (suspension de la connexion internet). Nous verrons *infra* que c'est ce que la Norvège et la Finlande ont décidé de mettre en place.

[46] Voy. notamment section 97 A et 24 (2) du *Copyright, Designs and Patents Act 1988.*

[47] V. DELFORGE, « La 'Réponse Graduée' en Europe et à l'étranger : comment venir à bout de la contrefaçon en ligne ? », *Le téléchargement d'œuvres sur internet. Perspectives en droits belge, français, européen et international*, Bruxelles, Larcier, 2012.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

a. Fonctionnement du système élaboré par le *Digital Economy Act*

Lorsqu'un ayant droit constate qu'un abonné à un service d'accès à internet viole son droit d'auteur, il doit faire un rapport de cette violation auprès du fournisseur de cet accès internet – un *Copyright Infringement Report*[48]. Ce rapport doit contenir le relevé de la violation ainsi que l'adresse IP du contrevenant. L'ayant droit n'est pas autorisé à faire correspondre cette adresse IP à l'abonné, seul le fournisseur d'accès détient cette information[49] et ne peut la transmettre à l'ayant droit sans une ordonnance préalable du tribunal[50].

Le fournisseur d'accès qui reçoit un tel rapport doit, après avoir vérifié sa pertinence, notifier à son abonné que l'adresse IP qui lui est associée est suspectée d'avoir été utilisée dans le cadre de téléchargement illégal d'œuvres protégées par le droit d'auteur[51]. Une telle notification doit être envoyée à l'abonné dans un délai d'un mois à compter du jour où le fournisseur reçoit le rapport[52]. La notification devra contenir un certain nombre d'informations, comme le nom de l'ayant droit qui a envoyé le rapport, des exemples de sources légales de contenu, *etc*.

Les fournisseurs d'accès doivent conserver une liste des rapports qu'ils ont reçus et des notifications qui ont été envoyées aux abonnés. Les ayants droit peuvent demander aux fournisseurs d'accès de leur fournir une liste anonymisée des violations du droit d'auteur – une *Copyright Infringement list* – pour une période donnée. Cette liste servira aux ayants droit à cibler les récidivistes les plus sérieux. Il est en effet impossible pour un ayant droit de savoir si la personne derrière l'infraction qu'il aura constatée est une habituée du téléchargement illégal ou seulement un individu curieux d'essayer le partage de fichier, ce qui dissuade la plupart du temps les ayants droit à se lancer dans des actions en justice très coûteuses et mauvaises pour leur image. De par l'obtention d'une liste ciblant spécifiquement les récidivistes permettra aux ayants droit de se lancer plus aisément dans une action judiciaire à l'encontre des internautes qui téléchargent leurs œuvres.[53]

Mesure importante pour la protection des données à caractère personnel, les données relatives aux utilisateurs ne pourront être fournies qu'après que les ayants droit aient obtenu une autorisation judiciaire[54]. Ils utiliseront donc cette liste anonymisée comme fondement de leur demande devant le juge afin d'obtenir le nom et l'adresse des utilisateurs détectés.[55] Une fois ces données obtenues, les ayants droit pourront alors directement envoyer aux contrefacteurs un dernier avertissement en leur demandant de mettre fin à l'atteinte en ligne et en les avertissant clairement qu'une action en justice sera menée s'ils ignorent cet ordre[56].

En cas de récidive, les ayants droit pourront introduire une action en justice[57]. Ne pas tenir compte des avertissements mène alors à la troisième étape de la réponse graduée : une limitation de l'accès internet de l'utilisateur ou la coupure pure et simple de sa connexion par le fournisseur d'accès[58].

---

[48] Article 124A du *Digital Economy Act* 2010.
[49] Article 124A (8) du *Digital Economy Act* 2010.
[50] *Idem* ; « *Digital Economy Act : Explanatory Notes* », disponible sur : http://www.legislation.gov.uk /ukpga/2010/24/pdfs/ukpgaen_20100024_en.pdf, point 42, p. 7.
[51] Article 124 A (4) du *Digital Economy Act* 2010.
[52] Article 124 A (5) du *Digital Economy Act* 2010.
[53] « *Digital Economy Act : Explanatory Notes* », point 45, p. 8.
[54] *Ibidem*, point 42, p. 7.
[55] *Ibidem*, point 46, p.8.
[56] *Ibidem*, point 37, pp. 6 et 7.
[57] *Idem*.
[58] « *Digital Economy Act : Explanatory Notes* », points 64 et 65, p. 11.

C'est le rôle de l'OFCOM de préciser les obligations et mesures techniques qui pourront être prises[59]. L'abonné ainsi sanctionné pourra bien évidemment faire appel de la décision prise à son encontre, et prouver qu'il n'est pas à l'origine des violations du droit d'auteur, et qu'il a pris des mesures raisonnables pour prévenir une infraction[60].

Enfin, des sanctions peuvent être prises à l'encontre des fournisseurs d'accès s'ils ne respectent pas leurs obligations d'imposer des mesures techniques aux abonnés, ou à l'encontre des fournisseurs et des ayants droit s'ils ne collaborent pas avec l'OFCOM[61].

b. Obligations de l'OFCOM

Il incombe à l'OFCOM de préparer un code qui fixera les modalités qui permettront de mettre en œuvre les obligations techniques des fournisseurs d'accès à internet, et qui sera destiné à accompagner le *Digital Economy Act*[62]. Tant que ce code ne sera pas en vigueur, les nouveaux articles de la loi n'auront aucun effet. L'OFCOM a soumis à consultation son projet de code en mai 2010[63] pour une période de 3 mois. Une fois approuvé, il devra être adopté par le Parlement et notifié à la Commission européenne.

Le système n'est pas encore mis en place à l'heure actuelle, le code n'étant toujours pas opérationnel. Le 26 juin 2012, l'OFCOM a publié une nouvelle version de son projet de code, avec le 26 juillet comme date limite pour la consultation publique. Après de possibles amendements, son adoption définitive est envisagée pour la fin de l'année. Cela a donc pour conséquence que les premières lettres d'avertissement ne seront pas envoyée avant 2014 car il est prévu un délai de 12 mois entre l'envoi de la première notification et le dévoilement des coordonnées de l'internaute qui a télécharger illégalement à l'ayant droit. Cela repousse donc d'un an l'envoi des avertissements, le directeur de l'OFCOM ayant déjà précisé en octobre 2011 que les lettres d'avertissement ne seront pas envoyées avant 2013[64]. Il avait indiqué à ce moment-là qu'une des causes du retard dans l'implémentation du mécanisme de réponse graduée est le choix de la technologie qui sera utilisée pour identifier chaque utilisateur soupçonné de partager illégalement des fichiers en ligne[65]. Une autre cause du retard dans la mise en place du mécanisme est l'affaire *British Telecom et Talk Talk* : en novembre 2010, les deux plus grands fournisseurs d'accès à internet du Royaume-Uni ont demandé à la *High Court of Justice* du Royaume-Uni de réexaminer le *Digital Economy Act* pour en vérifier la légalité[66]. Après avoir perdu en première instance, les FAI ont été déboutés en appel le 6

[59] *Ibidem*, point 61, p. 10.
[60] Article 124 K du *Digital Economy Act* 2010.
[61] Article 124 L du *Digital Economy Act* 2010.
[62] Article 124 C du *Digital Economy Act* 2010.
[63] « Online Infringement of Copyright and the Digital Economy Act 2010- Draft of Code of Practice to include processes to be followed, rights and obligations of rights owners, ISPs and subscribers », disponible sur http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/
[64] « DEA three strike letters won't start until 2013 », *CMU*, 24 octobre 2011, disponible sur http://www.thecmuwebsite.com/article/dea-three-strike-letters-wont-start-until-2013/
[65] Ibidem.
[66] Julien L., « La loi HADOPI britannique réexaminée par la Haute Cour », *Numerama,* 12 novembre 2010, disponible sur http://www.numerama.com/magazine/17311-la-loi-HADOPI-britannique-reexaminee-par-la-haute-cour.html. Cette affaire sera analysée dans le rapport II.

mars 2012[67], la cour ayant validé le système du DEA, l'estimant proportionné[68]. Elle a pourtant mis en garde les magistrats au niveau de la répartition des coûts du mécanisme entre les FAI et les pouvoirs publics.

En ce qui concerne le financement du mécanisme, il est prévu que les ayants droit interviendront à concurrence de 75 %, contre 25% pour les fournisseurs d'accès à internet. Les frais concernant l'OFCOM seront pris en charge exclusivement par les ayants droit.[69]

Le mécanisme de réponse graduée, bien que mis en place légalement, est plus qu'incertain quant à son implantation effective au Royaume-Uni.

3. La Corée du Sud

En 2007, la Corée du Sud a commencé à mettre à jour sa loi sur le droit d'auteur, en exigeant des fournisseurs de services en ligne de filtrer le contenu illégal à la demande des ayants droit[70].

Mais c'est en 2009 que la Corée du Sud a mis en place un système de réponse graduée, ce qui fait d'elle le premier pays à adopter un tel mécanisme[71]. La loi sur le droit d'auteur, suite à l'adoption le 22 juillet 2009 de plusieurs amendements, permet de limiter la responsabilité des intermédiaires sur Internet s'ils collaborent en vue de supprimer ou de mettre fin à la transmission de contenus identifiés comme étant en infraction. Un décret présidentiel fut adopté le 6 aout 2009 pour venir préciser les modalités procédurales de la loi[72]. Il prévoit une procédure initiale impliquant le ministère de la Culture, des Sports et du Tourisme et la Commission coréenne du droit d'auteur avant de pouvoir supprimer un contenu ou mettre en garde un contrevenant et fermer son compte Internet comme sanction ultime.

La loi coréenne prévoit deux types de procédure selon que le contrevenant est un individu ou un site de partage de fichiers qu'ils appellent *Bulletin Board*[73].

Pratiquement, en vertu de la procédure destinée aux individus, lorsque des œuvres sont transmises illégalement en ligne, le Ministre de la Culture, du Sport et du Tourisme peut ordonner au fournisseur d'accès à internet d'adresser à l'internaute contrevenant un avertissement du Ministre après une décision de la Commission du droit d'auteur. Il peut également exiger du fournisseur de

---

[67] *British Telecommunications Plc & Talk Talk Telecom Group Plc v. The Secretary of State for Culture, Olympics, Media and Sport* (2012) EWCA Civ. 232 (6 March 2012), confirmant (2011) EWHC 1021 (Admin) (20 April 2011), disponible sur http://www.bailii.org.

[68] A. STROWEL, « La lutte contre le téléchargement illicite : en attendant le succès de l'offre licite », *P.I.*, avril 2012 / n° 43, p.264.

[69] M. REES, « Le Royaume Uni civilise son HADOPI en facturant les ayants droit », *PC Inpact*, 24 août 2011, disponible sur http://www.pcinpact.com/actu/news/65262-royaumeuni-ofcom-HADOPI-cout-partage.htm.

[70] International Federation of the Phonographic Industry, « Digital Music Report 2012 », p. 22.

[71] J. MOYA, « South Korea to Become 1st Country with "Three-Strikes" for File-Sharers? », *ZeroPaid*, 29 mars 2009, disponible sur http://www.zeropaid.com/news/85895/south-korea-to-become-1st-country-with-three-strikes-for-file-sharers/ ; J. MOYA, « South Korea's "Three-Strikes" Law Takes Effect », *ZeroPaid*, 23 juillet 2009, disponible sur http://www.zeropaid.com/news/86703/south-koreas-three-strikes-law-takes-effect/

[72] Décret Présidentiel No. 21676- du 6 août 2009.

[73] Selon la définition de Wikipédia, un *Bulletin Board* « consiste en un serveur équipé d'un logiciel offrant les services d'échange de messages, de stockage et d'échange de fichiers, de jeux via un ou plusieurs modems reliés à des lignes téléphoniques ». Il s'agit d'une ancienne terminologie qui n'est plus très fréquente chez nous à l'heure actuelle.

supprimer ou suspendre la transmission illégale.[74] Si l'internaute reçoit au moins trois avertissements, le Ministre peut alors lancer la procédure de suspension de sa connexion internet. Pour cela, la Commission du droit d'auteur doit procéder à un examen de la situation, entendre les parties – le fournisseur d'accès et l'internaute. Si elle confirme la suspension, le Ministre transmettra alors l'ordre de suspension du compte au fournisseur d'accès.[75] Cette procédure se fait donc sans le passage devant un juge, le garde-fou étant assuré par le contrôle de la Commission du droit d'auteur.

En vertu de la procédure réservée aux *Bulletin Board*, le Ministre pourra exiger la fermeture de tels sites pour une durée maximale de 6 mois, en cas d'infractions renouvelées – réception de plus de trois avertissements – après avis de la Commission du droit d'auteur[76].

L'article 133-3 du *Copyright Act* prévoit une procédure complémentaire, par laquelle la Commission du droit d'auteur peut recommander – et non exiger – aux fournisseurs d'accès d'envoyer un avertissement aux utilisateurs qui reproduisent illégalement des œuvres protégées, ou de supprimer ou de cesser de transmettre des œuvres contrefaisantes ou de suspendre les comptes des utilisateurs récidivistes concernés[77]. Dans les 5 jours suivant la recommandation d'avertissement et dans les 10 jours suivant la recommandation de suspendre les comptes d'utilisateurs, le fournisseur d'accès à internet devra faire rapport à la Commission de droit d'auteur sur l'exécution de ces mesures[78]. Si le fournisseur ne suit pas les recommandations de la Commission du droit d'auteur, celle-ci peut saisir le Ministre afin qu'il prenne des mesures pour remédier à ces manquements, son avis n'étant dès lors plus requis[79].[80]

Au cours de la première année d'application de cette loi – jusqu'en juillet 2010 – 32 000 avertissements ont été lancés et 31 comptes d'utilisateurs ont été fermés, dans un pays considéré comme possédant l'un des taux de piratage les plus élevés du monde. L'industrie musicale coréenne considère qu'il s'agit d'une réussite susceptible de la sauver, même si les données indiquent qu'un nouvel essor des systèmes légaux avait déjà commencé avant l'adoption de ces dispositions spécifiques.[81]

Dans son *Digital Music Report* de 2012, l'IFPI annonce que la Commission du droit d'auteur a envoyé environ 100 000 *recommendation notices* aux fournisseurs d'accès leur enjoignant de demander aux contrevenants de cesser leurs agissements[82]. Selon le gouvernement coréen, 70 % des internautes téléchargeant illégalement arrêtent à la réception du premier avertissement, et 70 % des internautes récidivistes arrêtent après réception du deuxième[83].

---

[74] Article 133-2 (1) du *Korean Copyright Act*.
[75] Article 72-3 du décret présidentiel.
[76] Article 133 (4) du *Korean Copyright Act*.
[77] Article 133-3 (1) du *Korean Copyright Act.*
[78] Article 133-3 (2) du *Korean Copyright Act*
[79] Article133-3 (3 et 4) du *Korean Copyright Act*
[80] Dispositions disponibles sur: Heesob's IP Blog, « Facts and Figures on Copyright Three-Strike Rule in Korea », article du 24 octobre 2010, disponible sur http://hurips.blogspot.com/2010/10/facts-and-figures-on-copyright-three.html ; Voir également Annual Report 2009 Korea APAA Copyright Committee – Major Amendments to Korean Copyright Act – April, 2009"
[81] *Media Consulting Group*, « Le 'forfait sur le contenu' : une solution au partage illégal de fichiers ? », *op. cit.*, p. 56.
[82] International Federation of the Phonographic Industry, « Digital Music Report 2012 », p. 22.
[83] *Idem*.

Mais la Corée du Sud ne s'est pas arrêtée à la réponse graduée. Dans son rapport, l'IFPI parle aussi d'une autre mesure de lutte contre le partage illégal d'œuvres protégée. En avril 2011, est introduite une nouvelle loi qui exige que les sites de partage de fichiers et les services de *peer-to-peer* s'enregistrent auprès du gouvernement et implémentent des mesures de filtrage. La loi sur le droit d'auteur requiert donc que les fournisseurs de services en lignes, incluant les services de *peer-to-peer*, bloquent la distribution illégale de contenus contrevenants. Les services de *peer-to-peer* et les sites de partage de fichiers non-autorisés – au niveau international – sont ciblés par un programme de blocage de sites internet. La Commission coréenne des télécommunications a rapporté que 24 sites, pour la plupart internationaux, ont été bloqués dans les cinq premiers mois de l'année 2011.[84]

En Asie, toujours selon l'IFPI, la Corée du Sud reste le marché de la musique digitale légale ayant le plus de succès, avec environ trois millions d'abonnés. [85]

4. La Nouvelle-Zélande

En Nouvelle-Zélande, le Gouvernement a présenté en février 2010 un projet de loi intitulé *Copyright Infringing File Sharing Amendment Bill* (projet de loi modificative en matière de droit d'auteur partage de fichiers illégal) au Parlement[86]. Ce projet de loi est passé en première lecture le 22 avril 2010 et transmis à la Commission du commerce le 17 juin 2010. La Commission a rendu son rapport, accompagné de propositions d'amendements, le 3 novembre 2010[87]. Ce projet de loi a été adopté en avril 2011[88], et est entré en vigueur le 1er septembre 2011[89]. Début novembre, le système de réponse graduée a été lancé avec l'envoi des premières lettres d'avertissement aux internautes qui ont procédé à un partage illégal de fichiers protégés par le droit d'auteur[90]. Elle est à l'heure actuelle le dernier pays en date à avoir implémenté dans son droit national un mécanisme de réponse graduée.

Le nouvel article 122B du *Copyright Act* 1994 résume les nouvelles dispositions de la loi – les articles 122A à 122R – créant un régime spécial permettant aux ayants droit de prendre des mesures d'exécution à l'encontre des personnes qui violent le droit d'auteur par le partage de fichiers. Les ayants droit, après avoir repéré des téléchargements en ligne, enjoignent aux fournisseurs d'accès d'envoyer des avis d'infraction aux contrevenants présumés. Il y a trois types de notification : l'avis de détection, l'avis de mise en garde et l'avis d'exécution. Une fois ce dernier avis transmis au

[84] *Idem*.
[85] *Ibidem*, p. 8.
[86] Copyright (Infringing File Sharing) Amendment Bill 119-1 (2010), introduit le 23 février 2010, disponible sur : http://www.legislation.govt.nz/bill/government/2010/0119/8.0/DLM2764312.html ; Voyez Cabinet Economic Growth and Infrastructure committee's Paper : "Illegal Peer-to-peer file sharing", décembre 2009, disponible sur : http://www.med.govt.nz/upload/71039/FINAL%20PUBLIC%20Cabinet%20Paper%20for%20 the%20Copyright%20(Infringing%20File%20Sharing)%20Amendment%20Bill%202010,%20RIS%20Atta.PDF – « This paper makes recommendations for amendments to the Copyright Act 1994 (the Act) to provide a process for right holders to pursue repeat online copyright infringers. »
[87] Copyright (Infringing File Sharing) Amendment Bill 119-2 (2010), Government Bill – Reported from the Commerce Committee on 3 November 2010, disponible sur : http://www.legislation.govt.nz/bill/government/2010/0119/latest/DLM2764327.html
[88] Copyright (Infringing File Sharing) Amendment Act 2011 No 11, Public Act, disponible sur : http://www.legislation.govt.nz/act/public/2011/0011/latest/DLM2764312.html.
[89] Julien L., « La riposte graduée est active en Nouvelle-Zélande », *Numerama*, 3 septembre 2011, disponible sur http://www.numerama.com/magazine/19690-la-riposte-graduee-est-active-en-nouvelle-zelande.html
[90] « New Zeland three strikes gets underway », *CMU*, 1er novembre 2011, disponible sur http://www.thecmuwebsite.com/article/new-zealand-three-strikes-gets-underway/

contrevenant, qui a donc ignoré les avertissements, l'ayant droit peut prendre des mesures d'exécution à son encontre et tenter d'obtenir une injonction du tribunal pour le payement d'une amende ainsi qu'une injonction de suspension du compte internet pour une durée de six mois maximum.

L'association de l'industrie musicale de Nouvelle-Zélande RIANZ aurait déjà déposé 42 avis d'infraction qui seront transmis aux fournisseurs d'accès à internet des contrevenants présumés[91]. A l'heure actuelle, les trois fournisseurs principaux ont chacun un client à qui ont été envoyé les 3 avertissements, ce qui signifie que RIANZ peut maintenant les poursuivre devant le *Copyright Tribunal*[92].

D'après de récentes statistiques de la *Federation Against Copyright Theft* néo-zélandaise, depuis que la réponse graduée a été mise en place en Nouvelle-Zélande, les téléchargements illégaux de films auraient diminué de moitié[93].

5. Les Etats-Unis

Aux USA, un partenariat a été instauré entre le RIAA, MPAA et les principaux fournisseurs d'accès du pays pour mettre en place un système de réponse graduée pour lutter contre le téléchargement illégal. Leur volonté n'est pas de suspendre la connexion internet de l'abonné à qui aura été envoyée une série d'avertissements, mais plutôt de ralentir cette connexion.

Un tiers se chargera de la collecte des adresses IP des internautes présumés, qui seront alors inscrites dans une base de données et transmises au fournisseur d'accès qui sera chargé d'envoyer à son abonné suspecté une « copyright alert ». Ce qui diffère ici des mécanismes de réponse graduée français et anglais par exemple, c'est que ce sera seulement après cinq « strikes » que le fournisseur d'accès pourra prendre des mesures, telles que le ralentissement de la vitesse de la connexion, ou encore le renvoi de l'internaute vers des plateformes offrant des contenus légaux. Il est possible pour les internautes ayant reçu une ou plusieurs « copyright alert » de demander un réexamen indépendant de leur dossier, dont les frais s'élèvent à 35$.

B. Les pays dans lesquels le mécanisme est en projet

1. La Belgique

Le sénateur Miller, précédé quelques mois plus tôt du sénateur Monfils, a déposé une proposition de loi « visant à promouvoir la création culturelle sur Internet »[94]. La proposition prévoyait un procédé de réponse graduée en 4 étapes : l'envoi d'un avertissement à l'abonné par l'intermédiaire du fournisseur d'accès ; si l'abonné commet une nouvelle infraction dans les 6 mois l'envoi d'une lettre recommandée reprenant les mentions de la première lettre et proposant à l'abonné le paiement d'une amende ; la transmission du dossier au Parquet si l'internaute persiste dans ses

[91] *Ibidem*.
[92] « New Zealand three-strike law results in 50% decrease in infringement », *The 1709 Blog*, 23 juillet 2012, disponible sur http://the1709blog.blogspot.be/2012/07/new-zealand-three-strike-law-results-in.html
[93] *Idem*.
[94] Proposition de loi favorisant la protection de la création culturelle sur Internet, *Doc. Parl.*, Sénat, 2010-2011, n° 5-741/1.

comportements illégaux. Le juge pouvait alors décider de condamner l'internaute à une amende et à une limitation de l'accès au service de communication au public en ligne. Mais suite à l'audition des parties intéressées au Sénat le 11 mai 2011, et notamment des ayants droit, le sénateur Miller a déposé un amendement visant à retirer ce volet « réponse graduée » de sa proposition[95], par le retrait de ses articles 14 à 24.

2. L'Allemagne

Dans un premier temps l'Allemagne semblait rejeter la mise en place d'un mécanisme de réponse graduée à la française. Selon le Ministère de la Justice allemand, un tel mécanisme ne serait pas conforme à la législation allemande car il porterait atteinte à l'article 5 de la Constitution allemande, article qui garantit la liberté d'information et de communication ainsi que la liberté d'expression. De plus, toujours selon le Ministère de la Justice, la sanction du blocage de l'accès à internet serait constitutionnellement et politiquement très contestable.

Mais retournement de situation, le Ministre de la culture Bernd Neumann a annoncé fin mai 2011 qu'il envisageait de mettre en place un mécanisme de réponse graduée semblable au modèle HADOPI[96]. Il est nécessaire selon lui pour les fournisseurs d'accès à internet de « prendre leurs responsabilités ». Il a également annoncé qu'il rejetait la proposition de licence globale, système qu'il juge « inapplicable » et « anticonstitutionnel ».[97]

Outre cette volonté de l'Allemagne de se lancer dans la réponse graduée, la Cour fédérale allemande – la Bundesgerichtshof – a décidé que les fournisseurs d'accès à internet devaient fournir les noms et adresses des internautes qui partagent illégalement des fichiers protégés par le droit d'auteur à la demande des ayants droit, même si ces échanges sont réalisés hors du champ commercial[98].

II. Les systèmes d'avertissement

Nous pourrions également parler ici de mécanisme de réponse graduée « atténuée », car fonctionnant comme les deux premières étapes de la réponse graduée, mais sans la troisième, celle de la sanction de coupure ou suspension de la connexion internet du contrevenant. Notons que les systèmes présentés, celui de la Norvège (A) et de la Finlande (B) sont encore au stade de projet. Au Danemark (C), le système est seulement envisagé par le Gouvernement.

[95] Proposition de loi favorisant la protection de la création culturelle sur Internet, Amendement déposé par R. MILLER et F. BELLOT le 24 mai 2011, *Doc. Parl.*, Sénat, 2010-2011, n° 5-741/2.
[96] Cette annonce a été faite lorsque le Ministre s'exprimait lors d'une convention de la CDU, le parti démocrate-chrétien allemand.
[97] « L'Allemagne envisage un système de riposte graduée », *Le Monde*, 30 mai 2011, disponible sur http://www.lemonde.fr/technologies/article/2011/05/30/telechargement-l-allemagne-envisage-un-systeme-de-riposte-graduee_1529266_651865.html.
[98] http://the1709blog.blogspot.com/2012/08/more-on-file-sharing-german-isps-must.html

A. La Norvège

En Norvège, le Gouvernement a déposé une proposition de modification de la loi n° 2 du 12 mai 1961 relative au droit d'auteur sur les œuvres littéraires, scientifiques et artistiques (*Copyright Act*)[99], prévoyant la mise en place de mesures contre le partage illégal de fichiers et autres atteintes au droit d'auteur sur internet (surveillance et enregistrement de l'adresse IP, identification, blocage de sites web sur lesquels le droit d'auteur fait de toute évidence l'objet d'une atteinte considérable). L'optique de la proposition est de faciliter la lutte contre le téléchargement illégal pour les ayants droit. Le Gouvernement norvégien a répugné à adopter un quelconque mécanisme de réponse graduée, mais désire plutôt faciliter légalement l'identification individuelle des internautes pour les ayants droit, ainsi que l'envoi d'injonctions pour forcer les fournisseurs d'accès à internet à bloquer les sites coupables d'atteintes au droit d'auteur[100].

Cette proposition insère de nouveaux articles dans le *Copyright Act*. Le premier article, portant sur le traitement des informations personnelles relatives à la contrefaçon du droit d'auteur, exempterait les ayants droit d'obtenir une autorisation pour traiter des informations personnelles relatives à la contrefaçon du droit d'auteur, dans le cas où ce traitement est nécessaire pour établir, faire valoir ou défendre une prétention juridique[101]. Ce traitement de données servira à récolter les adresses IP des internautes contrevenants.

L'article suivant prévoit que les ayants droit peuvent saisir le juge pour que celui-ci exige des fournisseurs d'accès la remise de l'information qui identifie le titulaire de la connexion à l'origine de l'infraction[102]. Avant que la Cour ne rende sa décision, les ayants droit doivent demander à l'Autorité des Postes et Télécommunications d'exempter le fournisseur de son obligation de confidentialité prévue par la loi norvégienne de communication électronique[103]. Cette autorité peut bien évidemment refuser d'accorder une telle exemption si la demande est déraisonnable envers le bénéficiaire de la confidentialité[104]. Dans sa prise de décision, le juge devra faire la balance entre l'intérêt de l'abonné et celui de l'ayant droit, et la gravité, l'étendue et le caractère nuisible de l'infraction devront être spécialement pris en considération[105].

Mais la procédure ne s'arrête pas là. Si la Cour décide que l'information doit être transmise à l'ayant droit, la requête d'octroi doit être présentée au tribunal du district du fournisseur d'accès à la cause. Dans le mois de la décision, le fournisseur d'accès a l'obligation d'informer l'abonné de la communication des informations le concernant aux ayants droit. L'affaire ne peut être rendue publique qu'un mois après cette notification, ou au moins six mois après si l'affaire a été classée.[106]

---

[99] Proposed amendments to Act no. 2 of 12 May relating to copyright in literary, scientificand artistic works (Copyright Act), document disponible sur http://www.scribd.com/doc/68735157/Norvege.

[100] « Norway Government publishes anti-file-sharing proposals », *CMU*, 24 mai 2011, disponible sur http://www.thecmuwebsite.com/article/norway-government-publishes-anti-file-sharing-proposals/

[101] Nouvel article 56a du *Copyright Act*.

[102] Nouvel article 56b, al. 1 du *Copyright Act*.

[103] Nouvel article 56b, al. 2 du *Copyright Act*.

[104] *Idem*.

[105] Nouvel article 56b, al. 3 du *Copyright Act*.

[106] Nouvel article 56b, al. 4 et 5 du *Copyright Act*.

Nous pouvons constater que la Norvège a décidé de mettre en place des garde-fous importants pour protéger les données à caractère personnel des internautes. La décision de fournir de telles informations aux ayants droit est loin d'être automatique, contrairement au cas de la France.

Ces deux premières sections de la proposition de loi sont donc consacrées à la poursuite des utilisateurs finaux. Les deux dernières visent quant à elles le blocage des sites internet, avec une option pour le législateur entre deux alternatives : soit la compétence d'ordonner le blocage reviendrait à l'Autorité norvégienne des médias, soit cette prérogative reviendrait à un tribunal. Nous analyserons dans le paragraphe consacré au blocage de sites internet ces deux dernières sections de la proposition de loi norvégienne[107].

B. La Finlande

Le 29 octobre 2010, après plus de deux ans de discussions, la Finlande a déposé un projet de loi visant à combattre les contrefaçons d'œuvres protégées sur Internet. Le projet prévoit l'instauration d'un mécanisme de réponse graduée, mais atténué. Il se limite aux deux premières étapes du système – l'identification et l'envoi d'avertissements – laissant donc tomber la troisième, celle de la sanction. A l'instar de la Norvège[108], la Finlande insiste sur le fait qu'elle n'a aucune intention de lancer un mécanisme de réponse graduée intégral[109].

Ce projet amende la loi sur le droit d'auteur, ainsi que la loi sur la protection des données à caractère personnel dans le cadre des communications électroniques (*Act on Protection of Privacy in Electronic Communications*) et promeut l'*e-commerce* et la création des contenus sur internet[110].

A l'instar du Royaume-Uni, les ayants droit seraient chargés de collecter les adresses IP des personnes suspectées de téléchargement illégal. Une fois récoltées, les ayants droit enverraient ces adresses aux fournisseurs d'accès, qui seraient alors tenus d'envoyer les lettres d'avertissement sous forme de courriers électroniques aux abonnés titulaires de ces adresses IP. Si ces derniers ignorent les avertissements, ils ne subiront pas la troisième phase de la réponse graduée, à savoir la coupure de leur connexion Internet. La méthode finlandaise se veut donc plus éducative, avec une volonté de responsabiliser les internautes, que punitive[111]. Cette méthode se veut également respectueuse de la vie privée de l'internaute, le Gouvernement finlandais assurant que l'identité de l'abonné resterait entre les mains du fournisseur d'accès et ne serait en aucun cas révélée à l'ayant droit collectant les adresses IP[112].

Le 14 mai 2012, un tribunal de district finlandais a eu à examiner si le simple acte de fournir une connexion wifi non protégée par un mot de passe peut constituer une atteinte au droit d'auteur.

---

[107] Cf *infra.*

[108] Voir *infra.*

[109] « Finland introduces file-sharing warning letters », *CMU*, 3 novembre 2010, disponible sur http://www.thecmuwebsite.com/article/finland-introduces-file-sharing-warning-letters/

[110] Julien L., « La Finlande songe à une riposte graduée limitée aux avertissements », *Numerama*, 2 novembre 2010, disponible sur http://www.numerama.com/magazine/17221-la-finlande-songe-a-une-riposte-graduee-limitee-aux-avertissements.html

[111] *Idem*.

[112] ENIGMAX, « Files-shares to receive warning letters but no 3 strikes », *TorrentFreak*, 2 novembre 2010, disponible sur http://torrentfreak.com/file-sharers-to-receive-warning-letters-but-no-3-strikes-101102/

L'examen des dispositions finlandaises pertinentes s'est fait au regard des directives 2000/31, 2001/29 et 2004/48, et le tribunal en a conclu que le propriétaire du wifi ne peut pas être tenu pour responsable pour des infractions commises par des tiers via sa connexion.[113]

C. Le Danemark

Le précédent gouvernement danois avait proposé un modèle basé sur l'envoi d'avertissements[114]. L'idée était que les ayants droit qui ont détecté une infraction au droit d'auteur, associée à une connexion internet spécifique, pourraient demander au fournisseur de cet abonné d'envoyer une lettre à celui-ci lui indiquant qu'une infraction au droit d'auteur a eu lieu sur son compte. Si l'atteinte continue, une deuxième lettre pourrait alors lui être envoyée, mais sans que celle-ci n'ait de véritables effets juridiques.[115] Le gouvernement a été très friand de cette idée, mais le modèle n'a jamais été adopté au Parlement.

Une nouvelle élection nationale a eu lieu depuis au Danemark et le nouveau gouvernement n'a pas relancé la proposition. Le 20 juin 2012, le gouvernement a officiellement annoncé qu'il abandonnait cette idée. Il sera prévu à la place des mécanismes favorisant le développement et la création de meilleures offres légales, insistant plus sur l'éducation des internautes que sur leur poursuite.[116]

D. La Suède

En Suède, le législateur a adopté une loi[117] – qui transpose la directive européenne 2004/48/CE relative au respect des droits de propriété intellectuelle – destinée à réprimer les échanges illégaux d'œuvres sur Internet. Cette loi – dite « loi IPRED » – a été adoptée le 1er avril 2009. Son objectif est que les titulaires de droits puissent obtenir plus facilement les données à caractère personnel des internautes s'adonnant à ces pratiques illégales en forçant les fournisseurs d'accès à internet à leur fournir ces données grâce à une décision de justice. Sur base de ces informations, les ayants droit pourront envoyer directement un avertissement à l'utilisateur et éventuellement introduire une action civile dans le cas de récidive.[118]

---

[113] Ville Oksanen, disponible sur http://www.turre.com/2012/05/finnish-court-open-wifi-owner-not-liable-for-file-sharing-copyright-infringement/

[114] E. FORDE, « Denmark plans 'three strikes' law while South Korea ups 'one strike' disconnection », *MusicWeek*, 27 octobre 2010, disponible sur http://www.musicweek.com/story.asp?storyCode=1043063&sectioncode=1

[115] F. S. KIRKEGAARD, « Her er Danmarks svar på 3-strikes », *Comon*, 5 octobre 2010, disponible sur http://www.comon.dk/art/124218/her-er-danmarks-svar-paa-3-strikes

[116] http://torrentfreak.com/denmark-kills-file-sharing-warnings-launches-legal-services-initiative-120620/

[117] Chap.7 on penal and civil liabilities, Act 1960:729, of December 30, 1960, as amended up to April 1, 2009 disponible sur http://www.regeringen.se/content/1/c6/01/51/95/20edd6df.pdf.

[118] E. PALM, « Swedish antipiracy law stirs up political waters », *CNET*, 31 mars 2010, disponible sur http://news.cnet.com/8301-1023_3-10207718-93.html

Jusqu'à il y a peu, cette loi n'était pas réellement suivie d'effet car les fournisseurs d'accès refusaient de coopérer[119]. Mais depuis le 19 avril 2012, la Cour de justice a répondu aux questions préjudicielles qui lui avaient été posées[120], questions relatives à la compatibilité de l'obligation faite aux fournisseurs d'accès de communiquer des données à caractère personnel aux fins d'identification d'un abonné au regard de la directive 2006/24 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

De manière anecdotique nous pouvons également signaler que les « pirates » informatiques ont leur propre religion en Suède. En effet, elle a octroyé au « kopisme » (jeu de mot sur « copy me ») le statut de religion début janvier de cette année[121]. Cette religion, dont la Sainte Trinité est « Copiez, Téléchargez et Partagez » prône le téléchargement illégal sur internet.

III. Le blocage de sites internet

A. Les pays dans lesquels le mécanisme est implémenté

1. L'Espagne – la Ley Sinde

En Espagne, c'est la *Ley Sinde*[122] qui règle la question du téléchargement illégal en ligne, en prévoyant la possibilité pour les ayants droit de faire bloquer les sites proposant du contenu illégal et violant les droits d'auteur, et ce via une procédure accélérée. Elle entrera en vigueur en mars 2012. Son adoption n'a pas été de tout repos, suite à de nombreuses modifications et à une vive opposition émanant de différentes sphères.

Le 8 janvier 2010, le Conseil des Ministres espagnol a adopté de nouvelles dispositions relatives au respect des droits intellectuels sur internet qui ont été insérées dans une loi plus générale : la *ley de economia sostenible*, dite *Ley Sinde*, du nom de la Ministre de la culture Angeles Gonzales Sinde[123]. Ce projet de loi fut rejeté le 21 décembre 2010 par la Commission des affaires économiques du Congrès espagnol, une partie des députés (20 contre 18) estimant que la possibilité « de fermer des sites internet sans avoir l'aval d'une autorité judiciaire (…) ouvre la porte au non-respect de droits fondamentaux comme la liberté d'expression de la part du pouvoir politique »[124]. Après de légers amendements, dont une obligation de passer par le juge dans la procédure de blocage, la loi relative

[119] G. CHAMPEAU, « La loi suédoise IPRED est un succès : le piratage augmente, les ventes aussi », *Numerama*, 2 avril 2010, disponible sur http://www.numerama.com/magazine/15417-la-loi-suedoise-ipred-est-un-succes-le-piratage-augmente-les-ventes-aussi.html

[120] C.J.U.E. (3e ch.), 19 avril 2012, *Bonnier Audia AB* c. *Perfect Communication Sweden AB*, C-461/10, non encore publié au recueil. Nous analyserons *infra* cette décision de la Cour de justice.

[121] H. PUEL, « Le piratage reconnu religion officielle en Suède », *01.net*, 5 janvier 2012, disponible sur : http://www.01net.com/editorial/551822/le-piratage-reconnu-religion-officielle-en-suede/

[122] Ley 2/2011, de 4 de marzo, de Economia Sostenible, Boletìn Oficial del Estado n° 55 du 5 mars 2011, pp. 25033 et s., disponible en ligne sur http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf.

[123] Cette loi entraine la modification de trois autres lois, à savoir la loi relative aux services de la société de l'information, la loi relative aux droits de propriété intellectuelle et la loi relative au contentieux administratif ; Analyse juridique disponible sur http://derechoenred.com/blog/todo-sobre-la-ley-de-economia-sostenible/analisis-juridico-de-la-ley-de-econo mia-sostenible.

[124] C. CARUANA, « L'Espagne dit non à l'instauration d'une HADOPI ibérique », *DegroupNews*, 24 décembre 2011, disponible sur http://www.degroupnews.com/actualite/n5698-HADOPI-espagne-internet-telechargement-piratage.html.

à l'économie durable a été approuvée par le Sénat et par le Congrès le 15 février 2011[125]. La loi a finalement été adoptée le 30 décembre 2011 lors du second Conseil des ministres du nouveau gouvernement espagnol, par la publication dans le *Boletin Oficial del Estado* (BOE) d'un décret royal portant création d'une Commission de la Propriété intellectuelle[126]. Son entrée en vigueur était prévue pour mars 2012, mais à notre connaissance rien n'a eu lieu depuis. Il était nécessaire qu'une solution soit trouvée, l'Espagne ayant longtemps été considérée comme un paradis pour les sites de téléchargement illégal[127].

Il est créé une Commission de la propriété intellectuelle (Comisión de Propiedad Intelectual)[128], organe administratif collégial de niveau national composé de juristes indépendants et d'experts en technologie, qui dépendra du Ministère de l'éducation, de la culture et du sport, régie par la loi consolidée de propriété intellectuelle. Cette Commission est organisée en deux sections. La première exercera des fonctions de médiation et d'arbitrage[129], elle jouera donc plutôt un rôle préventif. Concernant la fonction de médiation, ses compétences s'étendent à toutes les matières directement liées à la gestion collective des droits de propriété intellectuelle. La fonction d'arbitrage s'étend quant à elle à la résolution des conflits entre les différentes sociétés de gestion, entre les ayants droit et les sociétés de gestion, ainsi qu'entre eux et les organismes de radiodiffusion. La seconde section aura un rôle plus répressif de « sauvegarde des droits de propriété intellectuelle » contre sa violation par les responsables de services de la société de l'information[130]. Il est alors prévu que la Commission saisie par les ayants droit en cas de partage non autorisé d'œuvres sur internet, sera en charge d'introduire les plaintes auprès du juge compétent, *los Juzgados Centrales de lo contencioso administrativo*. Relevons que ce recours au juge n'était pas prévu dans la première mouture de la loi, mais suite à de fortes contestations émanant tantôt des internautes, tantôt de l'Europe, le recours au juge a été rajouté dans la loi, et ce pour assurer la protection des droits fondamentaux concernés.

Concernant son rôle plus répressif, il est prévu que les ayants droit pourront saisir la seconde section de la Commission afin de faire bloquer ou fermer rapidement l'accès aux sites internet depuis lesquels des contenus protégés par le droit d'auteur sont susceptibles d'être téléchargés. La seconde section envoie alors à l'administrateur du site une injonction de retirer, dans les 48 heures, le contenu contrevenant. Le retrait volontaire du contenu violant le droit d'auteur met fin à la procédure engagée. En cas d'inaction ou de refus de l'administrateur du site, c'est au juge d'intervenir. Il aura alors quatre jours pour convoquer et entendre les arguments de toutes les

[125] Ley 2/2011, de 4 de marzo, de Economía Sostenible, Boletin Oficial del Estado n° 55 du 5 mars 2011, pp. 25033 et s., disponible sur http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf. Voir A. GALLEGO, « L'Espagne et la banalisation de la contrefaçon musicale et audiovisuelle », Propriétés Intellectuelles, Juillet 2011, p. 351.

[126] Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisiòn de Propiedad Intelectual, Boletin Oficial del Estado n° 315 du 31 décembre 2011, pp. 147011 et s., disponible en ligne sur http://www.boe.es/boe/dias/2011/12/31/pdfs/BOE-A-2011-20652.pdf

[127] « La 'ley Sinde' aprobada por el PP entrará en vigor en marzo », *El País*,31 décembre 2011, disponible sur http://cultura.elpais.com/cultura/2012/01/02/actualidad/1325458803_850215.html ; ENIGMAX, « Website blocking law implemented by new Spanish government », *TorrentFreak*, 2 janvier 2012, disponible sur http://torrentfreak.com/website-blocking-law-implemented-by-new-spanish-government-120102/

[128] Art. 158, 1° del Texto Refundido de la Ley de Propiedad Intelectual, « Se crea en el Ministerio de Cultura, la Comisión de Propiedad Intelectual, como órgano colegiado de ámbito nacional, para el ejercicio las funciones de mediación y arbitraje y de salvaguarda de los derechos de propiedad intelectual que le atribuye la presente Ley ».

[129] Capitulo II, Articulo 2, 1.

[130] Capitulo VI, Articulo 13, 1.

parties avant de rendre son jugement relatif à la question de savoir si le site devrait être fermé ou pas.[131] Il est bien évidemment donné au contrevenant présumé la possibilité de contester la décision. Ces dispositions sont sans préjudice des actions civiles, pénales et administratives appropriées.

Il s'agit d'une procédure accélérée de *notice and takedown*, sa durée ne dépassant pas en moyenne dix jours.

La Commission peut également ordonner à un prestataire de services de la société de l'information de divulguer les coordonnées d'un contrevenant, ou d'ordonner la fin du service, mais cette injonction, elle aussi, ne prend effet qu'après avoir été validée par un juge.

Comme nous pouvons le remarquer, cette loi ne crée aucune obligation générale de surveillance, mais elle est sans préjudice d'autres recours (procédures civiles, pénales ou administratives) accessibles aux titulaires de droits[132].

Cette loi se distingue à plusieurs égards du système de réponse graduée français ou anglais. Premièrement, aucune disposition de cette loi ne vise spécifiquement l'utilisateur final, la loi *Sinde* optant plutôt pour un mécanisme permettant de trouver et d'arrêter les prestataires de services qui facilitent directement ou indirectement les violations des droits d'auteur[133], avec un blocage de site à la clé. Deuxièmement, la procédure prévue dans la loi *Sinde* est extrêmement plus courte – et par là moins coûteuse – que celle de la HADOPI et que d'autres procédures que l'on peut rencontrer actuellement.

Cette loi rappelle le projet de loi SOPA qui est pour le moment à l'étude aux Etats-Unis[134]. Elle a été critiquée car justement trop influencée par les autorités américaines. Le quotidien *El Pais*, en possession d'informations provenant du site Wikileaks, avait démontré que cette loi espagnole avait été fortement instrumentée par les États-Unis[135].

Il faudra maintenant attendre les suites de son entrée en vigueur pour voir comment cette procédure se déroulera en pratique. Mais rien n'est encore sûr concernant son entrée en vigueur effective, la Cour suprême espagnole ayant annoncé le 8 février 2012 qu'elle acceptait de se saisir d'une requête déposée par l'Association des usagers d'internet, dans le but de procéder à une analyse de conformité de la loi espagnole, qui selon l'Association ne respecte pas le droit espagnol en confiant le pouvoir de bloquer un site internet à une instance administrative et non à un juge[136].

2. Le blocage prévu dans de nombreux pays via l'action en cessation

Outre la mise en place de règles spécifiques en matière de piratage en ligne implémentées dans le droit interne des pays, il est possible de procéder au blocage de site internet par les actions en

[131] Art.122*bis* de la Ley de la Jurisdicción Contencioso-administrativa
[132] *Media Consulting Group*, « Le 'forfait sur le contenu' : une solution au partage illégal de fichiers ? », *op. cit.*, p. 61.
[133] *Ibidem*, pp. 61 et 62.
[134] Voir *infra.*
[135] C. WOITIER, « L'Espagne adopte sa loi HADOPI sous la pression américaine », *Le Figaro*, 6 janvier 2012, disponible sur http://www.lefigaro.fr/hightech/2012/01/06/01007-20120106ARTFIG00499-l-espagne-adopte-sa-loi-HADOPI-sous-la-pression-americaine.php
[136] Julien L., « La lutte anti-piratage est à la peine en Espagne », *Numerama*, 18 février 2012, disponible sur http://www.numerama.com/magazine/21738-la-lutte-anti-piratage-est-a-la-peine-en-espagne.html

cessation de contrefaçon qui existent dans de nombreuses réglementations nationales, comme la Belgique par exemple. Ces pays disposent déjà d'une arme contre la pratique du téléchargement et du partage illicite en ligne mais qui s'avère souvent insuffisante et inconsistante lorsqu'il s'agit de bloquer durablement un site internet. Nous reviendrons sur le blocage par voie jurisprudentielle au point III de la présente section.

B. Les pays dans lesquels le mécanisme est en projet

1. Les Etats-Unis

Aux Etats-Unis, il y a actuellement[137] deux propositions de lois pendantes qui promettent une modification en profondeur des moyens de lutte contre le piratage en ligne, les projets « Stop Online Piracy Act » (SOPA)[138] – examiné à la Chambre – et « Protect IP Act » (PIPA)[139] – déposé au Sénat. Elles visent toutes deux à lutter contre le piratage d'œuvres protégées par le droit d'auteur sur internet par un blocage des sites internet, à la fois nationaux et étrangers.

a. Le projet de loi SOPA

La proposition de loi SOPA a été déposée à la Chambre des représentants des Etats-Unis le 26 octobre 2011 par le représentant républicain Lamar Smith, et a été examinée par la *U.S. House Comittee on the Judiciary.* La proposition de loi SOPA est un produit des lobbies américains du film, de la musique, et des chaînes de télévision.

Elle prévoit d'étendre la compétence juridictionnelle américaine à tous les sites localisés à l'étranger, dont les services sont dirigés vers les Etats-Unis et qui hébergent du contenu contrefait. Selon le texte de la proposition le Procureur Général peut obtenir un ordre de justice à l'encontre d'un site étranger commettant ou facilitant le piratage en ligne pour exiger le retrait du contenu illicite et prévenir du retour de ce contenu déjà retiré. Le Procureur peut, à ce titre, entamer une action *in personam* ou *in rem* en fonction de la possibilité d'identifier ou non l'exploitant du site ou du titulaire du nom de domaine.[140]

La loi SOPA permettrait également au Procureur ou à un ayant droit lésé par un site hébergé aux USA ou hors de ses frontières, de faire bloquer ce site ou d'obtenir une injonction imposant d'une part aux intermédiaires financiers de suspendre les revenus publicitaires de ces sites et de bloquer les moyens de paiement en ligne, et d'autre part aux moteurs de recherche de déréférencer le site. Le propriétaire du site, son exploitant, ou le titulaire du nom de domaine, peut fournir une contre-notification expliquant que le site en cause n'est pas dédié à la violation du droit d'auteur. Mais le site serait d'abord bloqué et ce n'est qu'après qu'il pourrait faire appel au tribunal via une contre-notification, ce qui peut constituer un obstacle pour les sites internet de moins grande ampleur. L'ayant droit peut ensuite intenter une action en injonction restrictive contre le propriétaire du site

[137] Màj au 20/01/2012.
[138] H.R.3261, *Stop Online Piracy Act* (SOPA) du 26 octobre 2011, 112ème Congrès (2011-2012), 1ère Session, disponible sur : http://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf
[139] S. 968, *Protect IP Act* (PIPA) du 12 mai 2011, 112ème Congrès (2011-2012), 1ère Session, disponible sur http://www.gpo.gov/fdsys/pkg/BILLS-112s968is/pdf/BILLS-112s968is.pdf
[140] Sec. 102 de la proposition de loi SOPA.

(ou le site lui-même en cas d'action *in rem*) si une telle contre-notification est fournie ou contre l'intermédiaire qui n'aurait pas suspendu ses prestations.[141]

Les fournisseurs de services en ligne, des moteurs de recherche et des intermédiaires financiers, sur réception d'une ordonnance du tribunal relative à une action du Procureur Général, devraient prendre certaines mesures préventives, y compris empêcher l'accès au site contrefaisant.

La loi SOPA offrirait une immunité de responsabilité pour les intermédiaires qui ont pris des mesures requises par la loi ou qui auraient volontairement bloqué l'accès ou mis fin à leur affiliation avec de tels sites. Ils seraient dès lors à l'abri de toute action ultérieure en dommages et intérêts émanant des sites bloqués par erreur.[142]

Elle étendrait l'infraction de contrefaçon du droit d'auteur à la représentation publique d'œuvres protégées par transmission numérique et d'œuvres destinées à la diffusion commerciale en les rendant accessible sur un réseau informatique. Le streaming illégal de contenu protégé serait alors qualifié d'acte criminel.[143]

b. Le projet de loi PIPA

Le projet de loi *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011* - ou *Protect IP Act* (PIPA) – a été proposé au Sénat américain le 12 mai 2011 par le sénateur démocrate Patrick Leahy. Il est une nouvelle version du projet de loi *Combating Online Infringement and Counterfeits Act*[144] (COICA) qui avait finalement été refusé malgré un passage avec succès devant le Comité judiciaire du Sénat.

Le projet de loi PIPA vise à mettre en place un filtrage des sites internet par leur nom de domaine. Il autorise le Procureur général à entamer une action contre le titulaire d'un nom de domaine étranger – *nondomestic domain name* – utilisé par un site internet dédié à des activités de contrefaçon, ou si ce titulaire est introuvable, déclencher une action *in rem* contre le nom de domaine lui-même.[145] A l'instar de la loi SOPA, ce projet étend également les compétences juridictionnelles des Etats-Unis à tous les sites localisés à l'étranger.

Dans ce cadre, le tribunal est autorisé, suite à une demande du Procureur Général ou d'un ayant droit, d'émettre une injonction d'interdiction temporaire, ou une injonction contre le nom de domaine étranger de cesser les activités du site lié à ce nom de domaine qui contient du contenu contrefait nuisant aux intérêts des ayants droit américains[146]. Cette injonction temporaire de « cease and desist » est mise en place pour ordonner à un intermédiaire de couper un flux et de s'abstenir de le rouvrir.

Le Procureur est chargé d'identifier et d'ordonner aux intermédiaires techniques – incluant les serveurs DNS, les services de paiement en ligne, de publicité sur internet, mais également les moteurs de recherche, les portails de liens hypertextes – intermédiaires dont l'action est nécessaire

[141] « Bill summary and status », disponible sur http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03261:@@@L&summ2=m&.
[142] Sec. 104 de la proposition de loi SOPA.
[143] Sec. 201 de la proposition de loi SOPA.
[144] S.3804, *Combating Online Infringement and Counterfeits Act* du 20 septembre 2010, 111ème Congrès (2009-2010), disponible en ligne sur : http://www.govtrack.us/congress/billtext.xpd?bill=s111-3804.
[145] Sec. 3, (a) de la proposition de loi PIPA.
[146] Sec. 3, (b) de la proposition de loi PIPA.

pour prévenir les infractions au droit d'auteur, de prendre toutes les mesures nécessaires à l'encontre de ces sites contrefaisants[147].

Le projet PIPA prévoit également, tout comme le projet SOPA, de protéger les intermédiaires qui ont pris des mesures provisoires à l'encontre d'un site internet, de leur propre chef ou sous contrainte d'une ordonnance de justice, de toute action ultérieure en dommages et intérêts de ces sites qui auraient été bloqués par erreur[148].

c. Qu'en est-il actuellement ?

Le vote des deux propositions, suite au nombre important d'oppositions exposées à leur encontre, a été reporté à une date ultérieure par le Congrès américain, afin de laisser du temps à leurs concepteurs de corriger les principaux défauts soulevés par leurs opposants[149]. Harry Reid, le leader des démocrates du Sénat a déclaré qu' « *À la lumière des récents évènements [...], il n'y a aucune raison pour que les problèmes légitimement soulevés par nombre d'entre nous au sujet de cette loi ne soient pas résolus* ». Lamar Smith, président de la Commission des lois, a annoncé que concernant la loi SOPA, la Chambre des représentants allait « *reporter l'examen du texte jusqu'à ce qu'il y ait un plus large consensus (…) J'ai entendu les critiques et je prends au sérieux leurs préoccupations. Il est clair que nous devons revoir l'approche sur la meilleure façon de s'attaquer aux problèmes des voleurs étrangers* ».[150]

Les politiques ne pouvaient se permettre d'ignorer les critiques et inquiétudes de l'opinion publique, les plus concernés étant les défenseurs des libertés individuelles et des acteurs de l'internet, parmi lesquels figurent des géants du web tels Google, Wikipédia, Facebook, etc. Parmi les détracteurs du projet, on retrouve également des universitaires[151]. Ses opposants estiment qu'il pose d'importantes questions en matière de liberté individuelle des internautes. Au final, ce sont plus de 7 millions de personnes qui ont signé la pétition lancée sur internet pour protester contre les projets de loi. Mais cela ne signifie pas que les deux lois sont abandonnées, leurs promoteurs considérant qu' « il est toujours essentiel de modifier la législation américaine afin de protéger l'économie du pays et les emplois américains dans un environnement numérique beaucoup plus difficile à maîtriser ». Attendons maintenant de voir comment les sénateurs parviendront à modifier les textes de telle manière qu'ils reçoivent l'approbation nécessaire à leur adoption.

Comme nous l'avons vu *supra*, certains fournisseurs d'accès américains ont pris l'initiative de mettre en place un mécanisme de réponse graduée pour lutter contre le téléchargement illégal d'œuvres sur internet, en collaboration avec les ayants droit.

---

[147] Sec. 3, (c) et (d) de la proposition de loi PIPA.
[148] Sec. 5 de la proposition de loi PIPA.
[149] Julien L. « Les lois SOPA et PIPA contre le piratage sont reportées », *Numerama*, 21 janvier 2012, disponible sur http://www.numerama.com/magazine/21356-les-lois-sopa-et-pipa-contre-le-piratage-sont-reportees.html
[150] J. PEPITONE, « SOPA and PIPA postponed indefinitely after protests », *CNN*, 20 janvier 2012, disponible sur http://money.cnn.com/2012/01/20/technology/SOPA_PIPA_postponed/index.htm
[151] http://americancensorship.org/#quotes

2. L'Irlande

Après le rejet de son mécanisme de réponse graduée mis en place volontairement par un fournisseur d'accès à internet[152] par la Commission vie privée irlandaise, il y a eu une volonté en Irlande de mettre en place un système de blocage de sites internet[153]. En effet, le Gouvernement irlandais a décidé de lancer une nouvelle proposition de loi dans le courant de l'année 2012 pour aider les ayants droit à combattre la pratique du téléchargement et du partage illicite en ligne, plus particulièrement en introduisant un système qui autorisera les industries de contenus à forcer les fournisseurs d'accès de bloquer les sites internet dont le but premier est la violation du droit d'auteur[154]. Cette proposition du Gouvernement vient en réponse à la menace d'EMI d'intenter une action judiciaire contre le Gouvernement s'il ne prenait aucune mesure de lutte contre le téléchargement illégal[155]. Les quatre maisons de disques irlandaises se sont associées à un procès qui a pour but de forcer les ministres à prendre de telles mesures, sur le fondement que l'Irlande n'a pas rempli ses obligations européennes obligeant à protéger les droits d'auteur en ligne[156]. Selon un site spécialisé, il y aurait de fortes chances que la proposition du gouvernement soit basée sur le système espagnol de la loi *Sinde*, mettant en place un mécanisme très rapide d'injonctions à l'encontre des fournisseurs d'accès à internet en vue de bloquer les sites violant le droit d'auteur[157].

3. L'Italie

En Italie, le législateur a déjà opté pour des mesures sévères contre le piratage en ligne avec le décret Urbani, n°128 du 21 mai 2004 relative à la lutte contre le piratage en ligne d'œuvres audiovisuelles. Cette loi prévoit que les échanges illégaux d'œuvres sur Internet, par le biais du *peer-to-peer*, sont passibles de sanctions pénales et administratives qui vont d'une amende de 15.493 € à un emprisonnement de 4 ans en cas d'échange de films ou de musiques[158]. Le décret s'applique aux réseaux *peer-to-peer* et aux publications sur les sites de téléchargement direct – de type Megaupload ou Rapidshare[159].

Avant elle, la loi n°248 du 18 août 2000, la « loi anti-piraterie », entrée en vigueur le 19 septembre 2000, et qui transpose la directive 91/250/CEE du 14 mai 2001 concernant la protection des programmes d'ordinateur, instaure le principe de l'interdiction de copie privée en matière de logiciel et prévoit de sévères condamnations pénales à l'encontre des personnes qui enfreindraient cette interdiction. Cette loi instaure en outre d'autres mécanismes concernant la copie privée, mais aussi

---

[152] Voir *infra.*

[153] ENIGMAX, « File-sharing 3 strikes killed in Ireland, Government promises site blocking », *TorrentFreak*, 19 décembre 2011, disponible sur http://torrentfreak.com/file-sharing-3-strikes-killed-in-ireland-government-promises-site-blocking-111219/

[154] B. O'HALLORAN, « Illegal downloading to be curbed by Government order », *Irish Times*, 19 décembre 2011, disponible sur http://www.irishtimes.com/newspaper/frontpage/2011/1219/1224309259318.html

[155] ENIGMAX, « File-sharing 3 strikes killed in Ireland (…) », *op. cit.*

[156] « Record industry sues Ireland », *CMU*, 13 janvier 2012, disponible sur http://www.thecmuwebsite .com/article/record-industry-sues-ireland/

[157] *Ibidem.*

[158] « Propriété Intellectuelle et lutte anti-contrefaçon », Revue du Réseau Propriété Intellectuelle et Lutte anti-contrefaçon, n°19, Décembre 2009, p. 3, disponible en ligne sur : http://www.inpi.fr/fileadmin/mediatheque /images/parutions/RevuePIetContrefacon.pdf.

[159] *Media Consulting Group*, « Le 'forfait sur le contenu' : une solution au partage illégal de fichiers ? », *op. cit.*, p. 60.

la défense des droits d'auteur avec la création d'un comité (*« Comitato per la tutela della proprieta intellettuale »*)[160].

Le 6 juillet 2011, l'*Autorità per le garanzie nelle comunicazioni* – Autorité de régulation des communications (AGCOM) – a adopté un projet de réglementation sur la protection du droit d'auteur en ligne[161]. Ce projet est basé sur l'étude que le Gouvernement italien a commandée à l'AGCOM, intitulée *Consultazione publica sullo schema di regolamento in materia di tutela del diritto d'autore sulle reti di communicazione electronica*. Par cette réglementation, l'AGCOM pourrait imposer aux fournisseurs d'accès le blocage, sur simple décision administrative, de l'accès à tout site italien impliqué dans des violations du droit d'auteur ou facilitant ces violations[162]. Ces sites feraient uniquement l'objet d'une procédure de *notice and takedown*. Ce projet de réglementation établit une procédure alternative qui intervient lors d'une demande de suppression d'un contenu en ligne protégé par le droit d'auteur. Cette procédure ne se substituerait pas à la procédure judiciaire et prendrait fin dès que l'une ou l'autre des parties exerce un recours.[163] Cette procédure de *notice and take down* aurait lieu dans un premier temps entre l'ayant droit et le fournisseur d'accès à internet, qui pourront se rendre devant l'AGCOM si la mesure de *notice* ne les satisfait pas. L'AGCOM aurait le pouvoir d'ordonner la suppression des contenus illégaux, avec une possible intervention du juge, la décision pouvant être contestée devant le tribunal administratif de Rome. Le projet de réglementation est en attente, d'une part suite à l'incompétence de l'AGCOM de légiférer en matière de droit d'auteur, et d'autre part de l'adaptation de la loi sur le droit d'auteur[164].

Relevons encore que le 30 novembre 2011, une proposition de loi a été présentée, proposition qui entend modifier les articles 16 et 17 du décret législatif 70 du 9 avril 2003[165]. Ces deux articles concernent respectivement la responsabilité des hébergeurs et l'absence d'une obligation générale de surveillance. L'article 16 de la proposition précise que la connaissance effective d'activités illicites pourra provenir d'informations fournies par les titulaires des droits violés par lesdites activités. L'article 17 de la proposition ne concerne quant à lui que la propriété industrielle et ne s'applique dès lors pas au droit d'auteur.

4. La Norvège

Comme nous l'avions vu *supra*, en plus d'un mécanisme d'envoi d'avertissements, la proposition de loi norvégienne prévoit également des mesures en matière de blocage de sites internet. La proposition laisse le choix au législateur entre deux alternatives.

---

[160] S. CARNEROLI, « La nouvelle loi italienne anti-piraterie », article *DNT* du 27 septembre 2000, disponible sur http://www.droit-technologie.org/actuality-343/la-nouvelle-loi-italienne-anti-piraterie.html ; cette loi est disponible en ligne sur : http://www.wipo.int/wipolex/fr/text.jsp?file_id=128285

[161] *Delibera* 668/2010 (décision 668/2010).

[162] *Media Consulting Group*, « Le 'forfait sur le contenu' : une solution au partage illégal de fichiers ? », *op. cit.*, p. 60.

[163] A. PERDIGAO, « Italie : Nouveau projet de réglementation sur le droit d'auteur en ligne », *Observatoire européen de l'audiovisuel*, 2011, disponible en ligne sur http://merlin.obs.coe.int/iris/2011/8/article34.fr.html

[164] E. ROSATI, « No online copyright regulation to be adopted in Italy (for now) », *The 1709 Blog*, 22 mars 2012, disponible sur http://the1709blog.blogspot.be/search?q=agcom.

[165] *Proposta di Legge*, *Camera dei Deputati,* 4549, disponible en ligne sur : http://ec.europa.eu/enterprise/tris/pisa/cfcontent.cfm?vFile=120110598IT.PDF

Suivant la première possibilité, à la requête d'un ayant droit, l'Autorité des médias pourrait ordonner à un fournisseur d'accès qui transfère, donne accès ou enregistre du contenu, d'empêcher l'accès à un site web qui porte atteinte dans une large mesure au droit d'auteur[166]. La décision de cette autorité pourra être contestée et être soumise à un Conseil des plaintes indépendant désigné par le Ministère. Toute personne ayant un intérêt, et donc même le Conseil norvégien des Consommateurs, peut porter cette décision devant le Conseil des plaintes. La décision du Conseil des plaintes peut à son tour être portée devant le tribunal, qui pourra rendre une décision sur le fond de l'affaire[167].

Suivant la seconde alternative, à la requête d'un ayant droit, c'est le tribunal qui pourrait ordonner à un fournisseur d'accès de bloquer un site web. Une telle requête doit être présentée au tribunal du lieu d'un des fournisseurs à la cause. Le propriétaire du site doit être déclaré comme partie adverse à l'action, ce qui n'est pas le cas dans la première alternative de la proposition de loi.

Remarquons que seuls les sites web dans lesquels le droit d'auteur fait de toute évidence l'objet d'une atteinte considérable peuvent être bloqués, ce qui démontre un fort contrôle de proportionnalité entre le problème et son traitement[168].

C. Le blocage de sites par la voie judiciaire

1. Belgique – L'article 87, §1er de la Loi sur le droit d'auteur

Le 26 septembre 2011, la Cour d'appel d'Anvers a condamné Belgacom et Telenet à bloquer l'accès au site *The Pirate Bay* pour leurs abonnés[169], dans une affaire opposant la *Belgian Anti-Piracy Federation* (BAF) aux deux fournisseurs d'accès à internet. En 2010 la BAF avait déjà tenté d'imposer le filtrage du site *The Pirate Bay* par une action en référé devant le tribunal de commerce d'Anvers, mais sans obtenir gain de cause, le tribunal estimant la demande de la BAF disproportionnée, les conditions du référé n'étant pas remplies par défaut d'urgence. En degré d'appel, il a finalement été donné raison à la BAF, les fournisseurs devant mettre en place un blocage DNS de onze adresses associées au site *The Pirate Bay*.

Peu de temps après cette première victoire, la BAF a exprimé la volonté d'étendre le filtrage de *The Pirate Bay* à toute la Belgique, et cela de manière volontariste. Elle a ainsi adressé un courrier à tous les fournisseurs les incitant à bloquer l'accès au site. Mais ne perdons pas de vue que depuis lors, la Cour de justice de l'Union européenne a rendu l'arrêt *Scarlet c. Sabam*[170] qui interdit l'obligation d'imposer aux intermédiaires techniques une surveillance généralisée des réseaux. Cet arrêt a été confirmé dernièrement par la Cour dans son arrêt *Sabam c. Netlog*[171]. Observons cependant que ces arrêts de la CJUE concernaient la conformité au droit communautaire d'injonctions de portée générale et non d'injonctions ciblées sur un site internet particulier utilisé comme média pour des activités illicites.

[166] Nouvel article 56c, al. 1 du *Copyright Act*.
[167] Nouvel article 56c, al. 6 du *Copyright Act*.
[168] Nouvel article 57c du *Copyright Act*.
[169] Antw. 26 septembre 2011, RABG n° 18/2011 du 15 novembre 2011, p. 1269.
[170] C.J.U.E. (3e ch.), 24 novembre 2011, Scarlet Extended SA c. SABAM, C-70/10, non encore publié au recueil.
[171] C.J.U.E. (3e ch.), 16 février 2012, SABAM c. Netlog, C-360/10, non encore publié au recueil.

2. *France – L'article L336-2 du Code de propriété intellectuelle*

En août 2011, trois syndicats du monde du cinéma et de la télévision français (SEVN, FDNF et l'APC) ont déposé une plainte visant à obtenir le blocage de quatre sites de streaming illégal (Allostreaming.com, Alloshowtv.com, Alloshare.com et Allomovies.com), tous dépendant du groupe Allo. La procédure vise à la fois les fournisseurs d'accès à internet et les quatre plus grands moteurs de recherche français (Google, Yahoo!, Orange et Bing). Les ayants droit demandent aux fournisseurs le blocage de ces sites, via un blocage de l'accès à leur nom de domaine, ainsi qu'à leur adresse IP et demandent aux moteurs de recherche de cesser de référencer ces sites.[172]

Pour obtenir ce blocage, l'argumentaire des ayants droit s'appuie sur un article né de la loi HADOPI : l'article L336-2 du Code de propriété intellectuelle, qui prévoit que « *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 (…) ou des organismes de défense professionnelle (…), 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.* »[173]

Cette mesure permet donc aux ayants droit de réclamer toute mesure à l'égard de toute personne pour faire cesser ou prévenir une atteinte à leurs intérêts. Cet article les autorise donc à réclamer à la fois le blocage et le déréférencement auprès des fournisseurs d'accès et des moteurs de recherche. Mais un simple blocage des quatre sites ne sera pas suffisant aux yeux des ayants droit, ceux-ci souhaitant également le blocage des éventuels sites miroirs, et ce dans un souci d'efficacité. Leur solution viserait alors à juger, identifier et qualifier les sites miroirs du groupe Allo pour en exiger le blocage par DNS par les intermédiaires techniques, et les blocages subséquents se feraient sans passer par le juge, qui n'interviendrait qu'en aval pour valider les futures opérations.[174]

3. *Autres cas de blocage (du site* The Pirate Bay*)*

Fin octobre 2011, un tribunal d'Helsinki a ordonné au fournisseur d'accès finlandais Elisa de bloquer l'accès pour ses abonnés au site *The Pirate Bay*, à la demande du CIAPC (Copyright Information and Anti-Piracy Center) et de la branche finlandaise de l'IFPI. Le fournisseur doit procéder à un blocage de noms de domaine liés à *Pirate Bay*[175], ainsi qu'au blocage des accès aux adresses IP utilisées par les serveurs du site, sous peine de devoir payer une amende de 100 000 euros.[176] Le fournisseur Elisa, bien qu'il ait fait appel de la décision, a procédé au blocage de *The Pirate Bay* le lundi 9 janvier 2012,

[172] M. REES, « HADOPI : avec TMG, déréférencement et blocage anticipatifs », article du 5 décembre 2011, disponible sur http://www.pcinpact.com/dossier/HADOPI-tmg-blocage-alpa-moteur/200-1.htm
[173] Article L336-1 du Code de Propriété Intellectuelle, disponible sur : http://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000020740348&cidTexte=LEGITEXT000006069414&dateTexte=20120128
[174] M. REES, « HADOPI : avec TMG, déréférencement et blocage anticipatifs », *op. cit.*
[175] Une trentaine environ, Voy. http://www.arcticstartup.com/2012/01/09/finnish-operator-required-to-block-access-to-thepiratebay-among-others
[176] ERNESTO, « Finnish ISPs ordered to block The Pirate Bay », *TorrentFreak*, 26 octobre 2011, disponible sur http://torrentfreak.com/finnish-isp-ordered-to-block-the-pirate-bay-111026/

à titre préventif, en attendant un jugement au fond[177]. Après sa victoire contre Elisa, l'IFPI veut étendre le dispositif de l'arrêt aux autres fournisseurs d'accès du pays – Sonera et DNA. Une injonction de blocage contre les deux fournisseurs a été demandée par l'IFPI fin novembre 2011.[178]

Au Danemark, une cour d'appel a confirmé en novembre 2011 une décision de première instance qui avait ordonné au fournisseur d'accès à Internet Tele2 de bloquer l'accès au site de partage de liens BitTorrent *The Pirate Bay*[179]. La décision de première instance, obtenue par l'industrie du disque à l'encontre du plus grand fournisseur d'accès à internet danois, de bloquer *The Pirate Bay* était une première mondiale[180].

En mars 2010, c'est au tour de l'Italie de bloquer un site miroir du site *The Pirate Bay*, blocage basé sur la décision de la Cour suprême italienne d'octobre 2009 ouvrant la voie au filtrage des sites BitTorrent, même si ces derniers ne sont pas hébergés en Italie ou administrés par des citoyens italiens[181].

En juillet 2011, la justice britannique a ordonné à *British Telecom* (BT), le plus grand fournisseur d'accès à internet du pays, qu'il bloque le site Newzbin.com, un site proposant des liens de téléchargement de contenus piratés[182]. C'est en se basant sur cette décision de justice que l'association *British Phonographic Industry* (BPI) – association de l'industrie du disque anglaise – a demandé à BT de bloquer volontairement l'accès au site *The Pirate Bay*, qui a répondu qu'il ne pourrait procéder à un tel blocage sans intervention d'une décision judiciaire dans ce sens[183]. Un premier obstacle a été levé le 20 février 2012, la Haute Cour de Londres ayant jugé[184] que les opérateurs et les utilisateurs du moteur de recherche BitTorrent violent les droits d'auteur des demandeurs[185]. Le juge a estimé que « les opérateurs de (*The Pirate Bay*) autorisent bien les actions de copie et de communication au public de ses utilisateurs qui portent atteinte (au droit d'auteur). Ils

[177] G. CHAMPEAU, « The Pirate Bay et l'EFF finlandaise censurés en Finlande », *Numerama*, 9 janvier 2012, disponible sur http://www.numerama.com/magazine/21208-the-pirate-bay-et-l-eff-finlandaise-censures-en-finlande.html

[178] ENIGMAX, « IFPI sues Pirate Bay admins in Finland, demands further ISP blocks », *TorrentFreak*, 26 novembre 2011, disponible sur http://torrentfreak.com/ifpi-sues-pirate-bay-admins-in-finland-demands-further-isp-blocks-111126/

[179] G. CHAMPEAU, « La justice confirme le blocage de The Pirate Bay au Danemark », *Numerama*, 27 novembre 2008, disponible sur http://www.numerama.com/magazine/11423-la-justice-confirme-le-blocage-de-the-pirate-bay-au-danemark.html

[180] G. CHAMPEAU, « The Pirate Bay bloqué par un FAI danois sous l'ordre de l'IFPI », *Numerama*, 6 février 2008, disponible sur http://www.numerama.com/magazine/6068-the-pirate-bay-bloque-par-un-fai-danois-sous-l-ordre-de-l-ifpi.html

[181] Julien L., « La Cour Suprême italienne ouvre la voie au blocage de The Pirate Bay », *Numerama*, 2 octobre 2009, disponible sur http://www.numerama.com/magazine/14134-la-cour-supreme-italienne-ouvre-la-voie-au-blocage-de-the-pirate-bay.html

[182] G. CHAMPEAU, « Le blocage de Newzbin ordonné en Grande-Bretagne », *Numerama*, 28 juillet 2011, disponible sur http://www.numerama.com/magazine/19438-le-blocage-de-newzbin-ordonne-en-grande-bretagne.html

[183] Julien L., « Le blocage de The Pirate Bay demandé en Grande-Bretagne », *Numerama*, 5 novembre 2011, disponible sur http://www.numerama.com/magazine/20455-le-blocage-de-the-pirate-bay-demande-en-grande-bretagne.html

[184] *Dramatico Entertainment Ltd & others v British Sky Broadcasting Ltd & others* [2012] EWHC 268 (Ch), disponible sur http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html

[185] « Pirate Bay 'a stronger case' of infringement than Newzbin », *The 1709 Blog*, 20 février 2012, disponible sur http://the1709blog.blogspot.com/2012/02/pirate-bay-stronger-case-of.html

vont bien au-delà du simple fait de permettre ou de faciliter » le piratage[186]. Les demandeurs pourront sur cette base poursuivre les fournisseurs d'accès pour qu'ils bloquent le site, comme cela a déjà été le cas en juillet 2011 envers Newzbin.

Aux Pays-Bas, l'organisation néerlandaise Stichting BREIN (Bescherming Rechten Entertainment Industrie Nederland) est très présente dans la lutte contre le piratage en ligne. Elle a récemment poursuivi les FAI ZIGGO et XS4ALL afin qu'ils bloquent l'accès de tous leurs abonnés au site internet suédois *The Pirate Bay*. Le 11 janvier 2012, une Cour du district de La Haye[187] a enjoint les deux FAI hollandais de bloquer dans les 10 jours 3 adresses IP et 24 noms de domaines qui conduisent vers *The Pirate Bay*, empêchant ainsi l'accès des internautes au site incriminé. Après un échec le 19 juillet 2010, la Cour estimant qu'un ordre général de blocage, envers tous les abonnés du fournisseur d'accès, même ceux qui ne portent pas atteinte aux droits des titulaires représentés par BREIN, n'est pas conforme à loi néerlandaise. La Cour a annoncé qu'en raison de la nature même du protocole BitTorrent, les utilisateurs ne font pas que télécharger des fichiers, ils *uploadent* également et par là violent le droit d'auteur – rappelons que c'est seulement l'*uploading qui* n'est pas autorisé aux Pays-Bas, le *downloading* l'étant.

4. La fermeture de Megaupload

Le 19 janvier 2012, le département de la Justice des Etats-Unis a fait fermer le site Megaupload, accusé d'avoir violé le droit d'auteur[188]. Cette fermeture s'inscrit dans une campagne plus large d'*anti-piracy* via *l'Operation In Our Sites v. 2.0* qui vise à fermer les sites commerciaux engagés dans la vente et la distribution illégales de biens contrefaits et d'œuvres protégées par le droit d'auteur[189].

[186] Paragraphe 81 du jugement du 20 février 2012.
[187] Gravenhage (civ.), 11 janvier 2012, *STICHTING BESCHERMING RECHTEN ENTERTAINMENT INDUSTRIE NEDERLAND (BREIN)* c. ZIGGO B.V. et XS4ALL B.V., 374634 / HA ZA 10-3184, www.rechtspraak.nl.
[188] « La justice américaine ferme le site de téléchargement Megaupload », *Le Monde*, 19 janvier 2012, disponible sur : http://www.lemonde.fr/technologies/article/2012/01/19/la-justice-americaine-ferme-le-site-de-telechargement-megaupload_1632197_651865.html.
[189] National Intellectual Property – Rights Coordination Center, Operation In Our Sites : http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

§2. La mise en place d'accords contractuels

En dehors des initiatives légales peuvent intervenir des initiatives « privées », qui émanent des acteurs eux-mêmes. C'est le cas de l'Irlande (I) qui a mis en place un système de réponse graduée dans un cadre privé, avec la collaboration d'un grand fournisseur d'accès à internet national. Contrairement à l'Irlande où l'accord est venu clore un litige opposant un fournisseur d'accès à l'industrie du disque, l'Australie (II) a cela de caractéristique que ce sont les cinq plus grands fournisseurs d'accès du pays qui se sont associés pour présenter une proposition commune en matière de lutte contre le piratage en ligne.

I. L'Irlande

En Irlande, la législation relative au droit d'auteur est consacrée dans le *Copyright and Related Act* de 2000[190]. Le mécanisme de réponse graduée mis en place n'est pas issu d'un projet de loi mais résulte d'accords contractuels entre un des plus importants fournisseurs d'accès irlandais, Eircom, et une société de gestion collective, l'*Irish Recorded Music Association* (IRMA), l'équivalent de la SABAM en Irlande[191].

C'est dans le cadre d'un règlement à l'amiable qui est venu clore un litige intenté par la société de gestion IRMA, que le fournisseur d'accès Eircom a accepté de mettre en place un système de réponse graduée à sa charge. Après l'envoi de deux lettres d'avertissement, le fournisseur d'accès s'est arrogé le droit de suspendre la connexion internet de l'usager, les ordres de suspension ne devant pas passer devant un juge pour accord. La société IRMA a bien évidemment essayé de faire pression sur les autres fournisseurs d'accès irlandais pour qu'ils adoptent à leur tour un tel mécanisme, mais sans succès. A ce titre, le 11 octobre 2010, la Haute Cour de Dublin[192] a jugé qu' « un fournisseur d'accès (en l'occurrence UPC Broadband) n'était pas obligé de participer à la *réponse graduée* en identifiant les internautes pour ensuite suspendre leur connexion en cas de téléchargement illégal et que la loi irlandaise ne comprenait aucune base juridique à un système de réponse graduée ».

Selon cet accord, sur base de preuves collectées par les ayants droit – eux-mêmes informés par des sociétés tierces, travaillant dans la détection d'échanges illégaux sur internet telles DetecNet – Eircom devra informer par téléphone ses utilisateurs que leur adresse IP a été identifiée comme étant utilisée en violation au droit d'auteur sur internet. L'on peut appeler cette phase la *detection warning*. Après un délai de 14 jours, sur base d'une deuxième atteinte détectée, Eircom enverra un second avertissement à l'utilisateur, par courrier ou courriel, en vertu duquel, à moins qu'il ne cesse ces atteintes au droit d'auteur, son compte utilisateur sera déconnecté – c'est la *second warning*. A

[190] *Copyright and Related Rights Act 2000*, Number 28 of 2000, disponible en ligne sur http://www.irishstatutebook .ie/2000/en/act /pub/0028/index.html

[191] Voy. « Three-strikes goes live in Ireland », *CMU*, 25 mai 2011, disponible sur http://www.thecmuwebsite.com/article/three-strikes-goes-live-in-ireland/ ; O. ROBILLART, « L'Irlande se met à la riposte graduée », *Clubic*, 25 mai 2010, disponible sur http://pro.clubic.com/legislation-loi-internet/HADOPI/actualite-342372-irlande-riposte-graduee.html

[192] High Court of Ireland, *EMI and others v. UPC*, [2009 No. 5472 P], disponible sur http://www.scribd.com/doc/39104491/EMI-v-UPC

défaut de se conformer à ce deuxième avertissement, la troisième phase – appelée *Termination warning* – sera enclenchée. Eircom devra alors revoir l'ensemble des preuves collectées à l'encontre de cet utilisateur et permettre à ce dernier de s'expliquer sur ces infractions à répétition. A cet égard, Eircom devra recevoir l'utilisateur et prendre en compte ses explications, sans qu'il n'y ait consultation des ayants droit. A défaut de faire valoir des circonstances atténuantes valables (par exemple le besoin de l'accès à internet pour des raisons médicales), une *termination notice* sera alors adressée à l'utilisateur, lui donnant 14 jours avant que son service internet ne soit bloqué.

En pratique, il est prévu que l'utilisateur ne pourra plus bénéficier de son accès internet pour une période de 7 jours, dans les cas où trois avertissements lui auront été adressés. Sa connexion pourra être suspendue pour un an si d'autres atteintes étaient encore identifiées par la suite.[193]

Ici, seuls les abonnés à Eircom sont sous le joug de la réponse graduée, il suffit donc à ceux-ci de changer de fournisseur d'accès pour ne pas risquer de voir leur connexion à internet suspendue. Cela crée une situation discriminatoire entre les abonnés à internet irlandais. Une autre critique qui peut être apportée à cet accord est que tous les pouvoirs sont donnés à Eircom qui décide seul de la coupure des accès à internet, sans aucun garde-fou judiciaire.

En juin 2011, la Commission irlandaise de protection des données a reçu une plainte d'un abonné qui avait reçu par erreur une lettre lui annonçant qu'il avait téléchargé illégalement. La Commission a alors relevé, après une enquête sur le système de réponse graduée d'Eircom, que ce dernier avait envoyé par erreur 300 lettres d'avertissement les accusant de partager de la musique[194]. Cela a entraîné une méfiance vis-à-vis de ce système, et en décembre 2011, la Commission a rendu une décision dans laquelle elle enjoint Eircom de cesser dans les 21 jours sa politique de réponse graduée[195]. La décision est fondée sur les prescrits de l'arrêt de la Cour de Justice de l'Union européenne du 24 novembre 2011 qui a jugé qu'une surveillance systématique des utilisateurs d'internet à la demande des ayants droit constitue une violation de leur vie privée[196].

Suite à cette obligation de mettre fin au système volontaire de réponse graduée, le Gouvernement irlandais a décidé de se pencher sur l'adoption d'une solution semblable à la loi *Sinde* espagnole, basée non plus sur les usagers mais sur les sites contrefaisants eux-mêmes[197].

Mais en juin 2012, les quatre géants de la musique – Universal, Sony, EMI et Warner – ont obtenu du juge Peter Charleton que la décision de la Commission vie privée irlandaise soit annulée. Selon eux, la décision de la Commission « désactivait » l'accord qu'ils avaient obtenu envers Eircom, et par cette ordonnance de justice, ils pourront continuer à appliquer le mécanisme de réponse graduée en Irlande. Le juge a en effet estimé que la manière dont la vie privée aurait pu être compromise par la détection et la répression des individus qui se livrent au partage illégal de fichiers sur Internet manquait de clarté.

---

[193] W. FRY, « Ireland confirms graduated response policy against illegal downloads », *William Fry*, 2010, disponible sur http://www.williamfry.ie/Libraries/Publications/Ireland-confirms-graduated-response-policy-against-illegal-downloads-1.sflb.ashx

[194] TJ MCINTYRE, « Data Protection Commissioner Investigating Eircom's 'three strikes' system », *TJ McIntyre*, 11 juin 2011, disponible sur http://www.tjmcintyre.com/2011/06/300-false-accusations-data-protection.html

[195] J. KENNEDY, « Eircom has 21 days to respond to halt 'three strikes' order by DPC », *Siliconrepublic*, 19 décembre 2011, disponible sur http://www.siliconrepublic.com/comms/item/25072-eircom-has-21-days-to/

[196] Point 51 de l'arrêt de la C.J.U.E. du 24 décembre 2011, Scarlet c. SABAM, *op. cit.*

[197] Voir *supra*.

II. L'Australie

Le 25 novembre 2011, les cinq plus importants fournisseurs d'accès à internet ont présenté une proposition détaillée pour faire face à la question du partage de fichiers illégaux[198]. Une proposition commune du *Communications Alliance* – le premier organe de l'industrie des télécommunications – et de fournisseurs d'accès[199], avec la collaboration de compagnies de télécoms[200] et de la *Internet Industry Association*, précise ce que les acteurs participants pensent être la meilleure solution pour traiter le problème. A ce titre, l'accord prévoit l'implémentation du système de l'envoi de lettres d'avertissements, mais contrairement au régime de la réponse graduée, il ne comprendrait pas la sanction de la coupure de l'accès à Internet. Au lieu de cela, les ayants droit devront retourner au système judiciaire pour punir les contrevenants persistants. [201]

Cette proposition, intitulée *A Scheme to Address Online Copyright Infringement*, met en avant le cadre pour un régime de notification qui visera à éduquer les abonnés à internet lorsque leurs connexions sont pointées comme se livrant à une infraction au droit d'auteur. La responsabilité de la surveillance des réseaux de partage de fichiers reposerait sur les ayants droit, qui ne pourraient utiliser que des systèmes de détection testés et approuvés[202]. Les avis de détection devront être envoyés aux fournisseurs d'accès à internet dans les 14 jours de l'enregistrement d'une infraction, et qui auront à leur tour 14 jours pour faire correspondre l'adresse IP fournie avec le compte d'un abonné et lui envoyer un avis d'infraction[203]. Les abonnés qui sont contactés à propos d'un premier avertissement de téléchargement illicite de fichiers devraient recevoir un *Education Notice* leur signalant qu'une infraction a eu lieu sur leur compte, mais sans mentionner le contenu du document qui a été partagé. L'avis devrait également inclure une information sur la manière d'obtenir du contenu légalement.[204] Après avoir reçu un *Education Notice*, suivrait alors une période de 12 mois, période durant laquelle si l'abonné est pris à nouveau, il recevra un *Copyright Infringement Notice*, ce dernier détaillant cette fois le contenu partagé en cause[205]. Lorsqu'un abonné a reçu un *Education Notice* et trois *Copyright Infringement Notice*, leur fournisseur d'accès leur enverrait un nouvel avis appelé *Discovery Notice*. Il y serait inscrit que le titulaire du compte a été insensible aux avis précédents, que les titulaires de droit ont été informés de ce fait, et que d'autres mesures pourraient suivre.[206] C'est à ce stade que les ayants droit auraient à décider s'ils souhaitent obtenir une ordonnance du tribunal pour obtenir l'identité du titulaire du compte afin de le poursuivre en vertu des lois existantes. A chaque étape, de l'*Education notice* au *Discovery Notice*, il est donné aux

[198] Australian Internet Service Provider Proposal : « A scheme to adress online Copyright Infringement », 25 novembre 2011, disponible en ligne sur http://www.commsalliance.com.au/__data/assets/pdf_file/0019/32293/Copyright-Industry-Scheme-Proposal-Final.pdf
[199] Telstra Bigpond, iiNet, Optus, iPrimus and Internode
[200] AAPT, Ericsson Australia
[201] ENIGMAX, «Aussie ISPs propose anti-file-sharing warning notice scheme », *TorrentFreak*, 25 novembre 2011, disponible sur http://torrentfreak.com/aussie-isps-propose-anti-filesharing-warning-notice-scheme-111125/
[202] Australian Internet Service Provider Proposal : « A scheme to address online Copyright Infringement », *op. cit.*, point 2, p. 4.
[203] *Ibidem*, point 3.3, p. 5.
[204] *Ibidem*, point 3.4, pp. 5 et 6.
[205] *Ibidem*, point 3.5, p. 6 et 7.
[206] *Ibidem*, point 3.6, pp. 7 et 8.

abonnés la possibilité de faire appel[207]. Les fournisseurs proposent ce mécanisme à l'essai pour 18 mois, et à l'issue de cette période d'essai il en sera fait une évaluation indépendante[208] qui définira si des changements devront être apportés à ce système.

Nous pouvons relever que les ayants droit ne sont pas partie à l'accord mais la déclaration du « Communication Alliance » signale que le mécanisme mis en place est le résultat de discussions qui se sont tenues en 2011 entre les fournisseurs d'accès, le gouvernement et les ayants droit[209].

Contrairement à leurs voisins Néo-Zélandais, ce n'est donc pas un mécanisme de réponse graduée intégral qui a été proposé par les fournisseurs d'accès pour traiter les contrevenants récidivistes, ce qui signifie qu'il n'y aura pas de suspension ou de coupure de l'accès à internet des abonnés. Au lieu de cela, serait mis en place un régime d'avertissements dont l'accent sera mis sur l'éducation des consommateurs.

Le 20 avril 2012, la Haute Cour australienne, dans le cadre d'un procès qui durait depuis plus de quatre ans, a confirmé que le fournisseur d'accès impliqué n'était pas responsable pour les infractions au droit d'auteur commises par ses abonnés[210].

[207] *Ibidem*, point 3.9, p. 9. Il sera créé un *Copyright Industry Panel* qui sera chargé de la procédure d'appel, ainsi que de l'information par la préparation des moyens de promotion des contenus légaux, de sécurisation des connexions, *etc.*

[208] Le rapport ne détermine pas qui exercera cette évaluation.

[209] ENIGMAX, «Aussie ISPs propose anti-file-sharing warning notice scheme », *op. cit.*

[210] Roadshow Films Pty Ltd & others v iiNet Ltd [2012] HCA 16 (20 April 2012)

§3. Les systèmes d'autorisation

Les solutions non punitives visent à autoriser les échanges et le téléchargement d'œuvres entre internautes à des fins non commerciales sur internet tout en redistribuant aux auteurs et autres titulaires de droits une rémunération appropriée. Certes, les auteurs peuvent autoriser les internautes à se livrer à de tels actes s'ils décident d'exercer leurs droits exclusifs. En effet, le principe en droit d'auteur est que l'auteur dispose de droits exclusifs sur ses œuvres. Toutefois, en raison de la masse d'œuvres et d'ayants droit susceptibles d'être concernés par de tels échanges ou téléchargements, l'autorisation sur base de l'exercice individuel des droits d'auteur et droits voisins est irréaliste et peu pratique pour l'utilisateur. Des propositions ont été faites dans le sens d'un recours à certains mécanismes du droit d'auteur afin de légitimer ces pratiques de manière globale. Il s'agit notamment de la licence non volontaire, de la gestion collective obligatoire et de la licence collective étendue.

I. La licence non volontaire

La licence non volontaire permet au public d'utiliser les œuvres protégées par le droit d'auteur en versant aux auteurs une contrepartie financière. Ce mécanisme retire à l'auteur son contrôle sur l'exploitation de ses œuvres. Ils ont simplement le droit de percevoir une rémunération[211]. Il y a donc transformation du droit exclusif en droit à rémunération : le fait de priver l'auteur de tous ses droits sur un type d'exploitation donné retire à son droit tout caractère exclusif. L'appellation de licence non volontaire désigne en réalité deux mécanismes : la licence légale et la licence obligatoire. La différence entre ces deux dispositifs réside dans le mode de fixation de la rémunération due en contrepartie. Dans l'hypothèse de la licence légale, le législateur a donné au pouvoir exécutif la mission de fixer la rémunération même si les parties intéressées sont consultées ; dans le cas d'une licence obligatoire, la rémunération doit être négociée entre les parties.

A. La Belgique

Dans leur proposition de loi visant à adapter la perception du droit d'auteur à l'évolution technologique tout en préservant le droit à la vie privée des usagers d'Internet, les écologistes ont opté pour la licence non volontaire[212]. Les objectifs consistent à sécuriser juridiquement les échanges d'œuvres sur Internet, financer les créateurs de contenus (auteurs, producteurs, éditeurs et interprètes) et créer une procédure de négociation entre les sociétés de gestion collective et les fournisseurs d'accès à Internet. Les rémunérations, perçues auprès des fournisseurs d'accès Internet,

[211] P. SIRINELLI, *Propriété littéraire et artistique*, Dalloz, Mémentos, Paris, 2ème éd., 2003, p. 68 : « une fois prise la décision de divulguer l'œuvre, l'auteur ne peut plus imposer sa volonté quant à l'étendue de la diffusion. Il peut seulement percevoir des revenus ».

[212] La qualification du système proposé par Ecolo en licence non volontaire n'est pas évidente car la proposition parle de négociation avec les ayants droit. Il s'agirait donc plus spécifiquement d'une licence obligatoire…

ne seraient pourtant pas répercutées sur les factures de connexion internet, jugées déjà trop élevées en Belgique. Pour garantir cette absence de surcoût pour les utilisateurs, la proposition de loi entend fixer légalement un prix maximum pour l'accès à Internet. Les rémunérations seraient en outre différentes selon le débit de la connexion. En cas de défaut d'accord sur les rémunérations, le Roi se verrait confier la charge de fixer les rémunérations. La proposition de loi suggère la création d'un Observatoire de l'Internet (mission supplémentaire pour l'Institut Belge des Services Postaux et de Télécommunications – IBPT) qui aurait pour mission d'établir une cartographie générale et anonyme de la réalité du téléchargement en Belgique sur la base d'enquêtes et de sondages. La clé de répartition des rémunérations des titulaires de droits serait ensuite décidée sur cette base.

B. L'Allemagne

Des discussions ont eu lieu dans certains partis politiques (Parti du Socialisme Démocratique, Parti Grune et Parti Linke) sur la mise en place d'une licence légale pour autoriser les échanges d'œuvres sur Internet et compenser financièrement les titulaires de droits[213]. Il s'agirait d'introduire un *Kulturflatrate*, une redevance culturelle forfaitaire et obligatoire sur les œuvres protégées par le droit d'auteur. Cette redevance consisterait en fait en une licence obligatoire, très proche de la licence globale, et qui aurait donc pour conséquence de réduire l'exercice du droit d'auteur à une simple demande de compensation[214]. Il s'agirait de prélever une somme – entre 5 et 10 euros – sur les abonnements à internet pour rémunérer par compensation les ayants droit des contenus digitaux (musique, film, livre, journal, image)[215]. En contrepartie, l'utilisation sur internet de tous ces contenus protégés par le droit d'auteur serait rendue légale.

II. La gestion collective obligatoire

La gestion collective obligatoire d'un droit exclusif est un mécanisme par lequel est retiré à l'auteur l'exercice individuel de son droit exclusif pour le confier à une société de gestion collective. L'auteur ne peut donc plus contrôler lui-même l'exploitation de ses œuvres dans le cadre fixé par le système puisqu'un exercice collectif par une société de gestion lui a été imposé. Toutefois et contrairement à un mécanisme de licence non volontaire, les sociétés de gestion conservent un pouvoir de négociation des conditions de licence avec les utilisateurs (conditions d'utilisation, tarifs). Elles ont ensuite la mission de collecter puis de répartir entre les ayants droit les rémunérations perçues pour l'utilisation des œuvres concernées par le dispositif.

---

[213] J. TWEER, « La plateforme Flattr : financement volontaire d'un produit gratuity, symbole du passé », *La Gazette de Berlin*, 2010, n° 35, disponible sur : http://www.lagazettedeberlin.de/6392.html

[214] V. DELFORGE, *op. cit.*, p. 25.

[215] Voy. Etude sur la licence globale « medialab » de Sciences-Po en France, « La licence globale : Projets de licence globale dans le monde », disponible sur : http://medialab.sciences-po.fr/controversies/2011/ecole_com/licence_globale/files/6013/0563/6764/carte monde2.swf

En 2005, en France, des sociétés de gestion collective, l'ADAMI et la SPEDIDAM – rejointes par des sociétés de consommateurs comme UFC Que Choisir ou l'UNAF – ont créé l'Alliance Public Artistes dont l'objectif est de proposer un système de licence globale pour liciter les échanges d'œuvres à des fins non commerciales sur les réseaux *peer-to-peer*[216]. Sous l'appellation de la licence globale, c'est en fait d'une gestion collective obligatoire dont il s'agit. L'objectif, comme indiqué sur le site internet de l'Alliance, est d'une part de « placer dans un cadre légal les millions d'internautes (…) qui partagent de la musique, des œuvres audiovisuelles, des images et des photographies en ligne », et d'autre part « de prévoir un mode de rémunération » pour les titulaires de droits. L'Alliance Public Artistes traite différemment le *download* alors envisagé en termes de copie privée et l'*upload* soumis à un régime de gestion collective obligatoire *via* le droit de mise à disposition du public. Les rémunérations seraient prélevées sur les factures de connexion internet des usagers – qui choisiraient de souscrire au système – puis reversées par les fournisseurs d'accès à internet aux sociétés de gestion collective les redistribuant ensuite aux ayants droit.

La gestion collective obligatoire de droits exclusifs a également été avancée comme un moyen de développer les offres légales d'œuvres sur Internet. En Belgique, la proposition de loi déposée par le Sénateur MR Richard Miller va dans ce sens en proposant dans son article 8, l'imposition de la gestion collective obligatoire à l'égard des « opérateurs de base de données », expression qui pourrait viser les sites de vente en ligne. En France, un rapport a été remis en janvier 2010 au Ministre de la Culture et de la Communication par MM. Patrick Zelnik, Jacques Toubon et Guillaume Cerutti[217]. Le rapport préconise – entre autres – le recours aux mécanismes de gestion collective pour les droits d'auteur et les droits voisins pour les services de mise à disposition en ligne des œuvres musicales. L'ensemble des professionnels du secteur est vivement encouragé à opter pour un système de gestion collective volontaire. Si, dans le délai d'une année, ces acteurs n'arrivaient pas à parvenir à des accords, le rapport recommande au législateur d'imposer le recours à la gestion collective des droits exclusifs. Dans un premier temps, la gestion collective serait volontaire ; et dans un second, en cas d'échec, elle serait rendue obligatoire. Ce dispositif serait expérimenté pour une durée de 3 ans ; il serait accompagné de mesures d'encouragement de la diversité culturelle sur internet[218]. Suite à ce rapport, Emmanuel Hoog a été chargé d'une mission de médiation sur la gestion des droits de la musique en ligne. Le 19 décembre 2010, le rapport de la mission conclut à l'impossibilité d'instaurer une gestion collective, volontaire ou obligatoire, des droits voisins pour la diffusion de la musique en ligne, telle que proposée par le rapport de MM. Zelnik, Toubon et Cerutti[219]. Seule une gestion collective des droits voisins pour ce qui concerne l'écoute linéaire en

[216] Le site internet se trouve à l'adresse suivante : www.lalliance.org. - Se reporter au Rapport du CSPLA, *La distribution des contenus numériques en ligne*, *op. cit*., spéc. pp. 62-73. Voir également le *Rapport n° 308 relatif au droit d'auteur et aux droits voisins dans la société de l'information*, fait au nom de la Commission des Affaires Culturelles sur le projet de loi, adopté par l'Assemblée Nationale, après déclaration d'urgence, par M. Thiolliere, pour le Sénat, 12 avr. 2006, 370 p., spéc. pp. 44-45.

[217] Rapport remis au Ministre de la Culture et de la Communication par MM. Patrick Zelnik, Jacques Toubon et Guillaume Cerutti, janvier 2010, disponible sur http://www.culture.gouv.fr/mcc/Actualites/A-la-une/Remise-du-rapport-de-la-mission-creation-et-internet.

[218] Sur tous ces points, voir le Rapport Zelnik (*op. cit*.), pp. 5-6.

[219] Rapport de la mission Hoog, 10/12/2010, disponible sur le site du Ministère de la Culture français (www.culture.gouv.fr).

ligne (webcasting et webcasting semi-interactif) sera mise en place. C'est l'objet de l'engagement n°13 de la mission Hoog[220].

III. La licence collective étendue

Le mécanisme de la licence collective étendue est propre aux pays nordiques (Danemark, Finlande, Islande, Norvège, Suède). Dans un premier temps, ce système se caractérise par le transfert volontaire, par les titulaires de droits, de leurs droits à une société de gestion collective pour l'utilisation de leurs œuvres. Le fondement du mécanisme consiste en l'adhésion volontaire des titulaires de droits. Les sociétés de gestion concluent alors avec des utilisateurs des contrats collectifs. Ce n'est que dans un second temps que ces licences sont élargies, par le législateur, à tous les titulaires d'une certaine catégorie d'œuvres. La licence collective devient alors étendue. Le répertoire de la société de gestion collective s'étendra aux ayants droit qui n'en sont pas membres. La seule condition à remplir est la suivante : la société de gestion doit représenter un nombre considérable d'ayants droit dans une catégorie d'œuvres donnée, ce qui atteste de sa légitimité.

Une hypothèse de licence collective étendue générale, introduite dans la loi danoise sur le droit d'auteur en 2008, concerne les « autres formes d'utilisation » dans certains domaines spécifiques couverts par un accord conclu entre une société de gestion représentant un nombre significatif de titulaires de droits, et les utilisateurs[221]. La singularité de cette disposition est qu'elle ne vise aucun type d'utilisation des œuvres en particulier. Par conséquent, tous les domaines du droit d'auteur sujets à licence qui impliquent un nombre significatif de titulaires de droits sont susceptibles de bénéficier du mécanisme de licence collective étendue[222].

Cette nouvelle disposition danoise pourrait éventuellement permettre d'appliquer à l'avenir le mécanisme de la licence collective étendue aux échanges d'œuvres sur les réseaux *peer-to-peer*, si les ayants droit, représentés par les sociétés de gestion collective, donnent leur accord pour ces échanges *peer-to-peer.* Il faudrait que les échanges d'œuvres à des fins non commerciales entre internautes sur les réseaux *peer-to-peer* puissent constituer un domaine spécifique et que les utilisateurs qui souhaitent bénéficier d'une extension de la licence concluent dans un premier temps un contrat collectif avec une société de gestion représentant un nombre substantiel de titulaires de droits dans le type d'œuvres en question. Dans un second temps, ce contrat pourrait être étendu à tous les titulaires de droits de la catégorie d'œuvres en question, à condition que la société de gestion représente un nombre substantiel de titulaires de droits. Le mécanisme devra prévoir que les auteurs qui ne souhaitent pas voir leurs œuvres utilisées dans ce contexte auront le droit de s'en

[220] Rapport HOOG, *op. cit.*

[221] Art. 50 (2) du *DCA* : "Extended collective license may also be invoked by users who, within a specified field, have made an agreement on the exploitation of works with an organisation comprising a substantial number of authors of a certain type of works which are used in Denmark within the specified field. However, this does not apply, if the author has issued a prohibition against use of his work in relation to any of the contracting parties".

[222] Th. RIIS et J. SCHOVSBO, « Extended Collective Licenses and the Nordic Experience - It's a Hybrid but is It a Volvo or a Lemon? », *Columbia Journal of Law and the Arts*, Vol. 33, Issue IV, 12 janvier 2010, disponible sur SSRN: http://ssrn.com/abstract=1535230, p. 6.

extraire grâce à l'option d'*opt-out* qui leur est donnée. Cela suppose donc que les échanges d'œuvres audiovisuelles et multimédia à des fins non commerciales entre internautes sur les réseaux *peer-to-peer* puissent constituer un domaine spécifique, et que les utilisateurs qui revendiqueraient une extension des effets du contrat collectif aient déjà signé avec les sociétés de gestion compétentes un accord leur permettant d'utiliser déjà les œuvres des titulaires de droits qui en sont membres dans ce cadre. Quels pourraient être ces utilisateurs ? Les représentants des consommateurs, les fournisseurs d'accès à internet, les fournisseurs de logiciels, les fournisseurs de contenus ? A l'avenir, il semble donc possible que la nouvelle disposition danoise puisse s'appliquer aux échanges d'œuvres audiovisuelles et multimédia sur les réseaux *peer-to-peer*, pour autant que les sociétés de gestion existantes aient autorisé contractuellement un tel échange de leur répertoire. Aucune proposition n'a toutefois été faite en ce sens.

§4. Décision d'inaction

Certains Etats, tels que les Pays-Bas (I), de manière non officielle, et la Suisse (II) plus officiellement, ont décidé de laisser faire le marché, le laisser s'autoréguler, les solutions approchées dans les autres Etats étant selon eux toutes critiquables.

I. Les Pays-Bas

Aux Pays-Bas, le téléchargement – *downloading* – n'est pas interdit, seul l'*uploading* est une violation du droit d'auteur selon la loi hollandaise. Il est de jurisprudence constante[223] que sous la loi néerlandaise, le téléchargement à partir de sources illégales, mais pour un usage privé est licite. Mais ces jugements ne créent pas une immunité pour les parties qui facilitent les atteintes au droit d'auteur, nous pensons à ceux qui téléchargent des œuvres ayant une source illicite sur des réseaux de partage P2P, le propre de ce système étant qu'après, le « téléchargeur » devient à son tour fournisseur de contenu, « uploader ». Il y a eu dernièrement une proposition d'interdire également le *downloading* s'il émane d'une source illégale, pour un usage privé. Mais le 23 décembre 2011, cette proposition a été rejetée par le Parlement hollandais[224].

Il n'y a à l'heure actuelle aucune proposition officielle pour lutter contre le piratage en ligne aux Pays-Bas. En 2009, les ministères néerlandais de l'éducation, de la culture et des sciences, des affaires économiques et de la justice ont commandé une étude sur les effets du partage de fichiers en ligne[225]. Les conclusions de cette étude se sont révélées fort perturbantes pour toutes les parties au débat, que ce soient ceux qui accusent le partage de fichier de détruire la culture ou ceux qui l'exonèrent de toute responsabilité dans le déclin des industries culturelles : «Ces recherches indiquent que les conséquences économiques du partage de fichiers pour la prospérité des Pays-Bas sont très positives à court terme comme à long terme. Le partage de fichiers permet aux consommateurs d'accéder à un large éventail de produits culturels, ce qui est typiquement propice au bien-être. Inversement, on pense que cette pratique provoque un recul des ventes de CD, de DVD et de jeux»[226]. Ce rapport a été fort controversé car il va dans le sens d'une non-action des autorités au profit d'une autorégulation par le marché lui-même.

---

[223] Cour d'appel de La Haye, ACI ADAM BV and Others v. Stichting de Thuiskopie and Others, 15 novembre 2010, n°200.018.226/01 ; Cour d'appel de La Haye, FTD v. Eyeworks, 15 novembre 2010 ; Rb. 's Gravenhage, 10 mai 2012, KG ZA 12-156, disponible sur : http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BW5387.

[224] ERNESTO, « Dutch Parliament : Downloading movies and music will stay legal », *TorrentFreak*, 24 décembre 2011, disponible sur : http://torrentfreak.com/dutch-parliament-downloading-movies-and-music-will-stay-legal-111 224/

[225] A. HUYGEN, N. HELBERGER *et al.*, « Ups and downs, Economic and cultural effects of file sharing on music, film and games », 18 février 2009, disponible en ligne sur http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorised_translation.pdf

[226] *Media Consulting Group*, « Le 'forfait sur le contenu' : une solution au partage illégal de fichiers ? », *op. cit.*, p. 52.

II. La Suisse

Le cadre juridique suisse du droit d'auteur et de l'utilisation d'offres illégales est semblable au cadre hollandais. En effet, en Suisse également, le téléchargement d'œuvres pour un usage privé est autorisé, sans que ne se pose la question de savoir si la source est légale ou illégale. C'est l'acte de mise à disposition de l'œuvre sur internet qui est punissable s'il n'est pas fait avec l'accord du titulaire du droit. Mais notons qu'un bon nombre d'utilisateurs des réseaux *peer-to-peer* n'ont pas conscience qu'eux aussi mettent à disposition des œuvres sur Internet[227], acte punissable au regard de la loi suisse sur le droit d'auteur.

Le Conseil des Etats suisse s'est posé la question de savoir ce qu'il était possible de faire pour remédier au téléchargement illégal d'œuvres. Dans ce cadre, le 19 mars 2010, il a chargé le Conseil fédéral de rédiger un rapport[228] faisant le point sur la question et d'examiner l'utilité de prendre des mesures contre les violations du droit d'auteur.

Le Conseil fédéral[229] a estimé que le cadre légal actuel suffisait et juge inutile une adaptation législative. La Suisse a décidé de ne pas se tourner vers un système de type HADOPI pour régler la situation du téléchargement illégal.

Dans son communiqué de presse, le Conseil fédéral a tenu les propos suivants : «*Internet a profondément modifié notre façon de consommer de la musique, des films et des jeux informatiques. Ces nouvelles habitudes ne devraient toutefois pas avoir de conséquences négatives sur la création culturelle. Le cadre juridique actuel permet de répondre de manière adéquate au problème des utilisations illicites d'œuvres. Il n'y a donc pas lieu de prendre des mesures législatives* »[230].

Concernant le comportement des utilisateurs suisses, le rapport relève qu'un tiers des jeunes de plus de 15 ans a téléchargé gratuitement de la musique, des films et/ou des jeux[231]. Se basant sur l'étude néerlandaise, le rapport suisse constate que ceux qui pratiquent le téléchargement illégal en ligne « continuent d'investir dans le secteur du divertissement les économies qu'ils réalisent en téléchargeant des contenus sur Internet, mais au lieu d'acheter des CD et des DVD, ils s'offrent des billets de concert et de cinéma et des produits de merchandising », et rajoute que « les craintes de voir cette évolution avoir un impact négatif sur la création culturelle suisse sont infondées ».[232]

Mais concrètement, le Conseil constate, avec bon nombre de chiffres à l'appui, qu'il est impossible de dégager un bilan clair sur l'impact de la mise en circulation illicite d'œuvres sur internet : « Alors que certains ayants droit imputent les pertes considérables qu'ils essuient à l'évolution des technologies, d'autres affirment que, dans leur secteur, les ventes sont restées stables depuis des

[227] Rapport du Conseil fédéral sur les utilisations illicites d'œuvres sur internet en réponse au postulat 10.3263 Savary, disponible en ligne sur : http://www.ejpd.admin.ch/content/dam/data/pressemitteilung/2011/2011-11-30/ber-br-f.pdf, p. 8.
[228] *Ibidem*.
[229] Communiqué du 30 novembre 2011 du Conseil fédéral suisse, « Violations de droits d'auteur sur Internet : le cadre juridique actuel est suffisant », disponible en ligne sur : http://www.ejpd.admin.ch/content/ejpd/fr/home/dokumentation/mi/2011/2011-11-30.html
[230] Rapport du Conseil fédéral sur les utilisations illicites d'œuvres sur internet (…), *op. cit.*, p. 7.
[231] Communiqué du 30 novembre 2011 du Conseil fédéral suisse, « Violations de droits d'auteur sur Internet : le cadre juridique actuel est suffisant », *op. cit.* et Rapport du Conseil fédéral, *op. cit.*, pp. 8 et 9.
[232] Communiqué du 30 novembre 2011 du Conseil fédéral suisse, « Violations de droits d'auteur sur Internet : le cadre juridique actuel est suffisant », *op. cit.*

années. Les études existantes ne permettent pas, elles non plus, de tirer des conclusions univoques. Une évidence s'impose toutefois : le marché se trouve à un tournant»[233].

Dans son point consacré aux actions envisageable, il constate que le nombre d'acteurs d'infractions est tellement élevé qu'il est impossible d'agir contre chacun d'entre eux dans la perspective d'une défense efficace des droits exclusifs, avec en plus des réserves liées à la protection des données. Lors de la révision du droit d'auteur qui a eu lieu le 1er juillet 2008, le législateur suisse a explicitement renoncé à interdire l'utilisation d'offres illégales, ce qui implique que « cette utilisation tombe sous le coup de l'art. 19 LDA qui régit la restriction aux droits d'auteur en faveur de l'usage privé » et qu'il n'est « pas indiqué de revenir sur la décision du législateur pour remédier au problème ». L'idée de mettre en place un système de type réponse graduée soulève des réserves de même ordre, ainsi que des questions sur sa compatibilité avec certains engagements internationaux de la Suisse[234]. Il rejette également le recours aux fournisseurs d'accès à internet pour verrouiller internet, car cette option « suscite des réserves comparables à celles formulées à l'égard de la réponse graduée ».[235] En fait, toute mesure répressive est écartée par le Conseil[236], qui se penche finalement sur la possible instauration d'une licence légale pour la mise à disposition d'œuvres sur Internet à des fins non commerciales tout en l'assortissant d'un droit à rémunération, sous la forme d'un forfait. Mais cette solution passe aussi à la trappe, l'autorisation générale de la diffusion des œuvres sur internet ne devant pas être l'œuvre du législateur mais plutôt émaner de la liberté contractuelle des ayants droit.[237]

Le Conseil fédéral conclut qu'une action du législateur ne semble pas s'imposer dans l'immédiat. Il « est d'avis que le cadre juridique tracé par le législateur suisse lors de la révision partielle du droit d'auteur entrée en vigueur en 2008 offre pour l'heure une marge de manœuvre suffisante pour parer aux utilisations d'œuvres dans l'environnement numérique. Il serait dès lors prématuré de légiférer. Il importe de donner au marché la possibilité de s'autoréguler afin d'éviter le maintien artificiel de structures dépassées »[238].

[233] Rapport du Conseil fédéral sur les utilisations illicites d'œuvres sur internet (…), *op. cit.*, p. 2.
[234] Il est fait référence ici rappel du rapport du Conseil des droits de l'homme de l'ONU selon lequel « le verrouillage d'Internet est considéré comme une violation de l'art. 19, al. 3, du Pacte international relatif aux droits civils et politiques ».
[235] Rapport du Conseil fédéral sur les utilisations illicites d'œuvres sur internet (…), *op. cit.*, pp. 10 et 11.
[236] « Eu égard à l'ampleur de la violation des droits et compte tenu de la modestie des moyens dont disposent les autorités de poursuites pénales, l'action répressive aura tôt fait d'atteindre ses limites ».
[237] Rapport du Conseil fédéral sur les utilisations illicites d'œuvres sur internet (…), *op. cit.*, pp. 11 et 12.
[238] Rapport du Conseil fédéral sur les utilisations illicites d'œuvres sur internet (…), *op. cit.*, p. 3.

Chapitre 2. Etude du cadre légal de la lutte contre les atteintes au droit d'auteur sur Internet

Section 1. Les questions de droit d'auteur

Les solutions proposées (notamment la licence globale) est-elle compatible avec le principe du **droit exclusif** des auteurs et titulaires de droits voisins, ce qui inclut la compatibilité avec le **test des trois étapes**), le principe de l'interdiction des formalités ou la notion de **rémunération équitable** applicable aux licences non-volontaires ?

Les actes de téléchargement d'œuvres sur Internet sont-ils couverts par l'exception de copie privée (ou d'autres exceptions telle la reproduction provisoire) et dans l'affirmative, celle-ci empêche-t-elle la mise en place de certaines exceptions ? Comment juger de l'éventuelle légitimité d'un acte de téléchargement ou de mise à disposition d'une œuvre protégée par Internet dans les procédures de blocage de sites web prétendument contrefaisants ou de réponse graduée ?

En cas de streaming, le droit d'auteur s'applique-t-il aux actes techniques accomplis lors de la réception du contenu par l'internaute (visualisation, audition) ?

§1. Qualification des actes de mise à disposition ou d'accès aux œuvres

I. La mise à disposition d'œuvres (*upload*)

Que ce soit dans des réseaux *peer-to-peer*, sur des sites web en téléchargement ou en streaming, la mise à disposition d'œuvres protégées par le droit d'auteur, musiques, films, livres numériques ou logiciels, relève du droit exclusif de l'auteur et, à ce titre requiert l'autorisation préalable de celui-ci[239]. Il ne fait pas de doute que l'*upload* de musiques, films ou autres œuvres protégées par l'intermédiaire de logiciels *peer-to-peer* ou encore sur des plateformes de téléchargement direct donne prise au droit d'auteur, car il s'agit d'un acte de mise à la disposition du public d'œuvres protégées, que seuls les titulaires de droit d'auteur ont le droit d'autoriser en vertu de l'article 1 de la loi sur le droit d'auteur[240]. La jurisprudence a systématiquement condamné de tels actes dans des réseaux *peer-to-peer*, les qualifiant d'actes de mise à disposition du public[241]. Peu importe que

[239] Voir A. STROWEL (ed.), *Peer-to-Peer File Sharing and Secondary Liability in Copyright Law*, Edgar Elgar, 2009.
[240] Ce même droit est reconnu aux différents titulaires de droit voisins.
[241] Voir aux Etats-Unis, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) ; en France, une série de décisions et notamment Cour d'appel Paris, 13ème ch., 27 avril 2007, http://www.legalis.net/jurisprudence-decision.php3?id_article=1954.

l'échange des œuvres se fasse dans un but non lucratif et non commercial, ce critère étant sans pertinence en droit d'auteur.

S'y ajoutent les reproductions nécessitées par cet acte de mise à disposition, telles que les numérisations ou copies des œuvres sur les serveurs et équipements qui offrent ce contenu protégé. Ces reproductions, ancillaires et préalables à l'acte de mise à disposition, requièrent également l'autorisation des ayants droit.

La même analyse vaut pour la diffusion sur les réseaux sociaux d'œuvres protégées, ces derniers espaces ne pouvant en principe relever du cercle de famille. De manière similaire, le stockage d'œuvres dans le *cloud*, couplée à l'organisation d'un accès du public à celui-ci, que ce soit par mot de passe ou non, est une mise à disposition du public.

Même si les internautes échangeurs d'œuvres dans les réseaux *peer-to-peer* n'ont pas été massivement poursuivis devant les juridictions belges, une décision de la Cour d'appel d'Anvers a considéré que ces échanges et téléchargements sans aucune autorisation des ayants droit portaient atteinte au droit de reproduction et au droit de communication au public[242].

La situation d'une liste d'hyperliens pointant vers des contenus illicitement mis à disposition sur Internet est plus délicate. Dans une décision anversoise déjà ancienne, l'auteur d'un site internet comprenant des centaines d'hyperliens vers des musiques mises à disposition sur Internet sans autorisation a été condamné pour complicité à un acte de contrefaçon[243]. Les responsables du site *The Pirate Bay* ont également été condamnés en Suède pour complicité à des atteintes au droit d'auteur en raison de la fourniture d'une base de données liée à un catalogue de fichiers *torrent* disponibles.

Que les hyperliens constituent directement un acte de mise à disposition du public est en revanche plus controversé[244].

II. Le téléchargement d'œuvres (*download*)

Le statut légal des actes par lesquels les internautes accèdent aux œuvres ainsi mises à disposition suscite davantage d'interrogations[245]. Lorsqu'une personne télécharge un contenu protégé mis à

[242] Anvers, 26 septembre 2011, *R.A.B.G.*, 2011, p. 1269.

[243] Civ. Anvers (réf.), 21 déc. 1999 (I.F.P.I. c. Beckers), *A&M*, 2000, p. 296. Voir en sens contraire, Provincial Court Madrid, sec.2 (Audiencia Provincial Madrid), 11 Septembre 2008, *Sharemula* (considérant qu'il ne s'agit pas d'une infraction pénale).

[244] A. STROWEL, « Liaisons dangereuses et bonnes relations sur l'Internet. A propos des hyperliens », *A&M* 1998/4, p.296 ; S. DUSOLLIER, «Les outils de référence: les nouvelles cartes au trésor de la société de l'information», in *Droit des Technologies de l'Information – Regards prospectifs*, Cahiers du CRID, n°16, Bruylant, 1999, p.33-54.

[245] Dans un premier temps, lors de la transposition de la directive 2001/29, le législateur français a érigé en contravention le fait de télécharger des œuvres sans autorisation, actes punis d'une amende de 150 euros pour l'*upload* et de 30 euros pour le *download*. Cet article a toutefois été censuré par le Conseil Constitutionnel en date du 27 juillet 2006, pour contradiction avec le principe d'égalité devant la loi. La loi HADOPI ne dit rien de la qualification de l'acte de téléchargement car le mandat de l'HADOPI est de poursuivre les internautes pour violation de l'article L. 336-3 du CPI qui érige la sécurisation de son accès à Internet en obligation. En Belgique,

disposition dans un réseau *peer-to-peer* ou sur un site de téléchargement direct de type Megaupload, la question de la qualification de cet acte en copie privée peut se poser. En effet, si l'internaute se contente de télécharger des œuvres pour son seul usage personnel, pourrait-il bénéficier de l'exception de copie privée ?

La copie de l'œuvre ainsi réalisée s'effectue en principe dans le cercle de famille et est réservée à celui-ci, selon les conditions de la copie privée posées par l'article 22, §1, 5° de la loi belge sur le droit d'auteur, du moins si l'utilisateur se contente de visionner ou d'écouter en privé le contenu ainsi téléchargé. Précisons d'emblée que les téléchargements de programmes d'ordinateur échappent à l'exception de copie privée, qui ne leur est pas reconnue en droit européen ou en doit belge.

Au Canada, la Cour fédérale s'est prononcée, dans une décision fort remarquée, en faveur de l'application de l'exception pour utilisation privée aux actes de *downloading*[246], mais la décision a été contestée sur ce point en appel, sans que la question ne soit pour autant définitivement tranchée[247]. Certaines décisions françaises ont également, dans un premier temps, appliqué l'exception de copie privée aux actes d'acquisition d'œuvres en *peer-to-peer*[248]. Le 15 novembre 2010, la Cour d'appel du district de La Haye s'est prononcée, à l'occasion de deux affaires[249], en faveur de l'admission de l'exception de copie privée pour les *download* réalisés sur les réseaux *peer-to-peer*. Cette qualification de copie privée a été rejetée par d'autres décisions[250].

Plusieurs arguments ont toutefois été soulevés à l'encontre de la reconnaissance de la copie privée dans ces hypothèses.

Voir Civ. Anvers (réf.), 21 déc. 1999 (I.F.P.I. c. Beckers), *A&M*, 2000, p. 296, qui a qualifié ce téléchargement d'atteinte au droit d'auteur sans plus de précision.

[246] Cour fédérale du Canada, 31 mars 2004, BMG Canada Inc. v. John Doe, 2004 FC 488, [2004] 3 FCR 241, disponible sur http://www.canlii.org/en/ca/fct/doc/2004/2004fc488/2004fc488.html ; voir les observations de M. Vivant, PI juill. 2004, n° 12, pp. 834-837.

[247] Cour Fédérale du Canada, 19 mai 2005, BMG Canada Inc. v. Doe, 2005 FCA 193, [2005] 4 RCF 81, disponible sur http://www.canlii.org/en/ca/fca/doc/2005/2005fca193/2005fca193.html, §50-52. Voir le commentaire de la décision par C. P. SPURGEON, « Chronique du Canada », *RIDA* janv. 2006, n° 207, pp. 178-282, spéc. pp. 268-276. En appel, les juges ont relevé les erreurs de droit commises par la première décision et les nombreuses questions qui n'avaient pas été tranchées quant aux conditions de l'exception de copie privée.

[248] TGI Rodez, 13 octobre 2004, *Comm. com. électr.* 2004, comm. n° 152, note Ch. Caron, confirmé en appel, CA Montpellier (3ème ch. Corr.), 10 mars 2005, *Comm. com. électr.,* Mai 2005, note Ch. Caron; TGI Paris, 31ème ch., 8 décembre 2005, disponible sur http://www.juriscom.net/jpt/visu.php?ID=785; TGI Bayonne (corr.), 15 novembre 2005, disponible sur http://www.juriscom.net/jpt/visu.php?ID=768; TGI Le Havre, 20 septembre 2005, disponible sur http://www.juriscom.net/jpt/visu.php?ID=748; TGI Meaux, 3ème ch., 21 avril 2005, disponible sur http://www.juriscom.net/jpt/visu.php?ID=705 (voir la note de L. Thoumyre, « Peer-to-peer : l'exception pour copie privée s'applique bien au téléchargement », *Revue Lamy droit de l'immatériel*, Juillet-août 2005, p. 13).

[249] Gerechtshof 's-Gravenhage, 15 november 2010, ACI c.s. v. Stichting De Thuiskopie & SONT, LJN BO3982, 200.018.226/01, 05-2233 (Cour d'appel de La Haye, 15 novembre 2010, ACI c.s. c. Stichting De Thuiskopie & SONT, LJN BO3982, 200.018.226/01, 05-2233) ; Gerechtshof 's-Gravenhage, 15 november 2010, FTD BV v. Eyeworks Film & TV Drama BV, LJN BO3980, 200.069.970/01, 0-639 (Cour d'appel de La Haye, 15 novembre 2010, FTD BV c Eyeworks Film & TV Drama BV , LJN BO3980, 200.069.970/01, 0-639). Pour un commentaire, voir E. YILDIRIM, "La Cour d'appel déclare légal le téléchargement à partir de sources illicites », IRIS Plus, 2001-4, pp. 34-35. Une proposition de loi visant à interdire également le downloading s'il émane d'une source illégale, pour un usage privé a été rejetée par le Parlement hollandais en décembre 2011. Voir ERNESTO, « Dutch Parliament : Downloading movies and music will stay legal », TorrentFreak, 24 décembre 2011, disponible sur : http://torrentfreak.com/dutch-parliament-downloading-movies-and-music-will-stay-legal-111 224/.

[250] En Espagne, Provincial Audience of Cantabria (Audiencia Provincial de Cantabria), 18 Février 2008 ; en France, TGI Rennes, 30 nov. 2006, *Comm. com. Electr*., mars 2007, comm. n° 38, obs. Ch. CARON.

Le premier est d'ordre technique et est propre à l'architecture du *peer-to-peer*. La position par défaut dans ces systèmes est en effet que l'utilisateur qui s'y connecte doive tout autant mettre à disposition d'autrui le contenu de son ordinateur que puiser dans le vaste répertoire offert illicitement. Refuser le partage des œuvres stockées requiert de désactiver la fonction de mise à disposition offerte par ces logiciels. Peu d'utilisateurs font consciemment cette démarche. Pour cette raison, une décision récente d'un tribunal hollandais accepte la copie privée mais considère que les internautes s'adonnant au *peer-to-peer* effectuent en tout état de cause des actes *d'upload* constitutifs d'une atteinte au droit d'auteur[251]. En outre, même si l'internaute opte pour le seul *download* de contenus, refusant d'*uploader* son propre répertoire, l'œuvre qu'il télécharge est automatiquement mise à disposition des personnes présentes dans le réseau *peer-to-peer* le temps du téléchargement. Cette particularité technique emporte deux conséquences juridiques : un simple téléchargeur mettra également ces œuvres à disposition du public, même à son insu, ce qui le rendra responsable d'une atteinte au droit d'auteur. D'autre part, cette mise à disposition, comme conséquence technique du téléchargement, pourrait disqualifier celui-ci en tant que copie privée, l'acte de copie n'étant plus potentiellement réservé au seul usage du cercle de famille.

On pourrait rétorquer à cette analyse que cet acte de mise à disposition est accessoire à la copie privée et se réalise à l'insu de l'utilisateur, ce qui n'invaliderait pas l'argument basé sur l'exception. En outre, l'accès à des œuvres sur des sites de téléchargement direct ou de streaming ne comporte pas cette mise à disposition indissociable du téléchargement et échappe donc à cette argutie en défaveur de la copie privée.

Un autre argument est celui de la nécessité d'une source licite. A l'appui de cette position, certains auteurs estiment que l'exigence d'une source licite est contenue implicitement dans la loi, qu'elle est présupposée[252], d'autres se fondent sur l'adage *Fraus omnia corrumpit*[253]. Pour certains, admettre le jeu de l'exception de copie privée malgré l'illicéité de la source irait à l'encontre du test des trois étapes[254] car cela permettrait l'acquisition d'une œuvre en dehors de son exploitation normale. En outre, la condition de la licéité de la source serait opportune au regard des raisons qui ont justifié l'adoption de l'exception de copie privée[255].

Une partie de la jurisprudence française a suivi cette doctrine en refusant d'accorder l'exception de copie privée aux téléchargeurs au motif que la source était illicite[256].

Cette condition de source licite reste controversée. Elle repose notamment sur un argument de texte, soit le fait que la loi belge exige que le bénéfice des exceptions soit limité aux œuvres

[251] Rb. 's Gravenhage, 10 mai 2012, KG ZA 12-156, http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BW5387.
[252] P.-Y. GAUTIER, *Propriété littéraire et artistique*, PUF, 5ème éd., 2004, n° 343, p. 397 ; F. VALENTIN et M. TERRIER, « Peer-to-peer : panorama des moyens d'action contre le partage illicite des œuvres sur Internet », *Légicom* 2004/3, n° 32, pp. 17-29, spéc. pp. 25-27, spéc. p. 22.
[253] A. LATREILLE, « La copie privée démythifiée », *RTD com*. juill./sept. 2004, pp. 403-411, spéc. p. 405 ; F. VALENTIN et M. TERRIER, « Peer-to-peer : panorama des moyens d'action contre le partage illicite des œuvres sur Internet », *op. cit*., spéc. p. 22.
[254] A. LATREILLE, « La copie privée démythifiée », *op. cit*., spéc. p. 406.
[255] A. ROBIN, note sous TGI Vannes, 29 avr. 2004, *Légipresse* oct. 2004, n° 215, III, pp. 180-187.
[256] TGI Rennes, 30 nov. 2006, *Comm. com. Electr.,* mars 2007, comm. n° 38, obs. Ch. CARON. Il a été jugé que « l'exception pour copie privée ne saurait avoir pour effet de rendre licite la reproduction d'une œuvre illicitement obtenue ». – CA Versailles, 9ème ch. corr., 16 mars 2007, *Comm. com. électr.,* juill./août 2007, comm. n° 91, note Ch. CARON.

« licitement publiées ». La majorité de la doctrine considérant toutefois qu'il faut entendre par là que l'œuvre doit avoir fait l'objet d'une divulgation[257], l'argument n'est pas en soi convaincant.

D'autres auteurs considèrent également que, dans un système fermé d'exceptions, « seule une disposition expresse de la loi pourrait fonder une telle exigence »[258], qui ne peut être déduite des dispositions légales existantes[259] : « la qualité de la source n'importe pas à la qualification de la copie privée licite »[260]. Force est d'ailleurs de constater que le législateur belge n'a pas souhaité modifier la disposition en insérant la condition d'une source licite, à l'occasion de la transposition de la directive « société de l'information ».

On peut formuler une autre opposition fondamentale à la nécessité de la source licite : si l'on soumet l'exception de copie privée à cette nouvelle condition sans aucun texte légal, pourquoi ne pas y subordonner toutes les exceptions ? Serait-il envisageable de refuser d'accorder l'exception de courte citation, en supposant que les conditions sont satisfaites, au seul motif que l'exemplaire sur lequel s'appuie l'utilisateur est une copie pirate ? L'enregistrement d'une œuvre radiodiffusée dans le cercle de famille deviendrait-il interdit si le radiodiffuseur ou les câblodistributeurs ne s'acquittent pas du paiement des droits requis ? La généralisation de la condition d'une mise à disposition licite de l'œuvre n'aurait pas de sens[261].

La seule manière pour que la condition d'une source licite soit retenue serait que le législateur décide de l'inscrire dans la réglementation[262]. Tel a été le choix du législateur allemand à travers la loi du 10 septembre 2003 transposant la directive « société de l'information ». En vertu de l'article 53 de cette loi, l'exception pour copie privée, et seulement cette exception, n'est pas admise si elle a été réalisée à partir d'une source manifestement illicite. Le Danemark a suivi la même voie avec la loi du 7 juin 2001[263], ainsi que la Finlande, le Portugal et la Suède[264]. La France a rejoint ces pays en

---

[257] F. DE VISSCHER et B. MICHAUX, *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000, p. 107 ; M.C. JANSSENS, « De uitzonderingen op het auteursrecht anno 2005 - Een eerste analyse », *A&M*, 2005, p. 489, nr 19 ; S. Dusollier, « L'utilisation légitime de l'œuvre : un nouveau sésame pour le bénéfice des exceptions en droit d'auteur ? », *Communications – Commerce Electronique*, Novembre 2005, p. 17-20 ; A. STROWEL et J.P. TRIAILLE, "Le droit d'auteur du logiciel au multimédia", Bruxelles, Bruylant, 1997, p. 40 ; Anvers, 25 juin 2007, *A&M*, 2007, p.461. Voir également en ce sens le texte de la proposition de loi ayant donné lieu à la loi sur le droit d'auteur du 30 juin 1994, Proposition de loi relative au droit d'auteur, aux droits voisins et à la copie privée d'oeuvres sonores et audiovisuelles, Doc. parl., 329-1, S.E. 1988, p. 15.

[258] A. et H.-J. LUCAS, *Traité de la propriété littéraire et artistique*, Litec, 2007, n° 354, p. 284 ; A. LUCAS, *Droit d'auteur et numérique*, Litec, Droit@Litec, 1998, spéc. n° 348, p. 177.

[259] V.-L. BENABOU, « La coexistence entre DRM et l'exception de copie privée, L'expérience française à l'appui de la Belgique ? », *A&M,* juin 2005, pp. 556-567, spéc. p. 562. Voir également la Note de l'OPRI concernant le champ d'application des exceptions et celui de la rémunération pour copie privée à l'attention des membres de la Commission consultative, 10 Juillet 2003.

[260] P. SIRINELLI et M. VIVANT, « Arrêt de Montpellier du 10 mars 2005 : ce n'est pas le Peyrou ! », *RLDI*, mai 2005, n° 5, p. 6-9, spéc. n° 5, p. 8. ; S. DUSOLLIER, *Droit d'auteur et protection des œuvres dans l'univers numérique, Droits et exceptions à la lumière des dispositifs de verrouillage des œuvres*, Larcier, coll. Création Information Communication, Bruxelles, 2005, n° 589, p. 458.

[261] Sur ces derniers points, voir S. DUSOLLIER, « L'utilisation légitime de l'œuvre : un nouveau sésame pour le bénéfice des exceptions en droit d'auteur ? », *Comm. Comm. Electr.,* nov. 2005, étude n° 38, spéc. n° 4, pp. 19-20.

[262] A. et H.-J. LUCAS, *Traité de la propriété littéraire et artistique, op. cit.,* n° 354, p. 285 ; S. DUSOLLIER, « L'utilisation légitime de l'œuvre : un nouveau sésame pour le bénéfice des exceptions en droit d'auteur ? », *op. cit.,* spéc. n° 4, p. 20.

[263] P. SCHONNING, « Chronique des pays nordiques », *RIDA*, avr. 2002, n° 192, pp. 252-308, spéc. pp. 266-268.

adoptant dans sa législation la nécessité de la licéité de la copie pour bénéficier de l'exception pour copie privée. Cette copie doit désormais être réalisée à partir d'une source licite[265].

Si le législateur souhaite introduire une telle condition à la copie privée, encore faudrait-il qu'il exige que l'illicéité de la source soit manifeste, exigence qui apparaît dans le texte de la loi allemande, mais non dans la loi française récemment modifiée. A défaut de cette précision, la charge de la preuve de la licéité de la mise à disposition reposerait trop lourdement sur l'utilisateur qui n'est pas à même de vérifier la réalité de l'obtention des droits. En revanche, la précision que la copie privée ne peut être admise si elle émane d'une source manifestement illicite suffit à écarter son bénéfice dans le cadre des échanges d'œuvres sur les réseaux, les internautes ne pouvant ignorer qu'ils s'adonnent là à des pratiques non autorisées par les titulaires de droit d'auteur et droits voisins. En revanche, il pourrait être plus difficile dans certaines hypothèses d'œuvres offertes au public sur des sites Internet ayant toutes les apparences de la légitimité de ne pas reconnaître le bénéfice de la copie privée dans le chef de l'acquéreur de ces œuvres.

En conclusion, il nous apparaît, en l'état actuel du droit belge et à défaut d'une mention explicite dans la loi sur le droit d'auteur, que même si la copie privée était effectuée à partir d'une source illicite, l'exception pourrait malgré tout être admise. Mais il convient toutefois de rester attentif aux futures décisions que la Cour de Justice de l'Union Européenne pourrait rendre à ce sujet.

Un dernier argument à l'encontre de l'admissibilité de la copie privée aux actes de téléchargement est le test des trois étapes. D'aucuns considèrent que l'accès à des œuvres par téléchargement direct ou échange en *peer-to-peer* dépasse les limites de la copie privée car il porte atteinte à l'exploitation normale des œuvres. Pour que cet argument prospère, encore faut-il que le test des trois étapes puisse être directement invoqué comme une condition supplémentaire aux exceptions. La Cour de Justice de l'Union Européenne a récemment affirmé que les actes souhaitant bénéficier d'une exception doivent satisfaire aux conditions du triple test[266]. Elle a toutefois considéré en l'espèce que le respect des conditions spécifiques des exceptions (en l'espèce celle de la reproduction provisoire) suffisait à remplir celle du test des trois étapes[267].

III. L'accès aux œuvres en *streaming*

Lorsque l'utilisateur se contente de visionner l'œuvre en *streaming* sans télécharger une copie de cette œuvre sur son ordinateur, cet acte de streaming peut être analysé sur base de trois exceptions au droit d'auteur : la copie privée d'une part, qui couvre tout autant les copies permanentes que les copies transitoires, la reproduction provisoire d'autre part et enfin, la communication d'une œuvre dans le cercle de famille.

---

[264] G. WESTKAMP, *The Implementation of Directive 2001/29/EC in the Member States, Part II of the Study on the implementation of Directive 2001/29/EC*, IVIR, 2007, p 20-21 (disponible sur http://ec.europa.eu/internal_market/copyright/studies/studies_en.htm).
[265] Nouvel article L. 122-5-2°, Modifié par la loi n°2011-1898 du 20 décembre 2011.
[266] C.J.U.E., 4 octobre 2011, Football Association Premier League e.a, C-403/08 et C-429/08, § 181.
[267] *Ibidem.*

S'agissant de la première, la discussion qui précède est transposable aux actes de *streaming*, à l'exception de la communication au public accessoire à l'accès à l'œuvre. Par principe, en effet un bénéfice de l'œuvre en *streaming* n'entraine aucun acte de mise à disposition de celle-ci.

Si l'on admet l'exception de copie privée, il ne sera pas utile d'envisager l'éventuelle application de l'exception de copie provisoire. Si tel n'est pas le cas, les actes de copie de l'œuvre réalisés par l'internaute lors de l'écoute ou du visionnage de l'œuvre peuvent être qualifiés de provisoire. Répondent-ils pour autant aux conditions de l'exception relative à ce type de reproduction ?

En premier lieu, il faudrait que cet acte de copie transitoire intervienne dans le cadre d'une utilisation licite, ce qui est définie comme une utilisation « autorisée par le titulaire du droit concerné ou lorsqu'elle n'est pas limitée par la réglementation applicable »[268]. Si l'accès aux œuvres ne relève ni de la copie privée, ni d'une autorisation en amont des ayants droit, on voit mal ce qui pourrait autoriser cette utilisation.

En deuxième lieu, la copie transitoire ne peut avoir une signification économique indépendante. La Cour de Justice a récemment considéré que lorsque « lesdits actes de reproduction réalisés dans le cadre d'un procédé technique rendent possible l'accès aux œuvres protégées. Ces dernières ayant une valeur économique, l'accès à celles-ci revêt ainsi nécessairement une signification économique »[269]. On peut considérer que celle-ci est indépendante puisqu'elle permet à l'internaute d'avoir accès à l'œuvre sans autorisation de l'ayant droit, et donc sans en assumer le coût et la rémunération.

En raison de l'exception de communication dans le cercle de famille, l'acte d'écoute ou de visionnage d'une œuvre à des fins privées pourrait être considéré comme échappant au droit d'auteur.

§2. Légitimité des régimes d'autorisation

L'acte de mise à disposition d'œuvres sur Internet relevant du droit exclusif des auteurs, il ne peut être autorisé que par le législateur sous le couvert d'une exception ou d'une licence non volontaire ou par l'ayant droit par le biais d'une gestion individuelle ou collective.

Il en est de même du côté du téléchargement, à moins qu'on ne le considère comme relevant de la copie privée. Dans ce dernier cas, ces actes de copie sont autorisés par la licence légale prévue à l'article 22, §1, 5° LDA, assortie d'un droit à rémunération organisé aux articles 55 et suivants de la loi. Cette conclusion implique toutefois qu'on s'éloigne des propositions de licence globale qui font reposer la charge de la compensation équitable sur les fournisseurs d'accès à Internet. Etant un acte de copie privée, la compensation perçue en faveur des auteurs et autres ayants droit prendrait pour assiette les supports et équipements de reproduction, tels que CD et DVD vierges, lecteurs MP3. L'inclusion de ces actes de téléchargement dans le champ de la copie privée devrait en outre influer sur le calcul du montant de la compensation équitable qui selon la Cour de Justice, doit se calculer en fonction du préjudice subi par les ayants droit[270].

[268] Voir C.J.U.E., 4 octobre 2011, *Football Association Premier League e.a*, C-403/08 et C-429/08, §168.
[269] *ibidem*, § 174.
[270] C.J.U.E., 21 octobre 2010, *Padawan*, C-467/08.

Il est à souligner que les propositions de licence globale, et c'est le cas de la proposition de loi Ecolo/Groen, embrassent généralement les actes d'*upload* et de *download* dans une nouvelle hypothèse de licence légale, qui s'écarte donc de la licence existante en matière de copie privée[271].

Outre l'hypothèse d'une exception pure et simple au droit d'auteur, jamais envisagée comme solution au téléchargement d'œuvres sur Internet[272], les mécanismes de licence légale, de gestion collective obligatoire ou de licence collective étendue doivent être analysés au regard de différents principes de droit d'auteur. La licence non volontaire, en tant qu'exception aux droits exclusifs est particulièrement sujette à restriction, que ce soit par rapport au caractère exhaustif des exceptions et limitations admissibles en droit européen ou au test des trois étapes. Ces conditions ne s'appliquent en revanche à la gestion collective obligatoire ou à la licence collective étendue que si celles-ci sont qualifiées de limitations du droit d'auteur et des droits voisins. D'autres questions peuvent également se poser au regard du principe d'interdiction des formalités en droit d'auteur.

I. Question préliminaire : qualification de la gestion collective obligatoire et de la licence collective étendue

La Convention de Berne admet de limiter les droits exclusifs qu'elle accorde dans plusieurs hypothèses. Outre des exceptions qu'il autorise explicitement les Etats contractants à adopter[273] et les exceptions mineures reconnues implicitement[274], le traité international reconnaît la possibilité d'aménager les conditions d'exercice du droit exclusif en matière de nouvelle radiodiffusion ou communication d'une œuvre radiodiffusée (art. 11*bis* (2))[275] et d'enregistrement sonore d'une œuvre musicale (art. 13)[276]. Le test des trois étapes légitime également et de manière plus générale les

[271] Sauf le cas de la proposition française de l'Alliance Public Artistes qui soumet les actes de téléchargement au régime existant de copie privée, l'*upload* étant soumis à un régime de gestion collective obligatoire..

[272] A notre connaissance, il n'existe pas de proposition d'adoption d'une exception pour l'hypothèse des échanges d'œuvres à des fins non commerciales sur Internet. Cela est compréhensible dans la mesure où les auteurs seraient non seulement privés du contrôle de leurs œuvres dans ce contexte, mais ils ne percevraient aucune rémunération en contrepartie. Cette solution serait trop radicale et ne passerait certainement pas l'épreuve du test des trois étapes.

[273] Il s'agit notamment de la citation (art. 10(1)), de l'utilisation à des fins d'enseignement (art. 10(2)), la reproduction par la presse (art. 10bis (1)), le compte-rendu d'actualités (art. 10bis (2)), et les enregistrements éphémères par les organismes de radiodiffusion (art. 11bis (3)).

[274] Les exceptions mineures sont admises en vertu des actes de la Conférence de Stockholm et visent des cas d'utilisation de l'oeuvre *de minimis*.

[275] Art. 11bis (2) : « Il appartient aux législations des pays de l'Union de régler les conditions d'exercice des droits visés par l'alinéa 1) ci–dessus [droit de radiodiffusion et droits connexes], mais ces conditions n'auront qu'un effet strictement limité au pays qui les aurait établies. Elles ne pourront en aucun cas porter atteinte au droit moral de l'auteur, ni au droit qui appartient à l'auteur d'obtenir une rémunération équitable fixée, à défaut d'accord amiable, par l'autorité compétente ».

[276] Art. 13 : « (1) Chaque pays de l'Union peut, pour ce qui le concerne, établir des réserves et conditions relatives au droit exclusif de l'auteur d'une œuvre musicale et de l'auteur des paroles, dont l'enregistrement avec l'œuvre musicale a déjà été autorisé par ce dernier, d'autoriser l'enregistrement sonore de ladite œuvre musicale, avec, le cas échéant, les paroles; mais toutes réserves et conditions de cette nature n'auront qu'un effet strictement limité au pays qui les aurait établies et ne pourront en aucun cas porter atteinte au droit qui appartient à l'auteur d'obtenir une rémunération équitable fixée, à défaut d'accord amiable, par l'autorité compétente ».

limitations et exceptions par lesquelles les législations nationales dérogent aux droits exclusifs de l'auteur.

Si la licence non volontaire constitue de manière évidente une limitation du droit exclusif des auteurs qui, à ce titre, doit soit relever d'une des hypothèses de la Convention de Berne, soit passer le test des trois étapes, la question est controversée[277] pour les modalités de gestion collective que sont la gestion collective obligatoire et la licence collective étendue.

M. Ficsor considère que ces deux modalités de gestion collective sont des limitations des droits exclusifs[278], s'appuyant sur des arguments de texte relatifs aux articles 11*bis* et 13 de la Convention de Berne, et de l'effet de cette obligation de gestion collective sur le plein exercice des droits qui doit, selon lui, rester en principe individuel.

D'autres auteurs se rallient à cette position et l'appliquent également à la licence collective étendue[279]. S'agissant de cette dernière modalité de gestion collective, il s'agirait d'une limitation, qu'elle soit assortie ou non d'une faculté d'*opt-out*. Le législateur imposerait, dans le premier cas, une présomption d'autorisation de l'auteur pour l'utilisation visée tant qu'il n'a pas manifesté son désaccord : ce qui revient à renverser le principe fondamental du système du droit d'auteur, basé sur le choix exclusif de l'ayant droit[280]. Par ailleurs, si l'*opt-out* n'est pas prévu, le système devient obligatoire pour les titulaires de droits qui ne sont pas membres de la société de gestion et en cela, le caractère exclusif de leurs droits ne serait pas sauvegardé.

Une autre partie de la doctrine rejette cette qualification de la gestion collective obligatoire[281] en « limitation » du droit d'auteur[282], au motif que ce mécanisme ne limiterait pas ce droit, mais se contenterait d'organiser différemment ses modalités d'exercice. S. von Lewinski estime qu' « en

[277] Pour les divers arguments de la controverse, voir C. Colin, *Etude de faisabilité de systèmes de licences pour les échanges d'œuvres sur internet*, Etude pour la SACD/SCAM, 2011.

[278] M. FICSOR, « La gestion collective du droit d'auteur et des droits voisins à la croisée des chemins : doit-elle rester volontaire, peut-elle être "étendue" ou rendue obligatoire ? », *e-Bulletin du droit d'auteur*, oct. 2003, p. 4. En ce sens également, D. GERVAIS, *Application d'un régime de licence collective étendue en droit canadien : principes et questions relatives à la mise en œuvre*, Etude pour le ministère du patrimoine canadien, Juin 2003, disponible sur http://aix1.uottawa.ca/~dgervais/publications/licence_etendue_questions.pdf, spéc. p. 43.

[279] En ce sens, *La distribution des contenus numériques en ligne*, Rapport du CSPLA, présidé par P. SIRINELLI, déc. 2005, disponible en ligne sur le site du CSPLA, p. 67 : « lorsque les Traités internationaux ne prévoient pas la possibilité d'instaurer une licence légale, on ne peut imposer de gestion collective obligatoire ou d'accords collectifs étendus pour la raison que lorsque les textes internationaux consacrent un droit exclusif, le bénéficiaire de ce droit se voit reconnaître la liberté de l'exercer individuellement » ; voir également, Th. RIIS et J. SCHOVSBO, « Extended Collective Licenses and the Nordic Experience - It's a Hybrid but is It a Volvo or a Lemon? », 12 Janvier 2010, *Columbia Journal of Law and the Arts*, Vol. 33, Issue IV, disponible sur SSRN: http://ssrn.com/abstract=1535230, § 4.3.1, p. 15.

[280] Ch. RYDNING, *Extented Collective licences, The Compatibility of the Nordic solution with the international conventions and EC law*, Norvegian Research Centre For Computers and Law, Complex n° 3, 2010, n° 2.4, p. 24 : "such a system turns upside down the starting point of copyright, namely that it is forbidden to use a work unless authorization is granted by its rights holder. Using contractual presumptions (…) cannot alter this fact if the presumption of acceptance verges on a simulation".

[281] L'argumentation s'est développée principalement sur la gestion collective obligatoire mais peut s'appliquer également, avec les adaptations qui s'imposent, à la licence collective étendue.

[282] S. VON LEWINSKI, « La gestion collective obligatoire des droits exclusifs et sa compatibilité avec le droit international et le droit communautaire du droit d'auteur, Etude de cas », *E-bulletin du droit d'auteur*, janv./mars. 2004 ; Ch. GEIGER, « Le rôle du test des trois étapes dans l'adaptation du droit d'auteur à la société de l'information », *e-bulletin du droit d'auteur*, UNESCO, janv./mars 2007.

réalité, l'auteur ne se voit limité que dans les conditions[283] d'exercice du droit : seul le droit d'exercer son droit exclusif par l'intermédiaire de la société de gestion lui est permis, mais le droit lui-même n'est pas limité en tant que tel (…) »[284] et l'auteur conserve toujours le pouvoir d'influer sur les conditions et les modalités d'une licence à accorder à tel ou tel utilisateur[285]. Pour d'autres auteurs, la gestion collective obligatoire semble légitime si l'exercice individuel du droit en question s'avère impossible ou irréaliste et que les sociétés de gestion collective « participent (…) à l'effectivité du droit privatif quand le législateur a fait le choix de la gestion collective obligatoire »[286].

Si l'on suit cette tendance doctrinale, l'adoption d'une gestion collective obligatoire pour l'hypothèse d'échanges d'œuvres ne poserait aucune difficulté puisque, s'agissant simplement d'une organisation des modalités d'exercice des droits de reproduction et de communication au public des titulaires de droits, elle ne serait pas inquiétée par la Convention de Berne et ne devrait pas satisfaire aux exigences posées par le test des trois étapes[287].

Ce raisonnement est parfois transposé aux licences collectives étendues, pour l'extension légale d'une licence intervenue au nom d'auteurs représentés par une société d'auteurs, à des auteurs non membres[288]. A ce stade, une obligation est posée à certains auteurs par le biais du législateur qui paraît réduire leur liberté d'exercice des droits. Un mécanisme de licence collective étendue dotée d'une possibilité d'*opt-out* réduit le risque de qualification en limitation du droit d'auteur, l'auteur gardant le choix de sortir du mécanisme de licence étendue pour gérer lui-même, de manière individuelle, ses droits. Dans ce contexte, la licence collective étendue pourrait être envisagée comme *une variante de gestion collective volontaire* dans le sens où les titulaires de droits conservent leur choix d'exercer individuellement ou collectivement leurs droits. En revanche, dans le cas d'une licence collective dépourvue de la faculté d'*opt-out*, la loi impose aux auteurs la gestion collective, sans possibilité pour ceux-ci de s'en défaire. On est alors dans une hypothèse assez similaire à la gestion collective obligatoire et la qualification de la licence collective étendue en limitation ou non suivrait le sort de la gestion collective obligatoire.

Quelle que soit la position doctrinale adoptée en définitive, il nous paraît utile en toute hypothèse de faire passer l'épreuve du test des trois étapes aux propositions de licence globale, qu'elles reposent sur une licence non volontaire, une gestion collective obligatoire ou une licence collective étendue.

---

[283] Ch. GEIGER, « Le rôle du test des trois étapes … », op. cit., spéc. p. 11.

[284] S. VON LEWINSKI, « La gestion collective obligatoire des droits exclusifs … », *op. cit.*, p. 5. En ce sens également, CH. GEIGER, « Le rôle du test des trois étapes … », *op. cit.*, p. 11.

[285] S. VON LEWINSKI, « La gestion collective obligatoire des droits exclusifs … », op. cit., p. 7.

[286] M. VIVANT et J.-M. BRUGUIERE, *Droit d'auteur*, Dalloz, Précis, 1ère éd., 2009, n° 886, p. 603. S. VON LEWINSKI, « La gestion collective obligatoire des droits exclusifs …», *op. cit.*, p. 2.

[287] Si l'objectif ultime de la qualification de la gestion collective obligatoire et de la licence collective étendue est d'être soumise au test des trois étapes, n'est-il pas contradictoire de confronter cet exercice du droit exclusif au critère essentiel du test qu'est l'absence d'atteinte à l'exploitation normale ? Selon nous, ces méthodes d'exercice du droit d'auteur ne portent en principe pas préjudice à cette exploitation normale puisqu'elles permettent de réaliser cette exploitation. C'est d'autant plus vrai pour la licence collective étendue, que le législateur n'impose aux auteurs non membres d'une société de gestion collective, qu'en raison des contrats déjà conclus par cette dernière au nom d'une majorité d'auteurs, qui peuvent être raisonnablement considérés comme une exploitation normale pour être étendus à l'ensemble des ayants droit.

[288] Th. RIIS et J. SCHOVSBO, Extended Collective Licenses and the Nordic Experience, *op. cit.*, § 4.3.1, p. 15; Ch. RYDNING, Extented Collective licences, *op. cit.*, n° 2.4, p. 23 : "ECLs are in fact a means of managing collectively the rights of a whole class of authors. And, contrary to outright mandatory licences, the ECLs entail an active management, i.e. the terms of use are not regulated by rigid, passive legislation, but by agreements negotiated in the free market".

II. La liste fermée d'exceptions de la directive 2001/29

La directive européenne 2001/29 sur le droit d'auteur dans la société de l'information contient une liste exhaustive d'exceptions au droit d'auteur qui peuvent être consacrées par les législateurs des Etats membres. Sans surprise, le partage d'œuvres et prestations protégées sur les réseaux *peer-to-peer* ou tout autre mode de téléchargement illégal n'en fait pas partie. Sous réserve d'une adaptation du texte de cette directive, l'introduction d'une licence légale ou obligatoire autorisant le partage non commercial des œuvres par le législateur belge ne serait pas conforme à ses obligations communautaires.

C'est un nouvel argument qui plaide en défaveur de l'introduction d'une licence légale autorisant le *peer-to-peer*. Quant à la gestion collective obligatoire ou à la licence collective étendue, sous réserve de la controverse mentionnée *supra*, il semble que le législateur européen ne les considère pas comme des exceptions et limitations au droit d'auteur, mais comme des modalités d'exercice des droits[289].

Ce caractère limitatif des exceptions admissibles dans les Etats membres de l'Union européenne est renforcé par deux principes régulièrement soulignés par la Cour de Justice de l'Union européenne, soit l'objectif d'un niveau de protection élevé poursuivi par la directive sur le droit d'auteur dans la société de l'information, d'une part, et le principe d'interprétation stricte des exceptions d'autre part[290].

III. Le test des trois étapes

Le principe étant le caractère exclusif du droit, toute limitation devant y être apportée est strictement encadrée à l'échelon international et européen par le test des trois étapes[291], ce qui implique que les Etats ne peuvent prévoir des exceptions au droit d'auteur et aux droits voisins que dans certains cas spéciaux qui ne portent pas atteinte à l'exploitation normale de l'œuvre ni ne causent un préjudice injustifié aux intérêts légitimes de l'auteur.

Il existe de multiples interprétations du triple test et la jurisprudence, assez rare, n'est pas d'une grande aide. La seule analyse jurisprudentielle internationale du test des trois étapes émane du

[289] Voir le considérant 18 de la directive 2001/29.

[290] Voir notamment C.J.U.E., 1er décembre 2011, *Painer*, C-145/10, point 109. La Cour a toutefois nuancé récemment ce principe en rappelant que les exceptions devaient être interprétées de manière à « sauvegarder l'effet utile de l'exception ainsi établie et de respecter sa finalité » (C.J.U.E., 4 octobre 2011, Football Association Premier League e.a, C-403/08 et C-429/08, points 162 et 163)

[291] Cf. la Convention de Berne (Acte de Paris, 1971, article 9.2), le Traité de l'OMPI sur le droit d'auteur du 20 décembre 1996 (article 10), le Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes du 20 décembre 1996 (article 16), l'Accord sur les ADPIC entré en vigueur le 1er janvier 1995 (article 13) et la Directive 2001/29 du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information en son article 5.5. Sur l'histoire et la notion du test des trois étapes, voir M. SENFTLEBEN, Copyright, Limitations and the Three-Step Test, An analysis of the Three-Step Test in International and EC Copyright Law, Kluwer Law International, La Haye, 2004.

Groupe spécial de l'OMC dans le cadre d'un litige opposant l'Europe aux Etats-Unis[292]. La lecture que cette décision fournit du test est empreinte de la compétence particulière du panel, dans le cadre de l'OMC, qui doit juger *in abstracto*, de la légitimité d'une exception adoptée par un législateur. A ce titre, la décision a pu être jugée trop restrictive par certains membres de la doctrine qui ont proposé de faire du test en trois étapes un outil permettant davantage de souplesse dans la consécration des exceptions ou tenant compte des trois conditions du test comme d'un ensemble de facteurs à prendre en compte[293]. La Cour de justice de l'Union européenne a également confirmé récemment que le test des trois étapes devait s'appliquer aux exceptions mais sans développer l'interprétation de ses conditions[294].

A. L'exigence d'un cas spécial

Le test des trois étapes exige en premier lieu qu'une exception ne soit adoptée que s'il s'agit d'un « certain cas spécial », ce qui renvoie, selon les actes préparatoires de la Conférence diplomatique de la conférence de Stockholm, « à des fins nettement définies »[295] ou selon la décision du Panel de l'OMC au fait que « l'exception ou la limitation prévue dans la législation nationale doit être clairement définie » [296] et devrait avoir « un champ d'application limité ou une portée exceptionnelle »[297] et « être restreinte au sens quantitatif aussi bien que qualitatif »[298]. Il ne faut pas que l'utilisation devienne un cas généralisé.

Le fait de permettre les échanges gratuits d'œuvres entre internautes peut-il constituer un « cas spécial » ? En d'autres termes, il faut se poser les questions suivantes : quels utilisateurs vont bénéficier de la limitation, quelles catégories d'œuvres sont concernées, quels actes sont permis, dans quelle proportion et à quelle fin[299] ? En termes quantitatifs, tous les internautes sont potentiellement concernés par une telle exploitation. En revanche, seuls les échanges entre internautes à des fins non commerciales seraient autorisés. Les actes permis seraient en outre bien délimités. De plus, l'exigence de gratuité des échanges – pour les internautes – permettrait encore de rétrécir le champ de l'utilisation. La satisfaction de la première étape ne semble donc pas poser trop de difficultés quel que soit le mécanisme d'autorisation choisi.

---

[292] Rapport du Groupe Spécial de l'Organisation Mondiale du Commerce, Etats-Unis – Article 110 5) de la loi des Etats-Unis sur le droit d'auteur, 15 juin 2000, WT/DS160/R, disponible sur le site de l'OMC (<wto.org>).

[293] Voir Ch. GEIGER, « Le test des trois étapes, un danger pour l'équilibre du droit d'auteur ? », op. cit., spéc. p. 54 ; S. DUSOLLIER, « L'encadrement des exceptions au droit d'auteur par le test des trois étapes », *I.R.D.I.*, 2005, p. 213-223 ; ainsi que la Déclaration en vue d'une interprétation du "test des trois étapes" respectant les équilibres du droit d'auteur, disponible sur le site de l'Institut Max Planck pour la propriété intellectuelle : http://www.ip.mpg.de/shared/data/pdf/declaration_three_steps.pdf

[294] C.J.U.E., 4 octobre 2011, Football Association Premier League e.a, C-403/08 et C-429/08, point 181.

[295] Voir Ch. RYDNING, Extented Collective licences, *op. cit.*, § 4.1.4 : « the first step indeed does require a reasonable degree of clarity and foreseeability".

[296] Rapport du Groupe spécial de l'OMC n° WT/DS160/R, *op. cit.*, § 6.108.

[297] *Ibid.*, §6.109.

[298] *Ibid.* Rappr. A. LUCAS, *Droit d'auteur et numérique*, *op. cit.*, n° 374, p. 187 : « la formule [les cas spéciaux] n'est pas très contraignante. Elle postule simplement l'exclusion des exemptions généralisées ».

[299] Ch. RYDNING, Extented Collective licences, *op. cit.,* § 4.2.2, p. 47.

Par ailleurs, si le choix se portait vers le système de licence collective étendue, cette première étape du test pourrait être franchie encore plus facilement. Tout d'abord, la base contractuelle du dispositif couplée à l'exigence de représentativité de la société de gestion collective constitue déjà un cadre défini. En réalité, seuls les auteurs non-membres subissent une limitation de leurs droits exclusifs ; les auteurs membres ont choisi de les exercer de manière collective[300]. Ensuite, cette base contractuelle implique que les dispositions qui autorisent l'extension de la licence collective étendue délimitent seulement une frontière extérieure. Le champ d'application actuel de la limitation est déterminé par l'accord collectif, lequel servira de base à l'extension de ses effets aux auteurs non-membres[301]. Les limitations imposées aux auteurs non-membres n'iront jamais au-delà de ce que prévoit l'accord collectif. Enfin, la nécessité d'un agrément de la société de gestion collective agit comme une limitation du champ[302]. Grâce au mécanisme de la licence collective étendue, le cas spécial dans l'hypothèse qui nous intéresse pourrait donc être bien délimité. La première étape du test pourrait être franchie.

B. L'exigence d'une absence d'atteinte à l'exploitation normale de l'œuvre

Le deuxième impératif du test en trois étapes consiste à apprécier si l'utilisation des œuvres en question porte atteinte à leur exploitation normale. Selon M. Senftleben, un « conflit avec une exploitation normale se produit lorsque les auteurs sont privés d'une source majeure de revenus, actuelle ou potentielle, qui revêt une certaine importance dans l'ensemble des modes de commercialisation des œuvres de cette catégorie »[303].

De manière assez similaire, le Groupe spécial de l'OMC a considéré qu'une exception aux droits exclusifs portera atteinte à l'exploitation normale de l'œuvre si elle « constitue une concurrence aux moyens économiques dont les détenteurs du droit tirent normalement une valeur économique de ce droit sur l'œuvre (…) et les privent de ce fait de gains commerciaux significatifs ou tangibles »[304], tant potentiels que réels. Cette approche peut inclure une dose de normativité, qui intègre une analyse en terme d'intérêt public, ce que l'OMC a confirmé dans une autre affaire en matière de brevets[305] et ce qui est conforme à la généalogie du test[306].

[300] *Ibid*., § 4.2.3, p. 49.
[301] *Ibid*., § 4.2.3, p. 49 et p. 50.
[302] *Ibid*., § 4.2.3, p. 49 et p. 50, 51.
[303] M. Senftleben, op. cit., p. 194.
[304] *Ibid*., § 6.183. Cette interprétation est conforme aux travaux préparatoires de la Conférence de révision de Stockholm : se reporter à M. Ficsor, « How much of that ? The three-step test and its application in two recent WTO dispute settlements cases », op. cit., spéc. p. 136.
[305] décidant qu'une exploitation sera normale lorsqu'elle est « essentielle pour réaliser les objectifs d'une politique de brevet » : voir Rapport du Groupe spécial de l'OMC du 17 mars 2000 (WT/DS 114/R) dans une affaire opposant les Communautés Européennes au Canada à propos de la protection des inventions dans le domaine pharmaceutique.
[306] Les actes de la conférence de Stockholm indiquent en effet qu'il s'agissait de tenir compte des intérêts publics et culturels formant le soubassement des exceptions. Les traités de l'OMPI incitent également à se préoccuper de l'intérêt public.

Le fait de permettre les échanges d'œuvres entre internautes, à des fins non commerciales, sur les réseaux *peer-to-peer* ou sur des sites de téléchargement direct porte-t-il atteinte à l'exploitation normale de ces œuvres ?

Il convient dans un premier temps de définir ce que peut être l'exploitation normale des œuvres, c'est-à-dire l'exploitation qui génère des recettes significatives ou tangibles actuellement ou qui pourraient y donner lieu à l'avenir, étant entendu que l'exploitation normale de l'œuvre ne peut correspondre au plein usage des droits exclusifs. Dans ce contexte, l'exploitation normale des œuvres peut se comprendre comme correspondant à l'offre de téléchargement légal. Mais on peut y ajouter également des modes d'exploitations classiques, tels que la sortie en salle, la vente de disques, de livres ou de DVD.

Dans un second temps, il s'agit de savoir si la limitation envisagée aux droits exclusifs porte atteinte à l'exploitation normale, en d'autres termes si elle constitue une exploitation concurrente qui aurait pour effet de priver les auteurs de revenus significatifs. Les échanges d'œuvres sur les réseaux *peer-to-peer* représentent assurément un mode de mise à disposition des œuvres au public qui est susceptible de concurrencer les plates-formes de téléchargement légal et autres modes d'acquisition des œuvres sur le marché contrôlé par les ayants droit[307]. Toutefois, certains estiment que cet effet n'est pas aussi automatique, se fondant sur certaines études économiques réalisées sur l'effet du *peer-to-peer* sur les ventes d'œuvres musicales[308], mais cette opinion est minoritaire et ne permet pas de valider la deuxième étape du test

La licence légale semble donc difficilement compatible avec cette condition du test des trois étapes.

Quant à la gestion collective obligatoire, la réponse doit être plus nuancée en ce sens que la société de gestion conserve une certaine marge de manœuvre pour négocier les contrats avec les utilisateurs et s'adapter en conséquence aux mécanismes déjà existants d'offres légales, et partant éviter la concurrence directe avec les offres légales. Et il ne faut pas négliger le fait que la négociation se fera sur une base volontaire de la société de gestion.

S'agissant de la licence collective étendue, il convient de souligner qu'à son origine intervient la signature d'un accord entre les sociétés de gestion collective auxquelles ont adhéré volontairement un nombre substantiel d'auteurs, et les utilisateurs. La licence collective étendue est le résultat d'un choix fait par les titulaires de droits d'une certaine catégorie d'œuvres pour les contrats collectifs au lieu de se livrer à une gestion individuelle[309]. On peut donc estimer que la licence collective constitue l'exploitation normale des droits dans certaines hypothèses particulières[310]. Lorsque l'accord collectif est ensuite étendu aux titulaires de droits non-membres, ceux-ci ne sont pas privés d'une exploitation normale de leurs droits ; bien au contraire, ils sont inclus dans une exploitation qui a été considérée comme « normale » par un nombre substantiel de titulaires de droits. De plus, les

[307] Ch. GEIGER, « Le rôle du test des trois étapes dans l'adaptation du droit d'auteur à la société de l'information », *op. cit.,* p. 9.

[308] Voir notamment P. AIGRAIN, *Sharing - Culture and the Economy in the Internet Age*, Amsterdam University Press, 2012, p. 110 et suiv. et les études citées.

[309] Th. RIIS et J. SCHOVSBO, "Extended Collective Licenses and the Nordic Experience", *op. cit.*, p. 16.

[310] *Ibid.*, p. 17 : « Within the special Danish/Nordic setting, (…) where ECL-rules have been part of the legal tradition and where the solutions is favoured by most interested parties it would seem hard not to conclude that the Danish ECL-rules would generally pass the second prong of the test". Ch. RYDNING, Extented Collective licences, *op. cit.*, § 5.2.3.2, p. 63 : "the requirement of representativity ensures that the ECL-agreement is at least a normal exploitation of the type of works covered".

limitations imposées aux auteurs non-membres ne peuvent excéder les termes de l'accord collectif. Et la limitation a été approuvée par un nombre substantiel d'auteurs de la même catégorie d'œuvres.

Par ailleurs, si l'*opt-out* est proposé aux auteurs – ce qui est loin d'être toujours le cas – le dispositif a encore plus de chances de passer avec succès la deuxième étape. En somme, si l'auteur peut s'extraire du système obligatoire et revenir à une gestion individuelle de ses droits exclusifs, l'exploitation normale de l'œuvre est encore moins susceptible d'être contrariée[311].

C. L'exigence d'une absence de préjudice injustifié aux intérêts légitimes de l'auteur

Le test des trois étapes impose enfin que l'exception « ne cause pas un préjudice injustifié aux intérêts légitimes du détenteur de droit ». Un préjudice, tant réel que potentiel, sera donc injustifié « si une exception ou limitation engendre ou risque d'engendrer un manque à gagner injustifié pour le titulaire du droit d'auteur »[312], ce dernier pouvant justifier l'attribution d'une compensation aux ayants droit, ce qui encourage particulièrement les mécanismes de restriction qui prévoient la rémunération de l'auteur[313]. Cette troisième étape du test constitue en quelque sorte un test de proportionnalité.

Le fait de retirer à l'auteur son contrôle sur les acquisitions d'œuvres en *streaming* ou dans les réseaux *peer-to-peer* lui cause-t-il un préjudice injustifié ? Est-il proportionné, au regard de ses intérêts légitimes à la fois économiques et moraux, de lui infliger une limitation de son droit exclusif pour ce qui concerne les échanges de ses œuvres sur les réseaux *peer-to-peer* ? En tout les cas, prévoir une exception au droit d'auteur sans aucune rémunération des ayants droit ne pourrait satisfaire cette dernière étape du test, le préjudice causé aux auteurs étant certainement disproportionné dans cette hypothèse.

Les intérêts des auteurs sont toutefois mieux pris en compte dans les systèmes d'autorisation basée sur de la gestion collective dans la mesure où ils bénéficient d'une négociation collective de leurs droits exclusifs des conditions et tarifs des licences, ainsi que d'une représentation par la société de gestion. Par ailleurs, si une licence collective étendue est prévue, cela suppose qu'un nombre substantiel d'auteurs a choisi de recourir à la solution contractuelle ; donc, pour ces auteurs, il n'existe pas de préjudice car ils ne font qu'exercer leurs droits. La question se pose uniquement pour les auteurs non-membres qui eux se voient infliger une limitation qu'ils n'ont pas choisie. Toutefois, étant donné qu'un nombre significatif d'auteurs a décidé, volontairement et sur une base collective, qu'un tel contrat était le meilleur moyen d'exercer leurs droits, il est possible de dire que le mécanisme de la licence collective étendue ne cause pas aux auteurs non-membres un préjudice injustifié[314]. De plus, la position de la société de gestion collective accroît son pouvoir de négociation

[311] A. PEUKERT, "A Bipolar Copyright System for the Digital Network Environment", *op. cit.,* p. 1.
[312] *Ibid.*, § 6.229.
[313] B. HUGENHOLTZ et R. OKEDIJI, *op. cit.,* p. 19 : "such compensated limitations are generally more likely to pass the test given the fact that prescribing compensation to authors or right holders is generally recognized as a crucial factor in assessing 'unreasonable prejudice' under the third step".
[314] Ch. RYDNING, Extented Collective licences, *op. cit*., § 6.2.4, p. 71 et § 6.2.6, p. 73.

avec les utilisateurs[315]. Quant à la faculté d'*opt-out*, elle réduit assurément le préjudice subi par l'auteur[316]. Toutefois, une licence collective étendue sans *opt-out* a tout de même de grandes chances de passer avec succès la troisième étape du test.

En conclusion, le mécanisme de la licence non volontaire pour autoriser les échanges d'œuvres sur les réseaux *peer-to-peer* ne semble pas apte à satisfaire le test des trois étapes dans la mesure où il retire toute possibilité aux titulaires de droits de contrôler l'exploitation de leurs créations dans ce contexte ; de surcroît, il risque fort d'être en concurrence directe avec les offres légales de téléchargement. En revanche, une solution de gestion collective renforcée par le biais d'une gestion collective obligatoire ou d'une licence collective étendue, a davantage de chances de réussir l'épreuve, à supposer que ces deux mécanismes soient qualifiés de limitations des droits exclusifs et soient soumis à ce titre au test des trois étapes.

IV. L'interdiction de formalités

En vertu de l'article 5.2) de la Convention de Berne, « la jouissance et l'exercice de ces droits ne sont subordonnés à aucune formalité ». Ainsi est posé le principe de l'absence de formalités à accomplir par les auteurs pour bénéficier de la protection par le droit d'auteur[317]. Le principe de l'absence de formalités vise aussi bien l'existence du droit d'auteur que son exercice[318].

Qu'en est-il des systèmes *d'opt-out* par lesquels soit l'auteur recouvre son droit exclusif, tel le cas d'une licence légale par défaut dont l'auteur pourrait sortir[319], ou celui d'une licence collective étendue dans lequel l'auteur peut recouvrer l'exercice individuel de son droit ?

Certains auteurs considèrent que le principe d'interdiction des formalités s'oppose à tout système de licences, soit légales, soit issue d'une gestion collective, dont l'auteur ne peut s'extraire qu'en exerçant un *opt-out* exprès[320], ce qui inclut les licences collectives étendues.

Pour la licence légale, la règle d'interdiction des formalités n'empêche pas l'adoption d'exceptions et limitations du droit d'auteur, notamment par le biais de licences non-volontaires, dans le respect du test des trois étapes[321]. *L'opt*-out qui serait prévu dans un tel système permettrait de recouvrer son droit exclusif, là où le législateur a opté pour une exception. Appliquer le principe de l'interdiction des formalités dans ce cas reviendrait à une protection moindre des auteurs ce qui est contradictoire

[315] *Ibid.*, § 6.2.5, p. 71 et s.
[316] *Ibid.*, § 6.2.8.3, pp. 84-85.
[317] Sur le principe d'interdiction des formalités, voir la thèse de S. van Gompel, *Formalities in Copyright Law - An Analysis of Their History, Rationales and Possible Future*, University of Amsterdam, March 2011.
[318] Il est à noter que ce principe ne vaut pas pour les droits voisins même si ces droits sont, en Belgique et en Europe, accordés sans aucune formalités.
[319] Voir la proposition en ce sens d'A. PEUKERT. Voir également D. GERVAIS, The Changing Role of Copyright Collectives, in D. Gervais (ed.), *Collective Management of Copyright and Related Rights*, 2006, p. 34.
[320] See FICSOR, Collective Management of Copyright and Related Rights in the Digital, Networked Environment: Voluntary, Presumption-Based, Extended, Mandatory, Possible, Inevitable?, in COLLECTIVE MANAGEMENT OF COPYRIGHT AND RELATED RIGHTS, 2006, p.48; voir également Peukert qui considère qu'un système de licence légale avec opt-out, proposé par une certaine doctrine américaine, se heurte pareillement à l'article 5(2) de la Convention de Berne (A. PEUKERT, *op. cit.*, p.184)
[321] S. VAN GOMPEL, *op. cit.*, p. 190.

avec l'objectif poursuivi. L'interdiction des formalités ne devrait donc pas constituer un obstacle à des conditions imposées aux auteurs pour ne pas être englobés dans une hypothèse d'exception ou de licence non-volontaire, pour autant que celle-ci satisfasse au test des trois étapes.

S'agissant de la licence collective étendue[322], on pourrait considérer que l'*opt-out* ne constitue pas une véritable restauration de l'exercice du droit d'auteur qui serait impossible par ailleurs – puisque c'est précisément l'objectif de la mise en place d'une licence collective étendue – mais un choix alternatif d'exercice que peuvent exercer les auteurs.

Selon S. van Gompel, l'*opt-out* « regulates the extent of protection rather than the enjoyment or the exercise of copyright. The possibility to 'opt out' merely reflects the choice that right owners can make between two different exploitation models that the law offers them. (…) It is comparable with the need to become a member of, and to register works with, a particular CMO to receive the compensation collected in a collective licensing scheme »[323].

Dans cette perspective, l'article 5.2 de la Convention de Berne posant le principe de l'absence de formalités pour jouir et exercer les droits d'auteur ne pourrait être opposé à une licence collective étendue assortie d'une faculté d'*opt-out*. Les droits étant déjà exercés collectivement par les sociétés de gestion, l'*opt-out* a simplement pour objectif non pas de créer des conditions d'exercice des droits *ex nihilo*, mais simplement de redonner aux titulaires de droits la possibilité d'une gestion individuelle.

V. L'étendue du répertoire

Dans les systèmes prônant l'instauration d'une licence globale, les internautes souhaiteront de toute évidence une légitimation de l'ensemble de leurs échanges non commerciaux sur Internet. Tout modèle d'autorisation devrait en conséquence couvrir un large répertoire, tant en termes de différentes catégories d'œuvres que de titulaires de droits. La licence légale, parce qu'elle s'impose à tous les objets protégés par un droit d'auteur ou un droit voisin répond à cette condition.

Les solutions basées sur la gestion collective ne peuvent qu'englober les œuvres contenues dans le répertoire des sociétés concernées. L'outil de la gestion collective obligatoire renforce en tout cas la position des sociétés d'auteur et de titulaires de droits voisins. Quant à la licence collective étendue, elle ramène dans le répertoire collectif les œuvres et prestations qui n'en feraient pas partie, constituant par-là la possibilité d'une véritable licence globale.

Toutefois, encore faut-il que l'ensemble des sociétés de gestion collective admettent d'autoriser contractuellement ce type d'utilisations. La gestion des droits, c'est bien connu, est fragmentée entre catégories d'œuvres (musique, films, images, …)[324], catégories d'ayants droit (auteurs, artistes-interprètes, producteurs, …), voire entre droits exclusifs eux-mêmes[325].

[322] Th. RIIS et J. SCHOVSBO, "Extended Collective Licenses and the Nordic Experience, *op. cit*., spéc. p. 13.
[323] S. VAN GOMPEL, *op. cit*., p. 190.
[324] D. GERVAIS, The Changing Role of Copyright Collectives, *op. cit*., p. 10–12.
[325] Le droit de reproduction et le droit de mise à disposition en matière musicale sont de plus en plus exercés directement par les éditeurs de musique qui sont sortis des sociétés de gestion collective, ces dernières continuant à exercer le droit de communication.

Une autorisation des échanges n'est pas non plus une solution uniforme pour tous types d'œuvres, dont le mode d'exploitation et les marchés diffèrent. Les ayants droit sur les films pourraient ne pas vouloir d'une éventuelle licence globale[326] notamment en raison de la règle de chronologie des média.

Si l'objectif est d'inclure toutes les œuvres et prestations dans l'autorisation donnée aux internautes, il s'agira de parvenir à un consensus entre tous les titulaires de droits et les sociétés de gestion les représentant, tout en parvenant à une rémunération globale qui à la fois tienne compte d'une rémunération équitable pour chaque catégorie d'ayant droit et reste raisonnable pour l'utilisateur.

Un autre obstacle réside dans la compétence des sociétés de gestion collective à intervenir pour le répertoire de leurs sociétés sœurs établies à l'étranger.

Les sociétés de gestion collective concluent des accords de représentation réciproque avec des sociétés sœurs. Ces accords permettront à l'usager d'utiliser les œuvres étrangères visées par ces accords pour les exploitations définies dans l'accord. En fait, « chaque membre (…) sera considéré par la société étrangère comme faisant partie de cette société étrangère, et réciproquement »[327]. Les sommes collectées en Belgique pour l'utilisation d'œuvres étrangères sont réparties à leurs ayants droit, par l'intermédiaire des sociétés de gestion collective de leur pays. Et réciproquement.

Mais le système a ses limites car il n'opère que pour des exploitations strictement définies. A l'heure actuelle, les échanges en *peer-to-peer* n'en font pas partie. Le seul autre instrument dont pourraient disposer les sociétés de gestion collective serait d'obtenir un mandat exprès des autres sociétés, ce qui serait laborieux et improbable. Plus spécifiquement, les droits sur les films américains sont détenus par les producteurs, en vertu du droit d'auteur américain et aucun accord de représentation réciproque n'existe ici, ces producteurs gérant leurs droits de manière individuelle et non par le truchement d'une société de gestion collective (celle-ci étant par ailleurs peu utilisée aux Etats-Unis).

La gestion collective obligatoire ne fait pas échec à cette représentation limitée des sociétés de gestion collective. En effet, si le législateur impose la gestion collective d'un droit, cela n'emporte pas pour autant la représentation des œuvres étrangères par la société désignée. La difficulté ne se pose pas pour la seule hypothèse que nous connaissons de gestion collective obligatoire, à savoir pour le câble, dans la mesure où des accords de représentation réciproque existent pour cette exploitation. Mais ce ne sera pas le cas pour le *peer-to-peer*.

En revanche, le mécanisme de licence collective étendue a, dans les pays nordiques qui la connaissent, un effet sur les œuvres étrangères également[328]. Leurs auteurs et titulaires de droit peuvent voir une licence conclue par une société jugée représentative s'imposer à eux. Toutefois, il semble que les dispositions relatives à la licence collective étendue exigent désormais non pas que la société de gestion collective gère une majorité d'œuvres nationales, mais aussi qu'elle gère une majorité d'œuvres exploitées sur le territoire sur lequel elle est établie[329]. En d'autres termes, la société collective doit également représenter un nombre suffisant de titulaires de droits étrangers

[326] D. GERVAIS, « User-Generated Content and Music File-Sharing: A Look at Some of the More Interesting Aspects of Bill C-32 », in M. Geist (ed.), *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda* , 2010, p. 458-59.
[327] N. ROUART, Sociétés de perception et de répartition des droits, Société des auteurs et compositeurs dramatiques (SACD), *J.-Cl. Propriété Littéraire et Artistique*, Tome 3, Fasc. 1570, nov. 1999, spéc. n° 43.
[328] J. ROSEN, « News from the Nordic Countries », *op. cit*., p. 185.
[329] *Ibid*.

pour le mode d'exploitation qui pourrait bénéficier de l'extension. A notre sens, cela implique que la société d'auteurs bénéficie d'accords de représentation réciproque pour cette exploitation, à défaut de quoi elle ne peut gérer les droits de ces œuvres étrangères et partant, atteindre le seuil de représentativité requis pour que s'enclenche le mécanisme légal d'extension des accords de licence qu'elle conclut. En conséquence, et si cette interprétation de l'application de la licence collective étendue était appliquée en Belgique, la limitation du répertoire donné en licence subsisterait, aucun accord de représentation réciproque n'existant en matière d'échanges en *peer-to-peer.*

Quel que soit le mécanisme juridique choisi, outre la licence légale, une solution de légitimation des échanges *peer-to-peer* risque de se limiter aux échanges belges d'œuvres appartenant au répertoire belge, ce qui constitue une des principales difficultés pour le succès de l'opération auprès des internautes.

VI. Le mécanisme étranger de la licence collective étendue

Une dernière difficulté s'attache au système de la licence collective étendue. Si celui-ci gagne en popularité, il reste une institution propre aux pays scandinaves et étrangère à la tradition juridique du droit d'auteur belge. Sa mise en place requiert en outre un certain délai puisque la licence collective étendue suppose au préalable une pratique contractuelle reconnue des sociétés de gestion collective représentatives. La transposition en Belgique de ce mécanisme ne va donc pas de soi.

Section 2. Les questions relatives à l'intervention des intermédiaires techniques

La règle de **l'exonération de responsabilité** des intermédiaires empêche-t-elle la mise en place de certaines solutions ou impose-t-elle certaines précautions dans cette mise en place ?

Les solutions de filtrage, de blocage de sites, d'avertissements envoyés aux internautes ou autres interventions requises des intermédiaires contreviennent-elles à la règle d'exonération de responsabilité ou à l'interdiction d'une **surveillance générale** ? Quelle est l'étendue admise d'une **cessation ou autre injonction** pouvant être prononcée à l'encontre des intermédiaires ?

Les effets des injonctions judiciaires à l'égard de certains FAI peuvent-ils être étendus à des FAI non parties à la cause, et si oui dans quelles conditions, afin d'assurer l'effectivité de ces mesures et l'absence de distorsion de concurrence entre les intermédiaires ?

Comment assurer un monitoring des injonctions judiciaires enjoignant aux intermédiaires de prendre des mesures visant à neutraliser des contenus illicites mis à disposition, afin d'assurer l'effectivité de ces mesures et l'absence de distorsion de concurrence entre les intermédiaires ?

Quels sont les principes et conditions d'un régime de limitation de responsabilité des intermédiaires qui prennent des mesures de neutralisation de contenus illicites ?

Sur toutes ces questions, comment tenir compte de la **règle de proportionnalité** dégagée par la Cour de Justice de l'Union européenne ?

A l'échelle européenne, le plan d'action de la Commission en matière de droits de propriété intellectuelle, publié le 24 mai 2011[330], suggère que la Commission « va étudier les moyens de créer un cadre permettant en particulier de lutter plus efficacement contre les atteintes aux droits de propriété intellectuelle sur internet »[331]. A cette fin, « toute modification devra viser à réprimer les infractions à leur source »[332] ; il faudra alors « encourager la coopération avec les intermédiaires, notamment les prestataires de services internet »[333]. La Commission indique qu'il ne s'agit pas de « porter atteinte aux objectifs des politiques en matière de haut débit ni aux intérêts des consommateurs »[334]. Elle précise d'ailleurs que ces modifications devront respecter tous les droits consacrés par la Charte des droits fondamentaux de l'Union européenne, à savoir notamment le droit au respect de la vie privée, à la protection des données à caractère personnel, à la liberté d'expression et à l'information[335]. Le commissaire de la DG Marché Intérieur, Michel Barnier, a déclaré, lors de la présentation du plan d'action, que son intention, « s'agissant de l'éradication des

[330] Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Vers un marché unique des droits de propriété intellectuelle, 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*, Bruxelles, le 24.5.2011, COM(2011) 287 final.
[331] *Ibid.*, spéc. pp. 22-23.
[332] *Ibid.*
[333] *Ibid.*
[334] *Ibid.*
[335] *Ibid.*

sites de piratage, est d'agir plus directement à la source, c'est-à-dire vers et avec les fournisseurs d'accès à internet »[336]. Pour l'heure, cette coopération avec les fournisseurs d'accès n'a pas été définie. Mais force est de constater que l'Europe envisage désormais de se tourner vers ces intermédiaires pour lutter efficacement contre les comportements enfreignant le droit d'auteur. La tendance européenne s'oriente donc vers une implication accrue des fournisseurs d'accès à internet, et notamment vers une définition plus claire des procédures de notification et de retrait des contenus illicites.

§1. Le régime de responsabilité

I. Cadre général

A. Objectifs de la directive 2000/31 sur le commerce électronique

Les Etats membres doivent prévoir des sanctions et des voies de recours efficaces contre les atteintes au droit d'auteur et aux droits voisins. Pour ce faire, ils prennent toutes les mesures nécessaires pour veiller à ce que ces sanctions et voies de recours soient appliquées[337]. La directive 2001/29 sur le droit d'auteur dans la société de l'information reconnaît le rôle que les intermédiaires peuvent jouer dans ce contexte, en rappelant que « dans de nombreux cas, ces intermédiaires sont les mieux à même de mettre fin à ces atteintes. Par conséquent, sans préjudice de toute autre sanction ou voie de recours dont ils peuvent se prévaloir, 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 œuvre protégée ou d'un autre objet protégé. »[338] Mais il ne peut pas être demandé n'importe quoi à ces intermédiaires techniques, ceux-ci étant bénéficiaires d'un régime spécial de responsabilité.

Tout le contenu de l'internet est distribué et hébergé par des intermédiaires en ligne, ce qui fait d'eux des acteurs essentiels de la société de l'information, et la part qu'ils y jouent est donc vitale[339]. Étant le passage obligé pour que circulent les informations sur l'internet, il y a bien évidemment un risque que des contenus illicites transitent par les réseaux qu'ils maintiennent, parmi lesquels des contenus qui portent atteinte au droit d'auteur et aux droits voisins. Si l'on applique les règles en la matière, quiconque contribue directement ou indirectement à la violation d'un droit exclusif peut être tenu responsable (ou complice) de contrefaçon[340], ce qui allait bien évidemment poser des problèmes pour les intermédiaires de l'Internet.

---

[336] S. ESTIENNE, « L'Europe relance le débat sur les droits d'auteur à l'heure d'internet », dépêche AFP, 24 mai 2011.
[337] Considérant 58 de la directive 2001/29.
[338] Considérant 59 de la directive 2001/29.
[339] L. EDWARDS, « Role and responsability of Internet intermediaries in the field of copyright and related rights », disponible sur http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf, p.3.
[340] C. ANGELOPOULOS, « Filtage des contenus protégés par le droit d'auteur sur Internet en Europe », *Iris plus*, OEA 2009-4, p. 2.

Trois facteurs ont été pointés par L. EDWARDS pour expliquer le développement du régime de limitation de responsabilité des intermédiaires techniques : l'impraticabilité factuelle et les restrictions légales ; l'équité ; les conséquences économiques indésirables[341]. Premièrement, il est impossible pour les fournisseurs de services de contrôler tout ce qui circule sur leur réseau ou est stocké dans leurs serveurs, sans que cela n'ait un impact important sur la rapidité, la qualité et le coût du service fourni, ainsi que sur la vie privée de leurs clients. Deuxièmement, en tant que fournisseurs de services et non de contenu, il serait inéquitable de les tenir pour responsables. Enfin, la promotion du commerce électronique et de la société de l'information dépend d'une infrastructure de l'internet fiable et en pleine expansion, et il ne serait pas dans l'intérêt du public de tenir les intermédiaires techniques pour responsables de tout ce qui se passe sur le réseau. A l'opposé, les intermédiaires techniques sont les seuls gardiens efficaces de l'internet pouvant prendre le rôle de « nettoyeurs du net »[342]. C'est ce rôle-là que les industries du contenu voudront par la suite leur voir jouer.

C'est en raison de ces considérations que le régime spécial de responsabilité a vu le jour au tout début des années 2000, avec la directive 2000/31 du 8 juin 2000 sur le commerce électronique. Un des objectifs principaux de cette directive était d'ailleurs l'établissement d'un tel régime d'exemption de responsabilité, dans certains cas et au profit de certains intermédiaires, et plus particulièrement au profit des activités de transmission d'informations sur un réseau de communication, de fourniture d'accès à un tel réseau, de stockage sous forme de copie temporaire de données (le *caching*) et d'hébergement[343].

B. Evolution du contexte

Mais ne perdons pas de vue que le système date d'il y a déjà 12 ans, et que le contexte actuel n'est plus le même que celui de l'époque. En effet, depuis l'adoption de cette directive, deux développements clés – en relation avec la protection des droits d'auteur et des droits voisins – ont changé la donne : l'apparition et la croissance du partage et du téléchargement illégal de fichiers contenant des œuvres protégées par le droit d'auteur sur les réseaux, et l'émergence de l'internet participatif, dit « Web 2.0 »[344]. L'internet participatif pose de nouvelles questions qui n'avaient pas été posées lors de l'adoption de la directive, liées à la caractéristique que ces nouveaux sites se présentent sous la forme d'une structure destinée à accueillir des contenus apportés par les internautes eux-mêmes[345]. Comme exemples de sites collaboratifs nous pouvons mentionner les réseaux sociaux (Facebook, Netlog, etc.), les sites de partage de contenus (Youtube, Dailymotion, Picasa, etc.), les plateformes de commerce électronique (eBay, etc.), mais aussi les *wikis*, les blogs, les forums de discussions, *etc.* Les plateformes de partage et de téléchargement illégal, ainsi que l'émergence du Web 2.0 constituent sans conteste un facteur d'aggravation des risques pour les intermédiaires techniques de voir leur responsabilité engagée, la frontière étant difficile à mettre en place entre la responsabilité des internautes qui postent les contenus, et celle des prestataires qui

[341] *Ibid.*, p. 5.
[342] *Ibid.*, p. 6.
[343] E. MONTERO, « Les responsabilités liées au web 2.0 », *R.D.T.I.*, n° 32/2008, p. 364.
[344] L. EDWARDS, *op. cit.*, p. 3.
[345] E. MONTERO, « Les responsabilités liées au web 2.0 », *op. cit.*, p. 365.

ont pour rôle d'accueillir et « mettre en page » ces contenus. Nous verrons *infra* ce que cela implique en matière d'activité d'hébergement, la question de la responsabilité étant pleinement d'actualité ici.

C. Définition des notions clés

Les articles 12 à 15 de cette directive introduisent un régime particulier qui est applicable à certains prestataires de services de la société de l'information qui jouent un rôle d'intermédiaire, Il faut entendre par prestataire d'un service de l'information, « toute personne physique ou morale qui fournit un service de la société de l'information »[346]. Cette notion de prestataire est définie largement et permet donc d'englober un certain nombre d'acteurs dans le régime spécial de responsabilité. Le destinataire de services est quant à lui « toute personne physique ou morale qui, à des fins professionnelles ou non, utilise un service de la société de l'information, notamment pour rechercher une information ou la rendre accessible »[347]. Enfin, un service de la société de l'information peut être défini comme étant « tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services »[348]. Notons qu'en vertu du considérant 18 de la directive 2000/31, le service fourni peut être gratuit pour ceux qui le reçoivent, comme par exemple les services fournissant des outils permettant la recherche de données, sans que cela n'enlève la qualification de fournisseur de service de la société de l'information au prestataire de tels services, dans la mesure où ces services représentent une activité économique. Nous pensons par exemple au service de moteur de recherche de Google, gratuit pour l'utilisateur, mais qui peut être considéré comme presté normalement contre rémunération étant donnés les gains indirects que lui rapporte la publicité entourant ledit service[349]. Mais selon la Cour de justice dans son arrêt *Google*, « la seule circonstance que le service de référencement soit payant (…) ne saurait avoir pour effet de priver Google des dérogations en matière de responsabilité prévues par la directive 2000/31 »[350]. Le considérant 18 précise également que même si les services de télévision et de radiodiffusion au sens traditionnel du terme (directive TSF 89/552) n'entrent pas dans le champ d'application de la directive, en revanche, tel est bien le cas des services de vidéo à la demande, qui sont des services transmis point à point. Sont hors du champ de la directive les activités de jeux d'argent[351], ainsi que tout le domaine de la vie privée et des traitements de données à caractère personnel – déjà régi par la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel[352].

[346] Article 2, b) de la directive 2000/31.
[347] Article 2, d) de la directive 2000/31.
[348] Article 1(2) de la directive 98/48.
[349] Nous verrons *infra* l'interprétation de la C.J.U.E. à ce sujet.
[350] Arrêt *Google*, § 116.
[351] Considérant 16 de la directive 2000/31.
[352] Considérant 14 de la directive 2000/31.

En Belgique, c'est la loi du 11 mars 2003 sur les services de la société de l'information[353] qui consacre dans son chapitre IV un régime de responsabilité allégée et une définition des obligation à charge des prestataires intermédiaire, loi qui est une transposition fidèle de la directive 2000/31.

Il ne s'agit pas ici de créer un régime d'exonération de responsabilité totale des intermédiaires visés par la directive, mais plutôt un système d'exonération conditionnelle qui fixe les conditions auxquelles la responsabilité des intermédiaires pourra ou non être mise en cause ainsi que les obligations particulières auxquelles ils pourront être soumis.

II. Règles pour les différentes fonctions (simple transport, hébergement, cache)

C'est donc une approche horizontale qui a été prise en la matière au niveau européen, mais au lieu de conférer une immunité totale de responsabilité en toutes circonstances à certains acteurs bien précis, c'est plutôt vers une démarche basée sur les différentes fonctions des intermédiaires que l'on s'est tourné. La loi vise les intermédiaires qui exercent une activité de simple transport, de fourniture d'accès, de stockage sous forme de copie temporaire ou d'hébergement de contenu ; rien n'est donc explicitement prévu pour d'autres intermédiaires comme les moteurs de recherche par exemple qui sont des acteurs importants dans la lutte contre le piratage en ligne. Nous verrons quelle est la position de la Cour de justice en ce qui concerne la définition des intermédiaires.

A. Les fournisseurs d'accès à Internet et simples transporteurs

Le fournisseur d'accès au réseau, ainsi que le simple transporteur, bénéficie d'un régime d'exonération de responsabilité sous certaines conditions. L'article 12 de la directive 2000/31 sur le commerce électronique envisage la responsabilité du fournisseur d'accès dans les termes qui suivent :

> « 1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire:
>
> a) ne soit pas à l'origine de la transmission;
>
> b) ne sélectionne pas le destinataire de la transmission et
>
> c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission ».

La loi belge de transposition du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, en son article 18, reprend dans les mêmes termes la disposition de l'article

[353] Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003 (telle que mise à jour en 2005), p. 12963.

12 de la directive. Ainsi un prestataire de service qui se contente de transmettre des informations fournies par un destinataire ou de fournir un accès au réseau de communication, c'est-à-dire un fournisseur d'accès, ne voit pas sa responsabilité engagée dès lors que les trois conditions cumulatives posées par les textes sont satisfaites[354]. Dans le cadre des échanges illégaux d'œuvres sur les réseaux *peer-to-peer* ou de téléchargements directs ou *streaming*, le fournisseur d'accès n'est en principe pas à l'origine de la circulation de ces œuvres, ne sélectionne pas les internautes se livrant à ces pratiques et ne sélectionne ni ne modifie les œuvres objets de cette transmission. Ce régime d'exonération ne joue plus si le prestataire outrepasse ses simples activités de transport – par exemple lorsqu'il « collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales »[355] ; il ne pourra plus bénéficier du régime de dérogation prévu par la directive. Par exemple, si le fournisseur d'accès mettait lui-même des œuvres sur le réseau pour des échanges en *peer-to-peer*, il ne pourrait plus bénéficier de l'exonération. Ce sont les seuls intermédiaires qui bénéficient d'une exonération totale de responsabilité, tant qu'ils ne sont pas à l'origine des données transmises, ni ne les modifient[356].

Si certains estiment que l'immunité des fournisseurs d'accès à internet devrait être révisée[357], les conclusions de l'avocat général rendues dans l'affaire *Scarlet* le 14 avril 2011, ainsi que l'arrêt lui-même, ne vont pas dans le sens d'une interprétation évolutive de la directive qui prendrait en compte l'évolution de la technologie et des usages d'internet[358]. Comme le souligne la Commission dans sa communication sur la confiance dans le marché unique numérique du commerce électronique, une révision de la directive 2000/31 n'est pas à l'ordre du jour[359].

[354] Voir également le considérant 42 : « 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 », et le considérant n° 43 : « Un prestataire de services peut bénéficier de dérogations pour le "simple transport" et pour la forme de stockage dite "caching" lorsqu'il n'est impliqué en aucune manière dans l'information transmise. Cela suppose, entre autres, qu'il ne modifie pas l'information qu'il transmet. Cette exigence ne couvre pas les manipulations à caractère technique qui ont lieu au cours de la transmission, car ces dernières n'altèrent pas l'intégrité de l'information contenue dans la transmission ».

[355] Cf. le considérant 44 : « Un prestataire de services qui collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales va au-delà des activités de "simple transport" ou de "caching" et, dès lors, il ne peut pas bénéficier des dérogations en matière de responsabilité prévues pour ce type d'activité ».

[356] S. DUSOLLIER, « Responsabilité des intermédiaires de l'internet : un équilibre compromis ? », *R.D.T.I.*, n° 29/2007, p. 269.

[357] R. CLARK, « Sharing out online liability : sharing files, sharing risks and targeting IPSs », *in* A. STROWEL (ED.), *Peer-to-peer file sharing and secondary liability in copyright law*, Edward Elgar, 2009, pp. 196-228, spéc. p. 222 et s.

[358] Conclusions de l'avocat général, M. Pedro Cruz Villalón, présentées le 14 avril 2011, *Scarlet Extended c. Sabam*, C-70/10, spéc. §112.

[359] Communication de la Commission, 11 janvier 2012, « Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne », p. 5.

B. Les hébergeurs

Si les activités de simple transport sont assez évidentes à identifier et dès lors à catégoriser, la fonction d'hébergeur est nettement plus controversée dans le régime prévu par la directive, ceux-ci hébergeant ou stockant, de manière non temporaire, des contenus appartenant à des tiers. Héberger signifie donc stocker, à la demande des utilisateurs du service, des informations qui proviennent de ces derniers.

L'hébergeur sera exonéré de toute responsabilité quant au contenu des informations qu'il stocke s'il répond à certaines conditions. A cet égard, l'article 14 de la directive prévoit que :

> « 1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que:
>
> a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ; ou
>
> b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible. »

Ce qui est donc visé ici pour que le prestataire ne voie pas sa responsabilité engagée est son absence de connaissance de l'activité illicite qui se produit par le biais de son service :

- soit il sera exonéré de responsabilité s'il n'a pas eu connaissance effective de l'activité ou de l'information illicite
- soit, dans le cadre d'une action en responsabilité civile, il sera exonéré de responsabilité à condition qu'il n'ait pas connaissance de faits ou de circonstances laissant apparaître le caractère illicite de l'activité ou de l'information

Dans le deuxième cas de figure n'apparaît plus la notion de connaissance effective, et intervient la notion d'illicéité apparente, ce qui a pour conséquence que sa responsabilité sera plus facilement retenue dans le cadre d'une procédure en dommages et intérêts[360].

Pour pouvoir bénéficier de l'exonération de responsabilité, l'hébergeur doit, dès qu'il prend effectivement connaissance du caractère illicite des activités – typiquement lorsqu'il aura reçu une notification dans ce sens ou qu'une décision de justice aura fait apparaître, agir promptement pour retirer les informations concernées ou rendre l'accès à celles-ci impossible[361]. Lorsqu'il procède à leur retrait ou lorsque l'accès est rendu impossible à un contenu illicite, cela doit bien évidemment être fait en respectant le principe de la liberté d'expression[362]. C'est ce que l'on appelle la procédure de *notice and takedown* que nous analyserons *infra.* En Belgique, en vertu de l'article 20, § 3 de la loi du 11 mars 2003 sur la société de l'information, l'hébergeur doit communiquer au Procureur du Roi les

[360] J. FELDS, « Forums de discussion : espaces de liberté sous haute responsabilité », *R.D.T.I.*, n° 38/2010, p. 113.
[361] Considérant 46 de la directive 2000/31.
[362] *Idem*.

activités ou informations illicites dont il a effectivement connaissance s'il veut bénéficier de l'exonération de responsabilité.

Une fois qualifié d'hébergeur, un prestataire de service, même autre que celui qui héberge un site au sens technique, doit encore ne jouer qu'un rôle entièrement passif par rapport au contenu ou à l'activité hébergée s'il veut pouvoir bénéficier de l'exonération de responsabilité. Il faut également tenir compte de l'indépendance du fournisseur de contenu à l'égard du prestataire. Il ne peut agir sous l'autorité ou le contrôle de ce dernier, le contrôle étant celui exercé par le prestataire d'hébergement sur le destinataire du service et non sur les informations elles-mêmes[363].

Il est question d'une conception distributive de l'activité d'hébergeur, « d'une qualification mixte qui consiste à distinguer le régime de responsabilité applicable en fonction de la nature de l'activité litigieuse »[364]. Le tribunal de commerce de Bruxelles a déjà jugé qu'un prestataire pouvait bénéficier du régime de la directive pour ses activités d'hébergeur quelles que soient les autres activités exercées par ce même intermédiaire[365]. Nous aurons l'occasion de nous pencher plus attentivement sur cette approche fonctionnelle de l'activité d'hébergement.

De manière synthétique, sont notamment compris dans cette notion, l'hébergement classique[366], les services de place de marché en ligne[367], les plates-formes participatives[368], le stockage de contenus sur le *cloud*, les réseaux sociaux, les forums de discussion.

C. Le *caching*

Les activités de *caching* n'étant pas pertinentes pour le présent rapport, nous ne nous y attarderons que brièvement.

L'article 13, 1. de la directive 2000/31 prévoit que :

> « Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que:
>
> a) le prestataire ne modifie pas l'information;
>
> b) le prestataire se conforme aux conditions d'accès à l'information;
>
> c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises;

[363] Commentaire article par article de la proposition de directive du Parlement et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, présentée par la Commission le 18 novembre 1998, COM (1998), 586 final, p. 31.
[364] E. MONTERO, « Chronique de jurisprudence 2002-2008 : Droit du commerce électronique », *R.D.T.I.*, n° 32/2008, p. 369.
[365] Comm. Bruxelles, 31 juillet 2008, *R.D.T.I.*, 33/2008, p. 521.
[366] Directive 2000/31.
[367] Arrêt *eBay*, § 110.
[368] Arrêt *Netlog*, § 27.

d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information et

e) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible. »

Cette activité est différente de celle de simple transport, ce qui implique que les conditions dans lesquelles la responsabilité pourra ou non être retenue sont différentes. Pourvu que les conditions de l'article 13 soient remplies, le prestataire ne sera pas responsable pour l'activité consistant en un stockage automatique, intermédiaire et temporaire des informations fournies par un destinataire du service fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande.

D. Conclusion : une approche fonctionnelle

Les régimes de responsabilité ne sont pas fondés sur la notion d'acteur – fournisseur d'accès, hébergeur ou prestataire d'un service de *caching* – mais plutôt sur le type d'activité exercée[369] : « La distinction en ce qui concerne la responsabilité n'est pas fondée sur le type d'opérateur, mais sur le type d'activité exercé. Le fait qu'un prestataire remplit les conditions pour être exonéré de responsabilité pour une activité donnée ne l'exonère pas de sa responsabilité pour toutes ses autres activités »[370]. Un même prestataire peut donc exercer plusieurs fonctions. Cela a été confirmé par la Commission européenne qui affirme que le régime de responsabilité de la directive s'applique « à certaines activités clairement délimitées de prestataires intermédiaires, plutôt qu'à des catégories de prestataires de services ou à des types d'information »[371]. Outre cette approche par fonctions et non par acteurs, il faut tenir compte du comportement du prestataire lors de l'exercice de l'activité technique rentrant dans le champ du régime d'exonération, dans la mesure où un prestataire ne pourra pas s'abriter derrière cette approche fonctionnelle s'il a influencé le contenu de manière évidente[372].

Concernant plus spécifiquement la notion d'hébergeur, le prestataire le plus influencé par l'avènement d'un internet participatif, la définition large de la directive permet tout à fait la conception d'un stockage des contenus à la demande de tiers, un stockage direct de données sur un serveur, ainsi que l'activité consistant en l'offre d'une structure d'accueil des données mises en ligne sur le site par les utilisateurs[373]. Cette approche fonctionnelle permet l'application du régime de

[369] E. MONTERO, « Les responsabilités liées au web 2.0 », *op. cit.,* p. 368.
[370] Commentaire article par article, *op.cit.,* p. 28.
[371] Premier rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen sur l'application de la directive 2000/31 sur le commerce électronique, 21 novembre 2003, COM(2003) 702 final, p. 13.
[372] E. MONTERO, « La responsabilité des prestataires intermédiaires sur les réseaux », *op. cit.*, p. 276.
[373] E. MONTERO, « Les responsabilités liées au web 2.0 », *op. cit.,* pp. 371 et 372.

responsabilité aux titulaires d'un site de partage de contenus, d'un réseau social, d'un blog, d'un *wiki*, d'un site d'enchères, *etc.*, ce qui est confirmé par la Cour de justice par les critères de neutralité ou de passivité définis dans les arrêts *Google* et *eBay*.

Les critères en la matière ne sont pas toujours aisément identifiables, les auteurs de doctrine et les cours et tribunaux ne s'accordant quant à leur détermination : « tout devient cas d'espèce, à apprécier soigneusement en fonction du service fourni et du rôle exact joué par le prestataire à l'égard des contenus stockés »[374]. Les récentes affaires en la matière devant la Cour de justice sont précieuses pour aider les juridictions nationales à appliquer de manière juste et sans ambiguïté les critères de la directive.

III. Interprétation par la Cour de justice de l'Union européenne

Sur cette question de la responsabilité des intermédiaires, la Cour de justice a rendu des arrêts importants ces dernières années, dont l'arrêt du 23 mars 2010 dans l'affaire *Google France SARL, Google Inc. c. Louis Vuitton Malletier SA* (ci-après « arrêt *Google* »), et celui du 12 juillet 2011 dans l'affaire *L'Oréal et autres c. eBay* (ci-après « arrêt *eBay* »). Nous verrons que les derniers arrêts en la matière, les arrêts *Scarlet Extended c. Sabam* du 24 novembre 2011 (ci-après « arrêt *Scarlet* ») et *Netlog c. Sabam* du 16 février 2012 (ci-après « arrêt *Netlog* ») traitent également de la question de la responsabilité des intermédiaires techniques, mais plutôt sous l'angle des obligations qui peuvent leur être imposées, des injonctions judiciaires qui peuvent être ordonnées à leur encontre, ainsi que de l'interdiction d'imposition d'une obligation générale de surveillance[375].

A. Notion d'intermédiaire

Dans son arrêt *Google*[376], la Cour de justice a conclu à l'applicabilité de l'article 14 de la directive 2000/31 sur le commerce électronique qui s'applique aux hébergeurs au service de référencement payant sur Internet (quant à l'hébergement d'annonces publicitaires), et parvient à la même conclusion dans son arrêt *eBay* en ce qui concerne les offres de vente postées sur la plateforme d'enchères en ligne. Mais ces services ne bénéficient pas en toutes circonstances de cette exonération de responsabilité : ils ne sont plus considérés comme simples prestataires intermédiaires si « au lieu de se limiter à une fourniture neutre (du service) au moyen d'un traitement purement technique et automatique des données fournies par ses clients, ils jouent un rôle actif de nature à lui confier une connaissance ou un contrôle de ces données »[377]. C'est toujours un raisonnement fonctionnel qui doit guider l'interprétation de la directive 2000/31, ce qui est à l'avantage des sites communautaires et participatifs, destinés à accueillir les contenus apportés par

[374] *Ibidem*, p. 379.
[375] D. GOBERT et J. JOURET, « L'arrêt *Scarlet* contre *Sabam* : la consécration d'un juste équilibre du rôle respectif de chaque acteur dans la lutte contre les échanges illicites d'œuvres protégées sur Internet »,*R.D.T.I.*, n° 46/2012, p. 35.
[376] C.J.U.E., 23 mars 2010, *Google France et Google*, aff. jointes C-236/08 à C_238/08, *Rec.*, p. I-2417.
[377] Arrêt *Google*, §§ 114 et 120 ; arrêt *eBay*, §§ 111 à 113.

les internautes eux-mêmes[378]. Une telle interprétation de la Cour permet donc de mettre le droit à jour, de le rendre compatible avec ce que l'on appelle le « Web 2.0 ». Elle est en outre conforme à l'exposé des motifs de la proposition de directive sur le commerce électronique et avec la lettre de l'article 14 qui dispose que « les prestataires de services de la société de l'information jouent un rôle d'intermédiaires lorsqu'ils transmettent ou hébergent des informations émanant de tiers (fournies par les utilisateurs du service) »[379], et que « les activités des intermédiaires en ligne se caractérisent par le fait que les informations sont fournies par les destinataires du service et qu'elles sont transmises ou stockées à la demande des destinataires du service »[380].

B. Le critère de passivité

En matière d'activité d'hébergement, la condition de neutralité à l'égard des données stockées est essentielle pour pouvoir bénéficier de l'exonération de responsabilité. En effet, l'article 14 s'applique à un prestataire de service « lorsque celui-ci n'a pas joué un rôle actif qui lui permette d'avoir une connaissance ou un contrôle des données stockées »[381]. Dès qu'il y a sélection ou orientation du contenu stocké, il n'y a pas possibilité de bénéficier de l'exonération, ce qui est le cas d'un titulaire de blog, ou encore, et cela est intéressant pour notre étude, « le gestionnaire d'un site de partage de contenus qui provoquerait à télécharger des œuvres piratées »[382], car il y a bien là un rôle actif qui est joué. Mais il est important que le critère de connaissance s'applique à un contenu concret car il serait impensable de refuser à un intermédiaire technique le bénéfice de l'exonération de responsabilité « sous prétexte qu'il peut soupçonner que des destinataires de son service de stockage fournissent des données illicites »[383]. La connaissance devrait seulement être présumée « dans les cas où le prestataire est informé du caractère illicite d'un contenu soit par une décision judiciaire constatant l'infraction, soit par une notification, dûment étayée, que lui aurait adressée un titulaire de droits »[384].

La Cour de justice a estimé que « le simple fait que l'exploitant d'une place de marché en ligne stocke sur son serveur des offres à la vente, fixe les modalités de son service, est rémunéré pour celui-ci et donne des renseignements d'ordre général à ses clients ne constitue pas un rôle actif de nature à le priver du bénéfice du régime dérogatoire de responsabilité »[385]. En matière de service de référencement, « (…) la seule circonstance que le service de référencement soit payant, que Google fixe les modalités de rémunération, ou encore qu'elle donne des renseignements d'ordre général à

[378] S. DUSOLLIER et E. MONTERO, « Des enchères et des fleurs (…) », *op. cit.* , p. 182.
[379] Exposé des motifs de la proposition de directive du Parlement et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, présentée par la Commission le 18 novembre 1998, COM (1998), 586 final, p. 11.
[380] Commentaire article par article de la proposition de directive du Parlement et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, *op. cit.*, p. 28.
[381] S. DUSOLLIER et E. MONTERO, « Des enchères et des fleurs (…) », *op. cit.*, p. 183.
[382] *Ibidem*, p. 183 et 184.
[383] *Ibidem,* p. 184.
[384] *Ibidem*, p. 185.
[385] Arrêt *Google*, § 115.

ses clients, ne saurait avoir pour effet de priver Google des dérogations en matière de responsabilité prévues par la directive 2000/31 »[386].

Il ne faut donc pas qu'il y ait promotion active ni orientation de la part du prestataire s'il veut conserver le bénéfice de l'exemption de responsabilité instituée à son profit, qu'il ne prête pas son assistance. Comme cela a déjà été signalé *supra*, il faut également tenir compte de l'indépendance du fournisseur de contenu à l'égard du prestataire qui ne peut agir sous l'autorité ou le contrôle de ce dernier : « (…) Google procède, à l'aide des logiciels qu'elle a développés, à un traitement des données introduites par des annonceurs et qu'il en résulte un affichage des annonces sous des conditions dont Google a la maîtrise. Ainsi, Google détermine l'ordre d'affichage en fonction, notamment, de la rémunération payée par les annonceurs. »

La Cour de justice dans son arrêt *Google* avait interprété le critère de passivité au regard du considérant 42 de la directive 2000/31, alors qu'il ne concerne pas l'activité d'hébergement mais celle de *caching*[387]. L'avocat général dans ses conclusions de l'affaire *eBay* a estimé que le considérant 42 ne visait pas l'activité d'hébergement et que l'on ne pouvait en déduire le critère de passivité pour cet intermédiaire[388]. La Cour dans son arrêt *eBay* ne s'y réfère plus.

§2. Une obligation d'instaurer une procédure de notification et de retrait des contenus illicites

Dans un rapport sur la responsabilité des intermédiaires en ligne, l'OCDE identifie quatre différents modèles pour la coopération des intermédiaires techniques[389] : « notice and takedown », « notice and notice », « notice and disconnection » (ou réponse graduée), et le filtrage. Nous analyserons ici ce que l'on appelle la procédure de *notice and takedown*, mécanisme qui vise à faire cesser un dommage actuel. Nous pouvons déjà relever à ce stade qu'en pratique il existe une multitude de procédures différentes en raison d'un manque d'harmonisation et qu'il n'est pas aisé ni pour les prestataires techniques, ni pour les victimes de déterminer laquelle s'applique, et de quelle manière[390]. Des systèmes ont donc été mis en place pour lutter contre les activités illicites des abonnés, y compris les activités portant atteinte aux droits de propriété intellectuelle.

I. Cadre général de la procédure de notification et de retrait

Comme nous l'avons vu *supra*, pour pouvoir bénéficier du régime de l'exonération, certaines conditions doivent être respectées. Parmi celles-ci, si l'hébergeur ou le prestataire de service de

[386] *Ibidem*, § 116.
[387] *Ibidem*, § 113.
[388] Conclusions de l'avocat général dans l'affaire *eBay*, §§ 139 à 142.
[389] OCDE, « The legal responsibilities of the Internet intermediaries, their business practices and self - or co-regulatory codes », in The role of internet intermediaries in advancing public policy objectives, 2010.
[390] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services », SEC(2011) 1641, p.25.

caching a une connaissance effective dans le cadre d'une procédure pénale du caractère illicite de l'activité ou de l'information – ou de circonstances laissant apparaître son caractère illicite – dans le cadre d'une procédure civile, il ne sera exonéré de sa responsabilité que s'il agit promptement pour retirer ces éléments ou les rendre inaccessibles. Nous verrons *infra* ce que cette obligation d'agir promptement implique comme questions et problèmes éventuels. La législation européenne prévoit en de nombreux endroits cette procédure de notification et de retrait : les articles 14, 3, *in fine*, et 13, 1 ainsi que les considérants 40, 41 et 46 de la directive 2000/31 sur le commerce électronique ; l'article 11 de la directive 2004/48 sur la propriété intellectuelle et l'article 8 de la directive 2001/29 sur le droit d'auteur ; les articles 19 et 20, § 1er de la loi du 11 mars 2003 sur la société de l'information. Selon cette procédure, le prestataire technique a l'obligation de répondre à une demande de suppression d'un contenu qui a déjà fait l'objet d'une transmission ou d'un stockage par le biais de son service, et donc à « une obligation de cessation d'un dommage actuel ».

Si le prestataire a une connaissance effective de l'activité ou de l'information illicite, reconnue comme telle par un juge, il est tenu de retirer le contenu promptement s'il ne veut pas être responsable. Si par contre les faits et circonstances révèlent au prestataire une illicéité apparente, il sera dans l'obligation d'agir, et cela sans attendre une notification ni la prise d'une décision sur la réalité de ce caractère illicite. Cette obligation de retrait sans notification préalable pose des questions lorsqu'elle est mise en parallèle à l'interdiction d'imposer une obligation générale de surveillance aux intermédiaires techniques, interdiction prévue en ces termes par l'article 15, 1., de la directive 2000/31 : « 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 ». Cette obligation n'interdit pas qu'une telle surveillance soit mise en place volontairement par un prestataire. Mais a-t-il intérêt à procéder lui-même à une telle recherche ? Les risques de voir leur responsabilité engagée en cas d'erreur et d'être poursuivi par le fournisseur de contenu pour non-exécution du contrat sont élevés. Une obligation pour un prestataire intermédiaire de procéder d'initiative ajouterait une condition au texte qui n'est pas prévue.

Le bénéfice de ce régime est soumis au respect d'une certaine neutralité vis-à-vis des contenus diffusés. En revanche, dès qu'ils reçoivent une mise en demeure d'un ayant droit ou d'un plaignant, les hébergeurs ont l'obligation de retirer promptement les contenus litigieux. Ni la directive, ni la loi belge ne précisent le « seuil de connaissance » requis dans le chef de l'hébergeur pour justifier son obligation d'intervention, et aucune procédure de *notice and takedown* n'est prévue. Certains pays ont prévu une procédure plus complète de *notice and takedown*, contenant un certain nombre d'éléments qui permettent de pallier le manque de précision dans sa mouture européenne.

En France, la loi pour la confiance dans l'économie numérique (ci-après « LCEN ») prévoit des formalités de notification dotant les hébergeurs d'outils leur permettant de distinguer le licite de l'illicite. L'article 6.1.5 de la LCEN impose un certain nombre d'informations à inclure dans la notification : « la description des faits litigieux et leur localisation précise », ainsi que les « motifs [de droit] pour lesquels le contenu doit être retiré »[391]. Nous pouvons relever que la mention dans la notification des dispositions légales justifiant le retrait peut s'avérer délicate à fournir par un non

[391] Un certain nombre de décisions ont débouté des demandeurs pour défaut du respect des formalités prévues dans la procédure de notification.

juriste, ce qui complique une procédure qui se veut facile à appliquer. L'intervention du juge sera nécessaire pour confirmer la connaissance effective par le prestataire d'un contenu illicite qui serait dès lors tenu de le retirer, cette intervention n'étant pas nécessaire lorsque le contenu est manifestement illicite[392].

Aux Etats-Unis, une procédure complète de notification est prévue dans le *Digital Millennium Copyright Act* (ci-après « DMCA »), qui énumère en son article 512 (c) (3) les éléments que la notification doit contenir pour être recevable. En plus de devoir prendre la forme d'une communication écrite signée par la personne concernée (l'ayant droit ou la personne autorisée par lui à agir), et d'être adressée à l'agent désigné par le prestataire, les éléments suivants doivent y être intégrés[393] :

- l'identification de l'œuvre protégée à laquelle il est prétendument porté atteinte
- l'identification du contenu prétendument illicite ainsi qu'une information raisonnablement suffisante pour permettre au prestataire de localiser ledit contenu
- une information raisonnable suffisante pour permettre au prestataire de contacter le plaignant tels qu'une adresse, un numéro de téléphone ou encore une adresse de messagerie électronique
- une déclaration selon laquelle le plaignant croit en toute bonne foi que l'usage de l'œuvre n'est pas autorisé par le titulaire du droit d'auteur, par son agent ou par la loi
- une déclaration que les informations contenues dans la notification sont exactes, et sous peine de parjure, que le plaignant est autorisé à agir au nom du titulaire du droit d'auteur

La sanction du non-respect de ces formalités obligatoires sera simplement l'absence de prise en considération de la notification. Elle ne sera donc pas prise en compte lors de la détermination de la connaissance des faits et circonstances par le prestataire de services. Si une procédure de *notice and takedown* est mise en place au niveau belge, il serait intéressant de se baser sur ces aspects de la procédure du DMCA.

Le DMCA prévoit également une procédure de *counter-notice and put back* qui prévoit le processus à suivre par l'hébergeur lors du retrait des contenus qui lui ont été notifiés : les notifications de retrait doivent être transmises au fournisseur de contenu qui peut contester cette demande, et en cas de différend, les parties iront devant le juge. Le modèle américain pose ici problème en ce qu'il oblige le prestataire à retirer le contenu ou à le rendre inaccessible, et c'est seulement après qu'il doit notifier au fournisseur du contenu cette action, qui a alors la possibilité – mais non l'obligation – de contester la légitimité du retrait du contenu par le biais d'une contre-notification. Ce modèle n'est pas complètement respectueux de la liberté d'expression ni du droit à un procès équitable, en raison du retrait automatique des contenus avant toute possibilité pour leur fournisseur de se défendre. Pour cela, un système de *notice and takedown* qui prévoirait la possibilité pour les éditeurs de contenus de réagir à la décision de retrait *avant* qu'il n'ait lieu serait moins attentatoire aux droits fondamentaux. C'est ce type de mécanisme qui a été mis en place en Espagne par la *Ley Sinde*[394]. De plus, prévoir une procédure de contre-notification avec remise du contenu en ligne est une nécessité minimale pour garantir les droits de l'éditeur du contenu. Ce mécanisme de contre-notification permet d'éviter les retraits arbitraires.

[392] L. THOUMYRE, « Comment les hébergeurs français sont devenus juges du manifestement illicite », 28/07/2004, www.juriscom.net.
[393] Article 512, c), 3) , A) du *Digital Economy Act*.
[394] Voir deuxième chapitre du rapport.

Il est également nécessaire de prévoir une sanction pour les cas de dénonciations abusives de contenus illicites de la part des ayants droit, ce qui consiste en un garde-fou nécessaire pour préserver les droits de l'éditeur du contenu et du prestataire. La LCEN prévoit dans son article 6.1.4 une sanction « d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende » pour les dénonciations abusives. Le DMCA prévoit comme sanction la responsabilité de la personne ayant fait de fausses allégations pour tous les préjudices subis par l'éditeur de contenu qui découlent de ces allégations. Prévoir des sanctions en cas de fausse contre-notification peut également s'avérer utile pour prévenir les abus.

Aux Etats-Unis, lorsqu'un fournisseur de service de la société de l'information procède à un retrait de bonne foi, il est protégé de toute responsabilité. On ne retrouve pas une telle règle dans le droit européen, or cela pourrait avoir un effet positif en termes de facilitation de la procédure de notification et de retrait en Belgique. Mais cette éventualité doit immédiatement être contrebalancée par un constat inquiétant à propos de cette procédure : il a été relevé que la procédure de notification et de retrait peut produire un effet dommageable (*chilling effect*) sur la liberté d'expression et conduire à une forme de censure privée. Le piège est que les intermédiaires retirent ou bloquent trop facilement les contenus qui leur sont notifiés, sans un examen préalable, dans le seul but d'éviter un litige[395]. A cet égard, les chercheurs de l'université d'Oxford ont conclu que « (…) the incentive to take down content from the Internet is higher than the potential costs of not taking it down »[396].

II. La connaissance effective

Il est nécessaire de bien comprendre la portée de cette « connaissance effective de l'activité ou de l'information illicite », qui porte sur un contenu spécifique, et non sur la connaissance de la simple *éventualité* que des informations illicites puissent être mises en ligne au niveau du prestataire. Dans l'affaire *eBay* du 12 juillet 2011, s'est posée la question de savoir quelles étaient les conditions pour pouvoir considérer qu'*eBay* avait connaissance de l'illicéité des contenus transmis par l'intermédiaire de son service. Un hébergeur ne peut être exonéré de toute responsabilité pour les données à caractère illégal qu'il a stockées qu'à la condition qu'il n'ait pas eu effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, qu'il n'ait pas eu connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicites est apparente. Est donc visée toute situation dans laquelle le prestataire concerné prend connaissance, d'une façon ou d'une autre du contenu illicite[397], et la Cour donne comme exemple « la situation dans laquelle l'exploitant d'une place de marché en ligne découvre l'existence d'une activité ou d'une information illicite à la suite d'un examen effectué de sa propre initiative, ainsi que celle dans laquelle l'existence d'une telle activité ou d'une telle information lui est notifiée »[398].

[395] L. EDWARDS, *op. cit.* p. 11.
[396] C. AHLERT, C. MARSDEN and C. YUNG, « How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation », disponible sur http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf
[397] C. SMITS et J. LIGOT, « Arrêt L'Oréal : clarifications sur le cadre légal des activités et des responsabilités des hébergeurs de sites internet », *J.D.E.*, 2010, p. 295.
[398] Arrêt *L'Oréal*, § 122.

Mais une notification ne saurait automatiquement écarter le bénéfice du régime de responsabilité des prestataires. S'agissant des circonstances qui devraient être ajoutées à la notification pour que l'hébergeur ne puisse pas bénéficier de l'exemption de responsabilité[399], la Cour précise qu' « il suffit, pour que le prestataire d'un service de la société de l'information soit privé du bénéfice de l'exonération de responsabilité prévue à l'article 14 de la directive 2000/31, qu'il ait eu une connaissance de faits ou de circonstances sur la base desquels un opérateur économique diligent aurait dû constater l'illicéité en cause et agir conformément au paragraphe 1, sous b), dudit article 14 »[400]. La Cour de justice confirme ici que lorsque l'illicéité est apparente, le prestataire devra procéder au retrait du contenu sans passage devant un juge, et seulement dans ce cas.

Notons enfin que la tendance ces dernières années est au développement de l'autorégulation en la matière, les accords volontaires étant d'ailleurs encouragés par la directive 2000/31 elle-même, en son considérant n° 40. Les Pays-Bas et la France ont mis en place de tels codes sur une base volontaire, et notamment en matière de contrefaçon du droit d'auteur sur internet, ainsi qu'au niveau européen.

III. Obligation d'agir promptement

Des problèmes se posent quant à l'application de cette notion, aucune définition n'étant donnée dans les textes européens pour l'interpréter. Le considérant 46 de la directive affirme uniquement que le retrait doit être réalisé « dans le respect du principe de la liberté d'expression et des procédures établies à cet effet au niveau national » et que « la présente directive n'affecte pas la possibilité qu'ont les États membres de définir des exigences spécifiques auxquelles il doit être satisfait promptement avant de retirer des informations ou d'en rendre l'accès impossible ». Rien donc sur les critères de cette promptitude exigée.

De nombreux problèmes peuvent se poser si le prestataire procède à un retrait trop rapide d'un contenu notifié comme illicite, sans un examen préalable du bien-fondé de la requête. Cela peut être préjudiciable à la fois pour le fournisseur de contenu qui peut subir un dommage résultant de ce retrait, mais également pour le prestataire de service qui peut voir sa responsabilité engagée pour non-exécution du contrat qui le lie au fournisseur du contenu. Rien dans les textes européens ne prévoit une exonération de responsabilité pour un prestataire ayant retiré un contenu qui se révèlerait finalement tout à fait légitime, contrairement aux Etats-Unis (DMCA).

Un autre écueil qui peut être pointé est celui du risque d'un retrait tardif si la notification est envoyée dans le mauvais service de l'entreprise qualifiée d'intermédiaire. En effet, le temps que la demande soit traitée, envoyée dans le bon service, qu'il soit procédé à un examen de la pertinence de la demande, un long moment peut s'écouler avant qu'un contenu ne soit retiré, ce qui peut porter préjudice à l'ayant droit. Mais si tout a été mis en œuvre par l'intermédiaire, peut-on vraiment estimer qu'il n'a pas agi promptement ? Pour peu que rien sur le site ou la plateforme par exemple ne soit prévu pour signaler un contenu illicite, telle une bannière ou le renvoi vers un lien, ce genre de situations sera légion. La généralisation de ce type de systèmes sur les sites et plateformes

[399] C. SMITS et J. LIGOT, « Arrêt L'Oréal (…) », *op. cit.*, p. 295.
[400] Arrêt *L'Oréal*, § 120.

pourrait être une bonne façon de recevoir les plaintes des ayants droit, couplée alors à une exonération de responsabilité à l'américaine avec sanctions possibles en cas de fausse notification.

En attendant une possible clarification des critères, les cours et tribunaux devront juger de la promptitude au cas par cas : « une fois la connaissance démontrée dans le chef du prestataire, les cours et tribunaux peuvent aussi apprécier plus ou moins sévèrement la promptitude avec laquelle il a procédé au retrait du contenu illicite ou rendu impossible l'accès à celui-ci »[401]. La Commission, dans son *working paper* sur le commerce électronique, a relevé que les fournisseurs de services de la société de l'information craignent que si l'on définit le terme « promptement », cela augmente la pression sur leurs épaules et les pousse à agir trop rapidement, sans une évaluation préalable suffisante[402]. Certains Etats membres ont spécifié le délai à respecter par les prestataires pour procéder au retrait d'un contenu illicite dont ils auraient connaissance : en Finlande, un prestataire doit agir immédiatement ; la Hongrie a prévu un délai d'action de 12 heures ; l'Espagne, un délai de 72 heures[403]. Nous pensons qu'il serait plus sage de ne pas prévoir de critères stricts pour cette notion de promptitude, la matière de la propriété intellectuelle comportant trop d'exceptions, qu'il faut donc plutôt s'en tenir à une application au cas par cas. Pour des matières plus sensibles, comme la pédopornographie, une définition claire des délais à respecter pourrait par contre s'avérer nécessaire.

IV. Pratiques des intermédiaires techniques

A titre d'exemple, nous pouvons citer les pratiques de Youtube, qui s'attèle à supprimer les contenus contrefaisants lorsqu'ils lui sont signalés. Dans les conditions générales de Youtube, on retrouve une partie consacrée aux droit d'auteur, dans laquelle Youtube « s'engage à aider les détenteurs de droits d'auteur à trouver et supprimer du site les contenus présumés en infraction aux droits de propriété. C'est pourquoi, nous avons créé un outil de vérification des droits d'auteur qui permet aux titulaires de ces droits de rechercher les contenus qu'ils estiment être en infraction et de fournir à Youtube les informations requises pour localiser ces contenus »[404]. Il prévient également les utilisateurs du site : « Si vous publiez du contenu portant atteinte à des droits d'auteur, votre compte pourra être résilié et vous pourrez être passible d'une condamnation pour dommages et intérêts au cas où le titulaire des droits déciderait de prendre des mesures juridiques (ne prenez pas cela à la légère, car vous pourriez être poursuivi en justice !) »[405]. Il y a donc un réel engagement de la part de Youtube d'éviter la publication de contenus protégés. Il propose également un mécanisme de Content ID, une mesure technique de protection qui permet aux titulaires de droit de « bloquer, suivre ou monétiser ses vidéos ». Les ayants droit fournissent à Youtube les fichiers de référence, qui prend alors une empreinte unique de chaque vidéo afin d'alimenter un catalogue. Youtube compare alors les vidéos mises en ligne avec le catalogue des fichiers, le contenu est identifié automatiquement et est appliqué la règle choisie par l'ayant droit : blocage, suivi ou monétisation[406].

[401] E. MONTERO, « Les responsabilités du web 2.0 », *op. cit.,* p. 380.
[402] SEC(2011) 1641, *op. cit.*, p. 38.
[403] *Ibid*., p. 44.
[404] http://www.youtube.com/t/copyright_program
[405] http://www.youtube.com/t/howto_copyright?gl=FR&hl=fr
[406] http://www.youtube.com/t/contentid

La monétisation peut se faire via l'affichage de publicités autour de la vidéo, dont les revenus générés seront reversés pour l'utilisation de l'œuvre. Pour pouvoir bénéficier d'un tel mécanisme, il faut bien évidemment signer un partenariat avec Youtube.

Les conditions d'utilisation de réseaux sociaux tels Facebook[407], Twitter, Instagram, *etc.* comportent une clause par laquelle ils insistent sur le respect des droits de propriété intellectuelle et se réservent le droit de retirer tout contenu violant ces droits[408]. Ils fournissent également des outils pour aider à protéger ses droits, en signalant du contenu contrefait par exemple. Des moyens pour un réseau social de détecter du contenu protégé par le droit d'auteur seraient par exemple le repérage d'une signature électronique dans le fichier qui indique la présence de matériel protégé, ou encore la reconnaissance d'une série de caractères qui correspondraient au titre d'une œuvre[409]. Mais on ne pourrait leur imposer une surveillance généralisée de leur réseau, car ils bénéficient d'une exonération de responsabilité en tant qu'intermédiaires techniques, ce qui a été confirmé par l'arrêt *Netlog* de la Cour de Justice de l'Union européenne concernant les réseaux sociaux[410].

Quant au moteur de recherche Google, il est l'un des services qui reçoit le plus de demandes pour rendre inaccessibles des contenus portant atteinte au droit d'auteur, en l'occurrence des demandes pour supprimer les résultats de recherche qui redirigent les internautes vers des contenus présumés attentatoires au droit d'auteur[411]. Les demandes reçues contiennent chacune des URL à supprimer, que Google a décidé de répertorier dans une base de données, dans le cadre de son *Transparency Report*[412].

§3. Obligations d'intervention

La loi a prévu à la charge des intermédiaires techniques trois obligations destinées à lutter contre les comportements illicites sur internet : une obligation de collaboration, une obligation particulière de surveillance et une obligation d'informer les autorités. Celles-ci attestent de la volonté du législateur de ne pas laisser ces intervenants en dehors de la lutte contre de tels agissements. Certes, ces obligations ne lient pas les intermédiaires envers les titulaires de droit, qui ne peuvent directement se prévaloir de ces obligations, mais elles témoignent d'une tendance récente – matérialisée par la nouvelle loi du 20 juillet 2005 modifiant la loi de transposition du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information de la directive 2000/31 sur le commerce

[407] https://www.facebook.com/legal/terms
[408] Voir première partie du rapport.
[409] P.-O. FORTIN, « Facebook : attention aux droits d'auteur ! », article du 26 février 2012, disponible sur : http://www.cyberpresse.ca/le-soleil/actualites/societe/201202/25/01-4499854-facebook-attention-aux-droits-dauteur.php
[410] C.J.U.E. (3e ch.), 16 février 2012, *Sabam* c. *Netlog*, C-360/10, non encore publié au recueil.
[411] ENIGMAX, « Google starts punishing 'pirate' sites in search result », *TorrentFreak*, 10 août 2012, disponible sur http://torrentfreak.com/google-builds-largest-database-of-links-to-pirated-media-120717/ et ENIGMAX, « Google URL Takedown requests up 100% in a month, up 1137% in 2011 », *TorrentFreak*, 24 août 2012, disponible sur http://torrentfreak.com/google-url-takedown-requests-up-100-in-a-month-up-1160-on-2011-120824/
[412] http://www.google.com/transparencyreport/removals/copyright/

électronique[413] et qui a notamment étendu certaines des obligations aux prestataires – à les impliquer davantage dans la lutte contre les comportements illicites, y compris ceux relatifs au droit d'auteur.

I. Obligations de collaboration

Le régime d'exonération de responsabilité des prestataires n'interdit pas aux autorités judiciaires ou administratives de leur imposer des mesures visant à prévenir ou faire cesser une violation[414]. Ils ont à leur charge une obligation de collaboration. L'article 15, 2., de la directive 2000/31 prévoit que « les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services (…) ». L'article 21, §2, alinéa 2 de la loi sur la société de l'information impose aux prestataires intermédiaires de « communiquer aux autorités judiciaires ou administratives compétentes, à leur demande, toutes les informations dont ils disposent et utiles à la recherche et à la constatation des infractions commises par leur intermédiaire ». L'alinéa 1 prévoit quant à lui que « les prestataires (…) ont l'obligation d'informer sans délai les autorités judiciaires ou administratives compétentes des activités illicites alléguées qu'exerceraient les destinataires de leurs services, ou des informations illicites alléguées que ces derniers fourniraient ». Une obligation de collaboration avec les autorités judiciaires et administratives incombe donc aux prestataires.

La cour d'appel de Liège, dans un arrêt du 22 octobre 2009[415], a estimé que l'article 21, § 2, alinéa 2 impose aux prestataires de communiquer aux seules « autorités judiciaires et administratives compétentes », « à leur demande » les informations visées. Cet article « ne fonde aucun droit subjectif dans le chef d'une personne physique ou morale autre que lesdites autorités, à obtenir les informations en cause, que ce soit directement, par une injonction immédiate à l'égard du prestataire, ou encore indirectement, via une rétrocession des informations par l'autorité judiciaire ou administrative, procédure non prévue par cette disposition ». Cette position a été confirmée par la Cour de cassation[416].

---

[413] E. MONTERO, « Droit du commerce électronique », « Responsabilités des intermédiaires », point n° 4, pp. 27-28, in *Chronique de jurisprudence en droit des technologies de l'information (2002-2008), RDTI* juin 2009, n° 35.
[414] Cf. l'art. 12, 3 de la directive 2000/31 : « 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 le considérant n° 45 : « Les limitations de responsabilité des prestataires de services intermédiaires prévues dans la présente directive sont sans préjudice de la possibilité d'actions en cessation de différents types. 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 ».
[415] Liège (7e ch.), 22 octobre 2009, *R.D.T.I.,* n° 38, mars 2010, p. 95 et note J. FELD.
[416] Cass., 26 juin 2011, N° C. 10.0153.F.

L'article 46*bis* du Code d'instruction criminelle[417] permet au procureur du Roi (et au juge d'instruction) d'obtenir des données d'identification des utilisateurs d'un service de communication électronique auprès de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique après avoir procédé à leur identification[418]. Lors d'une telle décision, il faudra que la motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête[419]. Les données qui sont visées par ladite disposition sont toutes les données permettant « «1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé; 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée». Cela exclut donc du champ d'application *ratione materiae* de l'article les informations relatives aux communications électroniques elles-mêmes, entendons par là les informations relatives à leur contenu, leur durée, *etc*[420]. Concernant le champ d'application *ratione personae* de l'article, il faut savoir ce que l'on entend par les notions d' « opérateur d'un réseau de communication électronique » et de « fournisseur de services de communications électroniques », c'est-à-dire les intermédiaires auprès de qui peuvent être imposées les mesures de collaboration.

Dans une affaire mettant en cause la société américaine *Yahoo!*[421], s'est posée la question de l'interprétation de ces notions, et plus particulièrement de savoir si elles pouvaient être interprétées au sens de la loi du 13 juin 2005 relative aux communications électroniques. La Cour de cassation a estimé dans son arrêt du 18 janvier 2011 que « le 'fournisseur d'un service de télécommunications électroniques' au sens de l'article 46*bis* du Code d'instruction criminelle n'est pas uniquement l'opérateur belge au sens de la loi du 13 juin 2005 relative aux communications électroniques, mais quiconque dispense des services de communications électroniques, comme notamment la transmission de données de communication»[422]. *Ratione personae*, l'obligation de collaboration existe « aussi dans le chef de celui qui fournit un service consistant entièrement ou principalement dans la transmission de signaux par la voie de réseaux de communications électroniques et [que] la personne qui fournit un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques ». En adoptant une telle interprétation, la Cour mobilise le principe de l'autonomie du droit pénal, qui se traduit notamment par la liberté d'interprétation des notions empruntées à d'autres disciplines juridiques[423]. Au final, il appartiendra au juge pénal de déterminer, au regard des circonstances de l'espèce, si la personne requise peut ou non être considérée comme

[417] Cet article a fait l'objet d'une importante modification : Loi du 23 janvier 2007 modifiant l'article 46bis du Code d'instruction criminelle, M.B., 14 mars 2007.
[418] Article 46*bis*, §1er, alinéa 1.
[419] Article 46*bis*, §1er, alinéa 2.
[420] Ces données peuvent faire l'objet d'un repérage tel que prévu à l'article 88*bis* du CIC.
[421] Dans cette affaire, il était question de détournement de cartes bancaires par *phishing* via l'utilisation d'un compte mail attribué à *Yahoo!* Le réquisitoire du procureur du Roi s'est basé sur cette obligation de collaboration afin d'obtenir les données complètes d'enregistrement du compte (en ce compris l'adresse IP, la date et l'heure ainsi que la zone horaire), d'identifier l'adresse e-mail liée au profil et de recevoir toute autre donnée personnelle ou information permettant l'identification des utilisateurs du compte en cause. Après un refus d'accéder à la requête du procureur, celui-ci a cité *Yahoo!* sur base de l'article 46*bis* du Code d'instruction criminelle, qui incrimine le défaut de collaboration des opérateurs d'un réseau de communication électronique et des fournisseurs d'un service de communication électronique en prévoyant une amende à leur encontre.
[422] Cass. (2e ch.), 18 janv. 2011, *R.D.T.I.*, n° 3/2011, pp. 113 et s.
[423] F. KUTY, *Principes généraux de droit pénal belge. I. La loi pénale*, Bruxelles, Larcier, 2007, p. 110.

un opérateur d'un réseau de communication électronique ou comme fournisseur d'un service de communications électroniques[424].

II. Obligation de surveillance temporaire

Un juge peut également imposer aux intermédiaires une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par une loi, conformément à l'article 21, §1, *in fine* de la loi du 11 mars 2003 sur la société de l'information. Le juge pourrait donc décider d'une obligation de surveillance temporaire dans des hypothèses bien identifiées. Mais il ne pourrait pas, par exemple, prononcer une injonction destinée à bloquer les échanges illicites d'œuvres sur les réseaux *peer-to-peer* en ce que cela supposerait des mesures permanentes de sécurité et de filtrage, ce qui est notamment contraire à l'article 15 de la directive sur le commerce électronique posant le principe de l'interdiction de toute obligation générale de surveillance[425]. Le considérant 47 de la directive précise que cette obligation générale de surveillance est tempérée par cette possibilité de surveillance particulière.

Cette possibilité d'obligation de surveillance temporaire ne peut donc être généralisée ; en effet, l'article 21 §1 de la loi du 11 mars 2003, prévoit que les prestataires, incluant les fournisseurs d'hébergement, « n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ». Une surveillance dans un « cas spécifique », c'est-à-dire ciblée et temporaire peut être demandée par les autorités judiciaires ou policières compétentes, l'interdiction générale n'excluant pas « qu'un tribunal ou la police puisse demander à un prestataire de services de contrôler, par exemple, un site spécifique pendant une période donnée, afin d'empêcher ou de combattre une activité illicite particulière »[426].

§4. Actions en cessation à l'encontre des intermédiaires

I. Principe

Il est prévu, au dernier paragraphe des articles 12 à 14 de la directive 2000/31 sur le commerce électronique, « la possibilité pour une juridiction ou une autorité administrative (…) d'exiger du prestataire qu'il *mette un terme à une violation* ou qu'il *prévienne une violation* ». Les ordonnances d'injonction, quelles que soient leurs formes, sont donc formellement autorisées. La directive 2001/29 sur le droit d'auteur dans la société de l'information quant à elle prescrit en son article 8, 3. que « les États membres veillent à ce que les titulaires de droits puissent demander qu'une

[424] L. KERZMANN, « L'affaire Yahoo ! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46bis du Code d'instruction criminelle », *R.D.T.I.,* n° 44/2011, p. 121.
[425] E. MONTERO 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 ? », *R.L.D.I.,* juin 2010, n° 61, p. 86 et s.
[426] Commentaire article par article de la directive sur le commerce électronique, *op. cit.*, p. 31.

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 ». La directive 2004/48 reprend mot pour mot cette disposition de la directive 2001/29.

Le considérant 45 de la directive 2000/31 sur le commerce électronique prévoit « les limitations de responsabilité des prestataires de services intermédiaires prévues dans la présente directive sont sans préjudice de la possibilité d'actions en cessation de différents types. Ces actions en cessation ou en référé 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 ». L'interdiction pour les États membres d'imposer aux prestataires de services une obligation générale de surveillance ne vaut que pour les obligations à caractère général, cela « 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 »[427].

En Belgique, c'est à l'article 87, § 1er de la loi sur le droit d'auteur que l'on retrouve la transposition de ces règles en matière d'injonction, celui-ci prévoyant que « le président du tribunal de première instance et le président du tribunal de commerce, dans les matières qui sont respectivement de la compétence de ces tribunaux, constatent l'existence et ordonnent la cessation de toute atteinte au droit d'auteur ou à un droit voisin. Ils 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. (…) L'action est formée à la demande de tout intéressé, d'une société de gestion autorisée ou d'un groupement professionnel ou interprofessionnelle ayant la personnalité civile ». Il s'agit donc d'une action devant le président du tribunal de première instance ou du tribunal de commerce, siégeant comme en référé, avec dès lors le pouvoir de juger du fond du litige. Un juge saisi d'une action en contrefaçon peut également, en vertu de l'article 86*ter* de la loi sur le droit d'auteur, prononcer une telle injonction de cessation à l'encontre des intermédiaires.

Tout intéressé peut obtenir d'un juge de faire cesser les atteintes au droit d'auteur portant sur des œuvres protégées, et pas seulement les titulaires de droit d'auteur, du moment que la violation du droit en cause peut lui porter préjudice. La loi autorise expressément une société de gestion collective ou un groupement professionnel à agir à condition de disposer de la personnalité juridique, et que les membres – ou du moins certains – aient un intérêt propre à l'introduction de l'action[428].

Il est nécessaire qu'il y ait une atteinte fautive à un droit pour que le juge intervienne en cessation, ce qui implique que le juge saisi ne peut l'être que pour constater une atteinte au droit d'auteur avec en parallèle une demande de la faire cesser. Cela implique également que l'infraction doit encore exister ou être susceptible de se reproduire, auquel cas la cessation serait dépourvue d'objet. L'existence d'une atteinte aux droits de l'auteur sera jugée sur base de l'élément matériel correspondant à une reproduction ou une communication illicite, c'est-à-dire faite sans l'accord du titulaire du droit d'auteur ou du droit voisin ou au-delà des limites fixées dans l'autorisation[429]. Le juge a le droit d'ordonner la cessation des activités contrefaisantes, mais garde le pouvoir

[427] Considérant 47 de la directive 2000/31.
[428] Bruxelles, 22 mai 1996, *A&M*, 1997, p. 178, note A. STROWEL ; Liège, 8 décembre 1998, *A&M*, 1999, p. 67.
[429] *Idem*, p. 443

d'apprécier si la cessation n'est pas une sanction disproportionnée[430]. Le juge des cessations peut ordonner une mesure positive, si elle est la conséquence d'une interdiction, et donc prendre les mesures nécessaires pour que l'ordre de cessation produise un résultat et qu'il mette fin à la situation illicite de manière effective[431].

L'action en cessation intentée à l'encontre d'intermédiaires sur base des articles 86*ter* et 87 de la LDA trouve à s'appliquer lorsque l'atteinte au droit d'auteur n'est pas le fait du défendeur, ici simple intermédiaire technique, mais de tiers non présents à la cause (par exemple les abonnés d'un fournisseur d'accès qui procèdent au téléchargement illégal sur les réseaux de *peer-to-peer*)[432]. La Cour a précisé sur ce point que « l'article 87, § 1er, de la LDA interprétée à la lumière de l'article 8.3 de la Directive 2001/29 constitue en conséquence la base légale suffisante et nécessaire pour constater les infractions au droit d'auteur découlant de l'utilisation des logiciels *peer-to-peer* pour échanger des œuvres musicales protégées sans autorisation de la Sabam et pour ordonner à la SA Tiscali, en sa qualité d'intermédiaire dont les services sont utilisés pour commettre ces infractions, de prendre les mesures de nature à les faire cesser »[433].

La formulation large et claire de cet article ne s'oppose pas à ce qu'une mesure soit ordonnée à l'égard d'un tiers qui n'est pas l'auteur de l'infraction – ici l'intermédiaire technique – qui est la personne la mieux placée pour y mettre fin efficacement[434]. Dans le cadre d'une action en cessation introduite contre un intermédiaire et non contre l'auteur de l'atteinte au droit d'auteur, l'ordre de cesser est absolument indépendant de toute considération relative à la faute de l'intermédiaire. Il suffit de constater l'atteinte au droit d'auteur et la circonstance que l'intermédiaire est la personne la mieux placée pour faire cesser celle-ci, sans que cela suppose en aucune manière la démonstration d'un quelconque manquement au devoir de prudence dans le chef de ce dernier.[435]

Il est tout à fait possible pour le juge de la cessation d'ordonner des mesures positives au défendeur, sans quoi l'ordre de cessation demeurerait inefficace[436], et cela malgré le libellé de l'article 87, § 1er de la LDA dans lequel il est seulement question d'un ordre de cesser, d'une obligation de ne pas faire[437]. En plus de ces mesures positives, rien ne s'oppose à ce que le juge ordonne des mesures préventives, dont le but est d'empêcher la survenance d'une atteinte à des droits d'auteur autres que celles constatées jusqu'alors[438].

[430] Civ. Bruxelles (cess.), 5 janvier 1996, *I.R.D.I.*, 1996, p. 98.
[431] A. BERENBOOM, *Le nouveau droit d'auteur et les droits voisins*, *op. cit.*, p. 460.
[432] A ce sujet, voir le commentaire de Y. COOL et E. MONTERO, « Le *peer-to-peer* en sursis? », *R.D.T.I.*, n° 21/2005.
[433] Civ. Bruxelles (réf.), 26 novembre 2004.
[434] Voir le considérant 59 de la directive 2001/29.
[435] Y. COOL et E. MONTERO, « Le *peer-to-peer* en sursis », *op. cit.*, p. 99.
[436] Cass., 6 déc. 2001, *A&M*, 2002, p. 146 et note B. MICHAUX. A ce sujet, voir aussi F. DE VISSCHER et B. MICHAUX, *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000, n° 636.
[437] Y. COOL et E. MONTERO, « Le *peer-to-peer* en sursis », *op. cit.*, p. 99.
[438] F. DE VISSCHER et B. MICHAUX, *op. cit.*, n° 644, 645 et 655.

II. Champ d'application

A. A l'encontre de quels intermédiaires ?

1. Les intermédiaires au sens de la directive 2000/31

L'action en cessation visée à l'article 87 peut être dirigée à l'encontre de toute personne, qu'elle soit un intermédiaire ou non, qui pourrait contribuer à la cessation de l'atteinte ou de ses effets[439]. Le président saisi peut rendre une injonction à l'égard des « intermédiaires » dont les services seraient utilisés pour porter atteinte au droit d'auteur ou aux droits voisins[440]. Cette disposition n'est pas cantonnée aux intermédiaires au sens de la directive sur le commerce électronique, mais peut trouver à s'appliquer à l'égard de tout tiers dont les services sont utilisés à des fins de porter atteinte aux droits d'auteur[441], la notion d'intermédiaires est dès lors très large. Le rapport d'évaluation de la directive européenne 2004/48 sur la mise en œuvre des droits intellectuels dont dérive cette disposition, confirme que cette notion doit être interprétée largement et qu'elle ne requiert pas un rapport contractuel entre l'intermédiaire et l'auteur de l'atteinte[442].

Des mesures de cessation peuvent donc être imposées envers les fournisseurs d'accès à internet, les prestataires d'un service de *caching*, envers les hébergeurs, qui peuvent être des blogs, des forums de discussion, des places de marché en ligne, des hébergeurs de contenus générés par les utilisateurs comme les réseaux sociaux, les plateformes de partage de vidéo. Peuvent également être compris dans cette notion les moteurs de recherche, le prestataire DNS.be ainsi que les prestataires de paiement.

2. Les moteurs de recherche

Comme nous avons eu l'occasion de le voir *supra*, un moteur de recherche peut être considéré comme un intermédiaire pour l'application des dispositions des directives 2000/31 et 2004/48 relatives aux injonctions.

Le DMCA américain prévoit quant à lui spécifiquement que les « fournisseurs d'outils de recherche » bénéficient d'une exonération conditionnelle de responsabilité semblable aux fournisseurs d'hébergement.

Fin mai 2012, Google communiquait qu'il retirait plus d'un million de liens par mois des résultats de recherche, en raison d'atteintes au droit d'auteur. Depuis quelques mois, les principaux sites ciblés par les demandes adressées à Google par les ayants droit sont des moteurs de recherche pour sites de téléchargement direct ou des annuaires de partage de fichiers BitTorrent[443].

---

[439] B. MICHAUX, Commentaire de l'article 87, *Hommage à Jean Corbet. La loi belge sur le droit d'auteur – Commentaire par article*, Larcier, 2008, p.482.
[440] Article 86ter de la LDA.
[441] B. MICHAUX, « Aspects procéduraux : les dispositions expresses et implicites de la loi du 22 mai 2005 », *A. & M.*, 2005, p. 149 et s.
[442] Commission Staff Working Document, Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States, 22 Décembre 2010, SEC(2010) 1589 final, p. 14.
[443] http://www.google.com/transparencyreport/removals/copyright/domains/?r=last-year

3. DNS.be

Le gestionnaire de DNS.BE peut également être potentiellement visé par une mesure ordonnée par le juge de cessation.

Il convient de déterminer si l'on peut considérer que les services fournis par DNS.BE sont bien utilisés dans le cadre d'une atteinte au droit d'auteur.

En ce qui concerne la diffusion illicite de contenus protégés par le droit d'auteur, la réponse à la question devrait être positive, par exemple, en cas d'usage d'un site web ou d'une plateforme hébergée sous un nom de domaine .be. En effet, les services offerts par DNS.BE consistent en la mise à disposition d'un nom de domaine pour une durée limitée[444]. L'objet des services (le nom de domaine .be) est dès lors bien utilisé dans le cadre d'agissements portant atteinte au droit d'auteur.

Le blocage par nom de domaine est une mesure intéressante pour lutter contre le téléchargement illégal de par ses effets extraterritoriaux – le domaine visé sera inaccessible pour tous et de partout, sauf bien sûr si la mesure est contournée par l'addition d'une autre extension – et est applicable envers tous les FAI – contrairement à une mesure qui ciblerait le blocage par tel FAI de tel site contrefaisant.

4. Les prestataires de paiement

Au même titre que les moteurs de recherche et le DNS.be, des injonctions peuvent être ordonnées dans le cadre d'une action en cessation à l'encontre d'un prestataire de paiement, celui-ci entrant dans la définition large d'intermédiaire de la directive 2004/48, aux fins de suspendre tout paiement des services illicites fournis par le contrefacteur.

La proposition de loi modifiant l'article 87 de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins en ce qui concerne la responsabilité des intermédiaires lors d'atteintes au droit d'auteur et aux droits voisins, déposée à La Chambre le 19 janvier 2011[445], a pour objectif d'élargir la notion d'intermédiaire pour pouvoir y inclure les intermédiaires de paiement. La volonté est de pouvoir imposer aux prestataires de paiement qu'ils bloquent l'accès à leurs services auprès des sites qui vendraient illégalement des contenus protégés par le droit d'auteur – et de manière générale par des droits de propriété intellectuelle. Selon les auteurs de la proposition, l'article 87 de la LDA ne permettrait pas d'agir à leur encontre, or l'on sait que la directive 2000/31 sur le commerce électronique n'est pas interprétée restrictivement par la Cour de justice, et que les directive 2001/29 sur le droit d'auteur dans la société de l'information et 2004/48 sur le respect de la propriété intellectuelle acceptent une interprétation très large de la notion d'intermédiaire. L'article 87 permet donc, dans sa mouture actuelle, d'imposer des mesures aux prestataires de paiement.

Il s'agira plutôt de se poser la question de la nature et l'étendue des mesures qui peuvent leur être imposées (voir *infra)*.

[444] C. MANARA, thèse, Cahiers de l'IRPI, Paris, Litec, 2012.
[445] Proposition de loi déposée par Madame Karine LALIEUX et consorts modifiant l'article 87 de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins en ce qui concerne la responsabilité des intermédiaires lors d'atteintes au droit d'auteur et aux droits voisins, La Chambre, Doc 53, 1084/001

B. Etendue des mesures sollicitées

La Cour de justice a plusieurs fois eu l'occasion de se prononcer sur la validité d'injonctions ciblées contre des intermédiaires techniques sur pied de l'action en cessation. Les juridictions nationales doivent pouvoir enjoindre aux intermédiaires de prendre des mesures qui visent à mettre fin aux atteintes déjà portées aux droits de propriété intellectuelle au moyen de leurs services de la société de l'information, mais aussi à prévenir de nouvelles atteintes[446], et les modalités des injonctions relèvent du droit national[447]. Dans le cadre de ces injonctions, il est nécessaire de « respecter l'article 15, paragraphe 1, de la directive 2000/31, qui interdit aux autorités nationales d'adopter des mesures qui obligeraient un FAI à procéder à une surveillance générale des informations qu'il transmet sur son réseau »[448].

Les mesures prises doivent tendre à réaliser un compromis entre ce que S. DUSOLLIER et E. MONTERO ont appelé un « triangle diabolique »[449] : les mesures doivent être effectives et dissuasives, elles ne peuvent consister en une obligation générale de surveillance et doivent assurer un juste équilibre entre les droits et libertés. Comme exemple d'injonction à adresser aux intermédiaires techniques et qui respecterait ce « triangle diabolique », a été suggérée la mise en place d'une procédure de notification et de retrait, au cas où une telle procédure fait défaut, ou d'améliorer son efficacité s'il en existe une[450].

1. Types de mesures

Lorsque l'on se penche sur la question des types de mesures qui peuvent être mis en place, il faut toujours garder à l'esprit l'interdiction d'imposer une surveillance généralisée aux prestataires de services de la société de l'information prévue par l'article 15 de la directive 2000/31 : il est en effet difficile de concilier les réponses juridiques prévues aux violations concrètes du droit d'auteur et une obligation générale de surveillance potentiellement illicite[451]. La Cour de justice a rappelé que l'obligation générale de surveillance serait incompatible avec l'article 3 de la directive 2004/48, qui énonce que les mesures prises pour assurer le respect des droits de propriété intellectuelle doivent être équitables et proportionnées et ne doivent pas être excessivement coûteuses[452].

a. Le filtrage

L'articulation entre la directive sur le commerce électronique et la directive sur le droit d'auteur joue un rôle central pour déterminer dans quelles circonstances et dans quels cas il convient d'imposer l'usage de filtres internet lorsque cela est nécessaire[453].

---

[446] Arrêt *Scarlet,* § 31 et arrêt *L'Oréal*, § 131.
[447] Arrêt *Scarlet*, § 32 et arrêt *L'Oréal*, § 135.
[448] Arrêt *Scarlet*, § 35.
[449] S. DUSOLLIER et E. MONTERO, « Des enchères et des fleurs », *op. cit.,* p. 186.
[450] *Ibidem*, p. 188.
[451] C. ANGELOPOULOS, « Filtrage des contenus protégés par le droit d'auteur sur Internet en Europe », *op. cit.*, Editorial.
[452] Arrêt *eBay*, § 139.
[453] C. ANGELOPOULOS, *op. cit*., Editorial.

Selon le Comité des Ministres du Conseil de l'Europe, « une mesure de filtrage technique peut être définie largement comme l'application d'une limite technique à l'accès aux contenus Internet »[454]. Toujours selon le Conseil des Ministres, les mesures de filtrage technique sont « des applications logicielles permettant le blocage de l'accès et le filtrage de contenus illicites, préjudiciables ou inappropriés, que l'on peut afficher ou télécharger à l'aide d'un navigateur Web ou d'une application Internet »[455].

Lorsqu'est mise en place une mesure de filtrage, cela va plus loin que la simple inspection des paquets d'informations qui circulent sur le réseau, car il s'agit ici d'introduire une technologie qui permet de traiter le contenu du message et non plus son enveloppe[456]. L'avantage de telles mesures est qu'elles sont efficaces pour combattre un grand nombre de phénomènes différents tels que la pédopornographie, les jeux en ligne, les atteintes à la sécurité sur internet et la contrefaçon, mais avec une réserve – assez importante – en terme de capacité technologique et donc de faisabilité et d'efficacité[457]. Des mesures de filtrages sont déjà mises en place par les fournisseurs d'accès dans un but de protéger et désengorger leurs infrastructures, comme par exemple des outils pour lutter contre les *spams*[458], les virus et les logiciels malveillants.

Il est important de noter que le filtrage et le blocage sont deux mécanismes différents, « interdépendants »[459]. Comme image pour décrire le filtrage et le blocage, C. MANARA propose celle du filet : « 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 »[460]. Cette immersion du filet implique un contrôle de ce qui se passe sur les réseaux, car pour pouvoir chercher à empêcher des atteintes au droit d'auteur, toutes les communications électroniques doivent être passées au crible.

Il faut savoir ce que l'on va filtrer, et surtout quel critère va utiliser le filtre pour discriminer les données. Plusieurs catégories de filtrage de contenus illicites sont ici envisageables, en fonction de ce que l'on va filtrer et du critère qui va être utilisé :

- Le ***filtrage par port*** : filtrage qui consiste à fermer des numéros de port correspondant à des protocoles connus pour la communication distribuée entre applications[461], donc à fermer par exemple les portes qui sont utilisées par les logiciels *peer-to-peer* pour communiquer entre eux. Concernant les réseaux de *peer-to-peer*, ils sont actuellement capables d'utiliser d'autres ports que ceux qui leur sont à la base consacrés, ce qui rend impossible un tel filtrage sans coupure de l'accès à internet dans son entièreté[462].
- Le ***filtrage par protocole*** : filtrage qui consiste à analyser les paquets de données échangés entre les ordinateurs. Les technologies employées peuvent être le blocage IP par routeur et la redirection DNS, et peut être réalisé sur des adresses MAC des machines, ou sur des noms de domaine[463]. Les paquets de données contiennent une signature propre qui permet, en matière

[454] Recommandation du Conseil des Ministres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet.
[455] *Idem.*
[456] C. MANARA, « Bloquer le filtrage ! Une approche critique des affaires SABAM », www.juriscom.net p. 5.
[457] C. ANGELOPOULOS, *op. cit*, p. 2.
[458] C. MANARA, *op. cit.,* p. 6.
[459] *Idem*.
[460] *Idem*.
[461] http://fr.wikipedia.org/wiki/Filtrage_d'Internet
[462] F. COPPENS, « Filtrage P2P : possibilités techniques et obstacles juridiques », *R.D.T.I.*, n° 30/2008, p. 97.
[463] http://fr.wikipedia.org/wiki/Filtrage_d'Internet

de filtrage des réseaux *peer-to-peer*, au logiciel P2P de reconnaître ces données comme lui étant destinées, pour les interpréter ensuite. Le filtrage détecte ces signatures et peut ensuite bloquer l'échange des données.[464]

- Le ***filtrage par mots clés*** : filtrage qui consiste à empêcher l'accès aux pages dont l'adresse ou le contenu contiennent certains mots[465]. Des « listes noires » de mots sont créées, avec une interdiction de l'accès aux pages contenant les mots présents sur la liste. Ce type de filtrage paraît difficile à appliquer à la problématique du partage et téléchargement illégal d'œuvres protégées par le droit d'auteur. En effet, un mot ne peut suffire à savoir si une œuvre a été licitement mise à disposition ou non.
- Le ***filtrage par contenu*** est considéré par l'expert judiciaire dans l'affaire *Sabam* comme « le seul à tenter de répondre à la problématique de façon spécifique».[466] Il faut procéder à ce que l'on appelle du *deep packet inspection*, ce qui pose de sérieux problèmes concernant la protection de la vie privée des individus.

Le filtrage par contenu peut consister en la technologie de reconnaissance par empreinte, qui utilise « une représentation numérique unique de chaque élément du contenu protégé en vue de les identifier parmi tous les contenus téléchargés sur un site d'hébergement ou transférés sur un réseau, sur la base d'une comparaison avec une vaste base de données de référence contenant toutes les empreintes prélevées »[467], et c'est aux ayants droit de fournir une telle empreinte pour la base de données[468]. Si un contenu correspondant à une empreinte de la base de données est identifié lors de sa circulation sur internet, il est automatiquement bloqué. C'est cette détection automatique qui en fait un avantage par rapport à d'autres formes de filtrage / blocage, mais cet automatisme pose le problème de la « non-contextualisation » du filtrage : le transfert qui a lieu dans le cercle de famille ou dans le cadre de l'enseignement par exemple, est englobé dans la technologie qui n'est pas en mesure de savoir s'il s'agit ou non d'une utilisation légitime d'une œuvre protégée. Comme autre inconvénient de ce système, il a été pointé qu'il implique une surveillance de l'ensemble des informations qui passent par un fournisseur d'accès à internet, ce qui implique donc une surveillance généralisée de tout le réseau, mesure interdite par la directive 2000/31 sur le commerce électronique.

Concernant les mesures demandées par la Sabam, celles-ci auraient eu pour conséquence l'adoption de la forme la plus extensive du filtrage : il était en effet demandé un filtrage sans limitation dans le temps, sans limitation des échanges ni des internautes à surveiller. Il y aurait dans les faits un blocage des contenus qui se ferait de manière automatique et systématique. Une injonction exigeant la mise en place d'un système de filtrage ne peut être légalement prononcée à l'encontre des intermédiaires techniques qu'à la condition qu'elle ne concerne que des personnes et/ou des contenus spécifiques. L'article 20 de la directive 2000/31 sur le commerce électronique prévoit que « les sanctions prévues doivent être effectives, proportionnées et dissuasives ». On peut se poser ici la question de leur caractère dissuasif : les mesures étant relatives aux flux et non aux personnes qui en sont à l'origine, personnes qui ne seraient dès lors pas sanctionnées car seules les informations

[464] F. COPPENS, « Filtrage P2P (…) », *op. cit.,* p. 97.
[465] http://fr.wikipedia.org/wiki/Filtrage_d'Internet
[466] F. COPPENS, « Filtrage P2P (…) », *op. cit.*, p. 97.
[467] C. ANGELOPOULOS, *op. cit.,* pp. 2 et 3.
[468] C. ANGELOPOULOS, *op. cit.,* p. 3.

sont impactées, cela priverait la décision judiciaire d'impact social ou éducatif[469]. De plus, il n'existe pas encore à notre connaissance de technique de filtrage réellement efficace, qui puisse assurer une distinction entre les œuvres protégées qui circulent licitement des autres, alors qu'une des conditions d'application de telles mesures est justement leur efficacité.

b. Le blocage de sites

Une autre manière d'obtenir le concours des fournisseurs d'accès pour lutter contre la contrefaçon des droits d'auteur en ligne est le blocage de sites internet, qui consiste en la demande aux fournisseurs d'accès qu'ils bloquent certains sites internet à tous leurs clients, sites qui peuvent être des intermédiaires à des réseaux *de peer-to-peer* comme les sites de *torrent*, ou des sites qui hébergent eux-mêmes des œuvres contrefaites. Il appartient au juge des cessations, dans la détermination d'une mesure positive spécifique, d'apprécier, parmi les techniques existantes, laquelle permet d'éviter au mieux les atteintes au droit en cause. Il existe deux principales méthodes de blocage de site qui peuvent être pratiquées par les FAI, à savoir le blocage par DNS ou le blocage par adresse IP.

Le blocage par DNS est un moyen pour procéder au blocage d'un site internet qui consiste à demander aux sites qui traduisent les URL, les *Domain Name System*, de bloquer l'association du nom de domaine à son adresse IP correspondante notifié comme étant utilisé par des sites proposant du contenu illicite.

Le blocage par adresse IP est une technique qui consiste en la programmation des serveurs du FAI de telle sorte que plus aucune connexion n'est possible avec les adresses IP des sites en cause. Cette technique est plus invasive que le blocage par DNS car elle a pour conséquence qu'il n'est plus possible pour les internautes d'accéder au site lié à l'adresse IP, ce qui est encore réalisable dans le cas de la dissociation entre l'IP d'un site et son nom de domaine[470].

C'est un blocage par DNS qui a été demandé dans l'affaire belge *The Pirate Bay*. Par un arrêt du 26 septembre 2011, la cour d'appel d'Anvers a condamné[471] les deux FAI Belgacom et Telenet à bloquer l'accès pour leurs abonnés au site *The Pirate Bay*, par la mise en place d'un blocage par *DNS*. Le blocage a été ordonné aux deux FAI sur demande de la B.A.F., la *Belgian Anti-piracy Federation*, sur pied de l'action en cessation prévue à l'article 87 de la LDA. L'arrêt vient en opposition de la décision du tribunal de commerce d'Anvers[472] qui avait refusé d'imposer aux FAI une telle mesure de blocage, jugée disproportionnée selon lui par rapport à l'infraction, en remettant en question la pertinence et l'efficacité de la mesure demandée.

Selon la B.A.F., entreprendre des actions contre les hébergeurs et les fondateurs de tels sites n'est plus suffisant, ce pourquoi ils ont décidé de s'attaquer aux FAI, en les mettant en demeure de bloquer *The Pirate Bay* et les sites qui y sont liés pour le rendre inaccessible aux internautes[473]. La cour d'appel d'Anvers, dans sa prise de décision, a effectué un exercice d'équilibre afin de concilier

[469] C. MANARA, « Bloquer le filtrage ! (…) », *op. cit.,* p. 7.
[470] P. VAN EECKE et A. FIERENS, « Pirate Bay : schip voor anker in de Antwerpse haven », *R.A.B.G.*, n° 2011/18, pp. 1283 et 1284.
[471] Antwerpen, 26 september 2011, *RABG*, 2011/18, p. 1269 et s. et note de P. VAN EECKE et A. FIERENS, « Pirate Bay : schip voor anker in de Antwerpse haven », *RABG*, 2011/18, p. 1278.
[472] Comm. Antwerpen, 8 juillet 2010.
[473] Arrêt *The Pirate Bay*, p. 1273.

les intérêts des ayants droit, des fournisseurs d'accès et des internautes[474]. L'enjeu de l'affaire est la formulation précise de l'injonction. En appel, la B.A.F. a demandé qu'il soit procédé à un blocage par adresse IP, mais la cour, après un examen attentif de la pertinence et de l'efficacité des mesures, a opté pour un blocage par DNS[475].

Selon la cour d'appel d'Anvers, qui a procédé à la détermination de la technique la plus acceptable pour les FAI, celle qui n'engendrerait pas pour eux des coûts inacceptables. Elle a comparé les techniques disponibles : le blocage par DNS et par IP. Malgré que l'*IP blocking* puisse toujours être contourné, elle atteint de manière plus efficace son but que via le *DNS blocking*. Mais selon les FAI, une adresse IP peut héberger plusieurs sites, et donc avoir un impact sur des sites innocents. La cour a dès lors opté pour blocage DNS comme solution la plus adéquate. La question étant éminemment technique, il y a fort à parier que des juges, placés dans les mêmes circonstances, opèrent la même analyse d'impact des mesures.

Il est utile de relever que la non-efficacité totale de la mesure ne peut être un obstacle à la non-exécution d'une injonction. On n'attend pas des FAI qu'ils assurent que plus aucun de leurs abonnés ne puissent consulter le site bloqué. La cour d'appel d'Anvers, dans l'affaire *The Pirate Bay*, a en effet estimé que les FAI auront effectivement exécuté leur obligation dès que la mesure aura été appliquée, et qu'ils ne devront pas vérifier ultérieurement si certains abonnés ont su contourner la mesure en accédant au site litigieux. Le tribunal exclut l'obligation de résultat dans le chef des FAI, car l'on n'attend pas d'eux que plus aucun de leurs clients ne puissent consulter le site web. La mesure est considérée par la cour comme suffisante dès lors qu'elle s'avère utile pour les utilisateurs moyens d'internet.

Remarquons que la cour n'a pas fait droit à la demande des FAI d'attendre les arrêts de la Cour de justice dans les affaires *Scarlet* et *Netlog* pour rendre son arrêt. Selon elle, le manque d'analogie avec les affaires *Sabam* justifie un tel rejet, le litige en l'espèce portant sur le blocage de sites, et non sur l'installation d'un système de filtrage comme c'était le cas devant les instances européennes[476].

Un élément important dont il faut tenir compte lorsque l'on décide d'implémenter un système de blocage de site le risque que la mesure entraine le blocage de contenus tout à fait licites hébergés sur le site en cause. Il faudra donc veiller au respect de la proportionnalité et n'empêcher, à l'instar de ce que la Norvège a prévu dans sa proposition de loi[477], l'accès qu'à un site internet qui porterait atteinte *dans une large mesure* au droit d'auteur. Seuls les sites web dans lesquels le droit d'auteur ferait de toute évidence l'objet d'une atteinte considérable pourraient être bloqués. Cela aura pour conséquence qu'un site entier ne pourra être bloqué si seul un contenu illicite y est présent. La question se pose alors de savoir ce que le propriétaire du contenu licite qui aurait été bloqué pourrait intenter comme action à l'encontre du propriétaire du site en cause pour pouvoir récupérer ce contenu. Quoi qu'il en soit, il faut prévoir une disposition qui ôterait toute responsabilité au fournisseur d'accès à internet qui aurait procédé au blocage d'un site à l'encontre du propriétaire du contenu licite, à la condition qu'il ait agi dans le respect de la loi. Nous y reviendrons.

[474] *Ibidem,* p. 1278.
[475] Le risque encouru avec un blocage par adresse IP est qu'une même adresse peut héberger plusieurs sites, ce qui peut entraîner le blocage de sites « innocents », le blocage par DNS étant dès lors plus acceptable pour la cour.
[476] Arrêt *The Pirate Bay*, p. 1271.
[477] Voir premier chapitre du rapport ; Nouvel article 57c du *Norwegian Copyright Act*.

Il est toutefois difficile de déterminer le seuil que devrait représenter la part d'atteintes au droit d'auteur dans le site concerné. Par analogie, on pourrait s'en référer à la jurisprudence américaine sur le *contributory infringement* et ses applications aux applications *peer-to-peer* pour lesquelles une responsabilité peut être engagée si l'outil n'est pas capable de « *substantially non infringing uses* »[478]. La jurisprudence ayant appliqué ce critère n'a toutefois pas déterminé avec précisé le seuil requis, les cas lui étant soumis étant généralement caractérisés par des atteintes au droit d'auteur assez majoritaires[479].

c. Autres types de mesures possibles

Outre le filtrage et le blocage de sites, d'autres mesures peuvent être prises dans le cadre de l'action en cessation envers les prestataires de services de la société de l'information.

Il a été décidé par la Cour de justice que l'exploitant peut être obligé de prendre « des mesures permettant de faciliter l'identification de ses clients vendeurs »[480].

Comme cela a été signalé dans la première partie du présent rapport, les moteurs de recherche traditionnels, comme Google, permettent également de trouver des liens menant vers des contenus piratés, et sont à l'origine d'une grande part de téléchargements illégaux. En effet, Google ne fait pas la différence, sur son moteur de recherche, entre les liens renvoyant vers des contenus légaux et ceux qui violent le droit d'auteur. Les moteurs de recherche sont « une des pierres angulaires de l'Internet ». Pouvoir leur imposer des mesures est donc essentiel dans la lutte contre le piratage en ligne. Nous l'avons vu, ils peuvent être considérés comme des intermédiaires et bénéficient à ce titre de l'exonération de responsabilité conditionnelle, ils ne peuvent donc pas se voir imposer une obligation générale de surveillance. Une mesure spécifique dans le cadre d'une action en cessation telle que le déréférencement de contenus est tout à fait envisageable, mais sans qu'il ne puisse leur être imposé un filtrage généralisé des liens menant vers des contenus piratés « en amont », dans le but de faire remonter les liens légaux[481]. Il pourrait leur être appliqué les mesures de *notice and stay down* pour éviter le passage systématique devant la justice, qui prend alors la forme d'une obligation particulière de surveillance (voir *infra*).

On peut s'interroger sur le type de mesure que le président saisi d'une demande en cessation pourrait ordonner à l'égard de DNS.BE. Un blocage du nom de domaine nous semble parfaitement envisageable, car cette mesure est de nature à empêcher la poursuite de l'infraction. Sur le plan pratique, on observera cependant que la mesure n'est sans doute efficace qu'à court terme, car le contrefacteur pourrait parfaitement (en quelques heures) enregistrer un autre nom de domaine ressemblant à celui bloqué afin de rouvrir son site ou sa plateforme. Une autre mesure pourrait consister à bloquer une adresse IP. En effet, le gestionnaire d'un domaine (DNS.BE dans notre hypothèse) assure, d'un point de vue technique, le lien entre une adresse IP et des noms de domaine enregistrés dans son domaine (une adresse IP peut, par exemple, être reliée à plusieurs noms de domaine). Si l'on ordonne à DNS.BE de bloquer tout nom de domaine dirigé vers une adresse IP spécifique, l'efficacité de la mesure est (un peu) plus grande. On soulignera cependant que cette efficacité demeure limitée, car les fraudeurs parviennent facilement à contourner ce type de mesure via des manœuvres de redirection (faisant transiter les contenus via d'autres adresses IP), ou

[478] Voir *Sony Corp of America v Universal City Studios*, 464 US 417 (1984).
[479] *MGM Studios, Inc v Grokster Ltd*, 380 F 3d 1154 (9th Cir 2004), p.1162.
[480] Arrêt *L'Oréal*, § 142.
[481] Demande de l'IFPI.

simplement en y ajoutant une autre extension. En outre, le blocage d'adresses IP présente des risques de dommages collatéraux, dans l'hypothèse où les activités illicites sont hébergées sur un serveur comportant des données d'autres utilisateurs. Si ces derniers ont également recours aux services de DNS.BE une telle mesure pourrait leur causer préjudice alors qu'ils sont totalement étrangers aux activités illicites.

Comme nous l'avons vu, il peut être ordonné à l'égard des prestataires de service de paiement différentes injonctions judiciaires. Mais il apparaît que certains prestataires de paiement ont mis en place volontairement une politique préventive. Déjà au niveau de la conclusion de contrats avec les sites internet, certains intermédiaires de paiement ont pour pratique de filtrer leurs éventuels clients en procédant à une enquête avant tout engagement. Il est également possible pour ces intermédiaires de procéder au blocage, non pas du paiement en ligne, mais du transfert de l'argent vers le commerçant. L'argent reste donc entre les mains du premier, et cela le temps nécessaire au règlement du différend. Le blocage peut aussi s'opérer au niveau de l'affiliation du site lui-même envers l'intermédiaire, en cas de fraude par exemple. Ce type de politique laisse à penser qu'il serait tout à fait réalisable de s'organiser avec eux sur une base volontaire dans le but de les utiliser dans la lutte contre le piratage du droit d'auteur en ligne. Il pourrait également être demandé à ces intermédiaires, à l'instar des moteurs de recherches et du DNS.be, des informations concernant leurs clients, sur base de l'article 86*ter* de la LDA.

2. Dans le temps

L'action en cessation est, comme nous avons eu l'occasion de le voir, une action « comme en référé », ce qui signifie que les mesures décidées par le juge dans ce cadre ne sont pas temporaires. Le juge dans l'arrêt *Scarlet* a estimé que cela en fait une mesure plus lourde mais que cela ne pose pas de problème quant à son application, sous réserve d'une atteinte à l'article 15 de la directive 2000/31.

La portée matérielle des mesures de cessation n'est pas définie par la loi. L'ordre de cessation doit être suffisamment précis pour que son destinataire puisse en réaliser la portée[482]. Rien n'empêche toutefois qu'il puisse s'étendre à des actes apparentés à l'atteinte qu'on entend faire cesser[483], ni qu'il puisse viser la prévention de nouvelles atteintes[484]. La Cour d'appel d'Anvers, dans l'affaire *The Pirate Bay* a également admis que l'ordre de cessation à mettre en œuvre par les intermédiaires pouvait concerner des répertoires entiers.

Concernant l'article 11 de la directive 2004/48 sur la propriété intellectuelle consacré aux injonctions, la Cour de justice a dit pour droit que « la compétence attribuée conformément à l'article 11, troisième phrase, de ladite directive aux juridictions nationales doit permettre à celles-ci d'enjoindre au prestataire d'un service en ligne, tel que celui mettant à la disposition des internautes une place de marché en ligne », et dès lors de tout prestataire d'un service de la société de l'information, « de prendre des mesures qui contribuent de façon effective, non seulement à mettre fin aux atteintes portées au moyen de cette place de marché, mais aussi à prévenir de nouvelles

[482] D. MOUGENOT, « L'action en cessation : les particularités d'un mécanisme atypique », *Actualités de droit commercial*, 2010, n° 2.
[483] O. MIGNOLET, Les actions en cessation, in *Les droits intellectuels, Répertoire Notarial,* Larcier, 2007, p. 568.
[484] C.J.U.E., 24 novembre 2011, *Scarlet c. Sabam*, C-70/10, § 31.

atteintes »[485]. La Cour consacre donc la possibilité des injonctions visant à prévenir des infractions futures qui peuvent être obtenues par les titulaires de droit mais tempère immédiatement ce principe par le rappel de l'impossibilité d'imposer une obligation générale de surveillance et de la nécessité pour ces injonctions d'être effectives[486]. C'est cette condition d'effectivité qui risque de poser des problèmes lors d'injonctions prévues pour le futur. La question se pose en matière d'étendue dans le temps d'une injonction imposée à l'encontre d'un prestataire technique, à savoir celle de la faisabilité ou non de listes ouvertes de DNS, d'URL ou d'adresses IP du site internet visé, sur base de critères à déterminer par le juge. Il est évidemment d'un grand intérêt pour les ayants droit de s'assurer qu'une fois le blocage d'un site autorisé par un juge, un site miroir de celui-ci ne rouvre pas dans l'heure du prononcé du jugement.

Pourrait-on, sur la base d'un premier jugement prévoyant que tel contenu est illicite et doit dès lors être bloqué, que dès qu'un nouveau site, avec un contenu semblable, apparaît, il soit bloqué et cela sans devoir repasser devant la justice ? La condition d'un tel blocage « préventif » serait alors la similitude du contenu. En effet, ce qui est bloqué, c'est un contenu illicite, lequel peut être accessible via un nom de domaine. Mais ce qui est effectivement visé c'est le contenu, le nom de domaine ou l'adresse IP n'étant finalement que des moyens de faire apparaître sur internet les informations illicites. S'il y a eu constat judiciaire de l'illicéité d'un contenu, qui apparaît sous tel nom de domaine, il sera procédé au blocage via ce nom de domaine – car pour le viser il faudra bien évidemment y faire référence sous tel nom de domaine –, ou sous tout autre nom sous lequel apparaitrait ce contenu, qui permettrait d'y accéder. Mais il ne faut pas perdre de vue que la doctrine et la jurisprudence insistent sur la précision de l'ordre de cessation[487]. Le juge ne peut se contenter d'interdire tout acte qui aurait le même effet que l'acte interdit ; ce qui importe c'est de sanctionner une pratique plus qu'un acte précis[488].

Concernant la nécessité de procéder à un *monitoring* judiciaire en matière de blocage de sites, nous pouvons citer l'exemple de l'action en justice pendante actuellement en France contre le groupe Allo qui entend, via l'article L336-2 du Code de propriété intellectuelle français[489], assurer le blocage des éventuels sites miroirs, et ce dans un souci d'efficacité. Cette disposition permet aux ayants droit de réclamer toute mesure à l'égard de toute personne pour faire cesser ou prévenir une atteinte à leurs intérêts. Leur solution viserait alors à juger, identifier et qualifier les sites miroirs du groupe Allo pour en exiger le blocage par DNS par les intermédiaires techniques, et les blocages subséquents se feraient sans passer par le juge, qui n'interviendrait qu'en aval pour valider les futures opérations.[490]

En Belgique, une telle disposition n'est pas prévue. La Cour d'appel d'Anvers, dans l'affaire *The Pirate Bay*, avait refusé de faire droit à la demande de la BAF de pouvoir ordonner aux FAI de bloquer, en plus de la liste fournie de noms de domaine définie, les autres extensions possibles de « (the)piratebay ». La BAF avait en tête de notifier plus tard aux FAI une liste complémentaire de noms de domaine à bloquer, via l'envoi d'un email. La Cour a décidé de limiter l'injonction à une liste limitative de noms de domaine. Une éventuelle extension des mesures demandées requerra une

[485] Arrêt *L'Oréal*, § 131.
[486] C. SMITS et J. LIGOT, *op. cit.*
[487] Voir entre autres O. MIGNOLET, « Procédures civiles et commerciales, les actions en cessation », in D. KAESMACHER (dir.), *Les droits intellectuels*, Bruxelles, Larcier, 2007, n° 721, p. 568.
[488] D. MOUGENOT, « L'action en cessation : les particularités d'un mécanisme atypique », *Actualités de droit commercial*, 2010, n° 50, p. 118.
[489] Article L336-1 du Code de Propriété Intellectuelle.
[490] M. REES, « HADOPI : avec TMG, déréférencement et blocage anticipatifs », *op. cit.*

nouvelle citation. L'article 584 du code judiciaire admet que l'action soit introduite par simple requête mais uniquement en cas d'absolue nécessité, ce que les juges interprètent strictement, la cour de cassation exigeant une urgence exceptionnelle[491].

Il faudrait dès lors insérer dans la législation nationale une disposition qui permettrait, une fois le constat judiciaire obtenu de l'illicéité de contenus présents sur un site internet, et suivant le contexte dans lequel cela a lieu, de procéder au blocage ou au retrait de ce contenu qui réapparaitrait sous un autre nom de domaine, URL ou adresse IP. Il apparaît, au regard des différents droits fondamentaux qui risqueraient d'être touchés, que si c'est un contenu bien spécifique qui est visé, et non pas son enveloppe, contenu qui aurait une première fois été déclaré illégal par un juge, que rien ne s'oppose à l'introduction d'une telle disposition dans le droit interne.

Aux Pays-Bas, une première décision du tribunal de La Haye[492] avait admis que les noms de domaine et les adresses IP utilisés par *The Pirate Bay* dont les FAI devaient bloquer l'accès pour leurs abonnés pourraient être étendus à des adresses similaires. Un appel a été interjeté contre cette décision. La Fondation De Brein a ensuite intenté une action contre d'autres fournisseurs d'accès pour étendre à leur encontre la première décision, ce qui a été accordé par une décision du 10 mai 2012, mais cette fois-ci sans valider la possibilité d'une extension de l'ordre de cessation. Toutefois, une décision récente du même tribunal du 25 mai 2012[493] a admis que cet ordre de cessation par lequel des intermédiaires étaient enjoints de bloquer l'accès au site *The Pirate Bay* par le biais de deux adresses IP[494], pouvait être étendu à une nouvelle adresse IP vers lequel le site illicite avait été transféré, sur requête unilatérale et sans entendre les FAI qui avaient refusé ce nouveau blocage sans décision d'un juge. Le juge n'a pas non plus jugé nécessaire de revenir sur les considérations de la première ordonnance de cessation, notamment sur la constatation des atteintes, l'urgence et la nécessité de la mesure demandée, ou l'impact sur la liberté d'expression, pour simplement ajouter cette nouvelle adresse IP aux adresses devant être bloquées par les FAI. Quinze jours seulement se sont écoulés entre le premier ordre de cessation et le jugement rendu sur requête unilatérale par identité de motifs, ce qui constitue une réponse très rapide au changement d'adresse IP sur laquelle opérait le site *The Pirate Bay*.

Si l'on peut comprendre la volonté des ayants droit de pouvoir adapter promptement l'ordre de cessation à la rapidité de réaction des contrefacteurs, l'intervention d'un juge paraît nécessaire, même si elle pourrait être facilitée, dans les cas où les adresses dont le blocage est demandé renvoie au même site et au même contenu illicite. L'extension de l'objet d'une injonction doit rester prévisible pour ses destinataires, respecter le principe de proportionnalité et ne pas se transformer en obligation de surveillance pour le FAI.

Se pose également la question de la réitération (ou *notice and stay down*). Lorsqu'une notification a été faite à un site, par exemple un hébergeur, de retirer tel contenu, qu'il procède effectivement à ce retrait, et que par la suite ce contenu réapparait, il ne peut lui être imposée une obligation générale de surveillance et l'on ne pourrait pas non plus condamner cet hébergeur pour ne pas s'être imposé à lui-même l'obligation de filtrer son réseau afin que ce contenu ne réapparaisse plus. De nombreuses décisions françaises avaient été dans le sens d'une condamnation de ces prestataires

[491] Cass., 13 juin 1975.
[492] Rb. 's Gravenhage, 11 janvier 2012, HA ZA 10-3184, http://zoeken.rechtspraak.nl/ detailpage.aspx?ljn= BV0549.
[493] Rb. 's Gravenhage, 25 mai 2012, KG RK 12-1126, disponible sur www.boek9.nl.
[494] Rb. 's Gravenhage, 10 mai 2012, KG ZA 12-156, http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BW5387.

qui ne filtraient pas d'eux-mêmes la réapparition d'un contenu déjà notifié, ce qui est contraire au droit européen. Il ne peut en effet être imposé au prestataire un système de surveillance généralisée pour éviter une réapparition. Il n'a pas à s'assurer lui-même qu'un contenu ne réintègre pas son site car cela ajouterait une condition parmi les conditions de l'exonération de responsabilité non prévue dans le texte. Rien n'empêche cependant le juge d'ordonner une telle mesure de filtrage, c'est ce que l'on appelle l'obligation particulière de surveillance, ciblée et temporaire. Le juge peut alors inviter le prestataire, pour l'avenir, à retirer tel contenu déterminé qui réapparaitrait. Mais en pratique, cela reviendrait souvent à procéder à un filtrage généralisé pour cibler la réapparition d'un seul contenu.

3. *Dans l'espace*

Qu'en est-il de la territorialité de l'action en cessation ? Nous pouvons pointer le caractère essentiellement territorial de l'action judiciaire en cessation, dont les effets sont strictement nationaux, ce qui implique que pour empêcher la circulation internationale d'une contrefaçon, il faut obtenir un jugement dans chacun des pays impliqués[495]. Cela ne participe pas à la baisse de la prolifération du piratage en ligne, les œuvres contrefaites pouvant circuler instantanément sur internet, dans le monde entier.

La mesure qui serait prise, peu importe sa forme, aura des effets extraterritoriaux, elle n'affectera pas uniquement le prestataire d'un pays donné, ni seulement ses utilisateurs. Dans ses conclusions dans l'affaire *Scarlet*, l'avocat général spécifia que « la mesure sollicitée, présentée comme une injonction adressée à une personne morale identifiée lui imposant la mise en place d'un système de filtrage et de blocage, est en réalité appelée à affecter durablement un nombre indéterminé de personnes morales ou physiques, de FAI ou d'internautes, de prestataires de services de la société de l'information et d'utilisateurs desdits services »[496], et qu'elle vise « l'ensemble des communications électroniques transitant par les services dudit FAI »[497]. L'effet est donc bien extraterritorial.

Dans son arrêt *Pammer et Hotel Alpenhof*, la Cour a jugé que « la simple accessibilité d'un site Internet sur le territoire couvert par la marque ne suffit pas pour conclure que les offres à la vente y affichées sont destinées à des consommateurs situés sur ce territoire »[498]. Cette décision concernait plus spécialement des règles spécifiques en matière de protection des consommateurs, mais elle peut être transposée *mutatis mutandis* dans notre cas d'application pour déterminer les règles en matière de for compétent. L'accessibilité sur un territoire d'un site web ne le rend pas *ipso facto* soumis au droit de ce territoire[499]. La Cour de justice avait donné un certain nombre de critères qualifiés d'indices possibles pour déterminer si une activité commerciale était dirigée vers un Etat membre particulier : la mention que le commerçant offre ses biens ou services dans des Etats nommément désignés ; la nature internationale des services proposés ; l'utilisation d'un nom de domaine de l'Etat visé ou l'utilisation de nom de domaine de premier niveau génériques (.com, .org, .eu) ; le fait pour un commerçant de recourir aux services d'un moteur de recherche qui indiquerait

[495] A. BERENBOOM, *Le nouveau droit d'auteur*, *op. cit.*, pp. 442 et 443.
[496] Conclusion affaire *Scarlet*, § 62.
[497] *Ibid.*, § 58.
[498] Arrêt *Pammer*, §69.
[499] Arrêt *eBay*, § 64.

de manière évidente sa volonté de viser une clientèle internationale, *etc.*[500], ou encore lorsqu'il y a une part importante d'œuvres belges dans l'offre proposée. Ces indices peuvent résulter de « toutes les expressions manifestes de la volonté de démarcher les consommateurs » dans l'Etat membre vers lequel l'activité est dirigée[501]. Dans son arrêt *eBay*, relatif à l'application territoriale du droit des marques, la Cour va simplement faire un renvoi aux juridictions nationales dans l'appréciation de l'existence d'indices pertinents pour conclure à la destination d'un service ou d'un bien, appréciation qui se fera au cas par cas[502].

En matière de détermination de la loi applicable, le choix peut se porter sur le pays d'émission de la contrefaçon ou le pays de sa réception par le public comme critère de rattachement[503]. Dans l'affaire *Google c. Copiepresse*, la Cour a décidé que « l'acte illicite est commis lorsque les œuvres protégées sont diffusées en Belgique sur le site Google.be, peu importe si elles ont été ''injectées'' automatiquement par des robots, prétendument situés à l'étranger », et consacre ainsi la thèse du pays de réception. Ce qui compte c'est la réception de la copie par le consommateur local[504]. Or pour certains auteurs, il faut également tenir compte du lieu du fait générateur du dommage pour déterminer la loi applicable, et dès lors prendre en compte « le point de contact que constitue, dans le cas de la transmission numérique sur demande, l'acte déclenchant la mise en œuvre du droit exclusif »[505]. Toujours selon cet auteur, « l'acte contrefaisant consiste dans le seul fait de mettre les (contenus) numérisés à la disposition du public sur le réseau, indépendamment de la réception effective par les internautes »[506]. La règle générale sur laquelle il faudrait se baser serait celle de l'article 5.2 de la Convention de Berne qui contient le principe de la loi du fait générateur[507]. Or cela pose question en termes de risque d'une délocalisation des contrefacteurs vers des pays qui offrent une protection plus faible aux auteurs. La cour d'appel de Bruxelles a d'ailleurs déclaré que «privilégier la loi de l'injection peut conduire à décerner un brevet d'impunité au contrefacteur (…), ce qui est manifestement contraire au but recherché par la Convention de Berne ». Les règles ne sont pas tout à fait claires mais il apparaît que retenir la théorie du pays de réception en matière de contrefaçon au droit d'auteur sur internet serait plus judicieux.

La cour d'appel de Bruxelles a admis la compétence du juge, lors d'une action en cessation, pour des atteintes au droit d'auteur commises à l'étranger[508], ce qui justifie qu'une action puisse être intentée en Belgique contre des intermédiaires pour faire cesser des faits commis en dehors du territoire belge ou bloquer l'accès à des sites étrangers.

[500] Affaire *Pammer*, §§ 81 à 84.
[501] *Ibidem*, § 80.
[502] Affaire *eBay*, § 65.
[503] A. DE FRANCQUEN, L'arrêt *Google contre Copiepresse* et le choix de la loi applicable en matière d'atteinte au droit d'auteur sur Internet, *R.D.T.I.*, p.61.
[504] J . C . GINSBURG, note d'observations sous TGI, Paris, 20 mai 2008, RDTI, p. 510.
[505] A. LUCAS, « La loi applicable à la mise en ligne d'œuvres protégées par le droit d'auteur », La semaine juridique, n° 9‑ 10, 1er mars 2010, n° 247, p. 467.
[506] *Idem*.
[507] Note sous Bruxelles, 5 mai 2011, A. LUCAS, *Propr . Intell.*, juillet 2011, n° 40, pp. 311 et 312.
[508] Bruxelles, 30 septembre 2002, *A&M*, 2003, p. 205.

C. Obligation de tenir compte d'autres droits et libertés

Lors de la mise en place de telles mesures de filtrage et de blocage, il faut bien sûr tenir compte d'autres droits et libertés. Les mécanismes de filtrage et de blocage sont susceptibles de porter atteinte au droit à la liberté d'expression, au droit à la liberté d'entreprise ainsi qu'au droit à la protection des données personnelles. Toutefois, des limitations peuvent être apportées à ces droits, sous réserve qu'elles respectent un certain nombre de conditions, comme l'indiquent la Charte des droits fondamentaux et la Convention EDH. Il faut également s'assurer que la liberté d'expression et d'information ne soit pas remise en cause par l'adoption de telles mesures. Ce point fera l'objet d'un autre chapitre du présent rapport.

La question de savoir jusqu'où les fournisseurs d'accès à internet peuvent interférer avec les contenus qu'ils transmettent et reçoivent, relève de la question de la neutralité du net, qui sera également traitée plus loin.

§5. Le droit d'information de l'article 86*ter* de la LDA

L'article 86*ter* de la LDA, introduit par la loi du 9 mai 2007, prévoit dans son paragraphe 3 une mesure d'injonction de fournir à la partie qui introduit une action toutes les informations et données relatives à l'origine et aux réseaux de distribution des biens ou services contrefaisants. Cet article est la transposition de l'article 8 de la directive 2004/48 sur le respect des droits de propriété intellectuelle. L'objectif de ce droit d'information est précisé par le considérant 21 de ladite directive : « obtenir des informations précises sur l'origine des marchandises ou des services contrefaisants, les circuits de distribution et l'identité des tiers impliqués dans l'atteinte ».

La notion d'intermédiaires visés par cette obligation de communiquer correspond à « toute personne qui a été trouvée en possession de biens contrefaisants à l'échelle commerciale, qui a été trouvée en train d'utiliser des services contrefaisants à l'échelle commerciale ou qui a été trouvée en train de fournir, à l'échelle commerciale, des services utilisés dans des activités contrefaisantes ». La fin de cette définition vise les intermédiaires dont les services sont utilisés par l'auteur de l'atteinte. En conséquence, on peut y inclure les fournisseurs d'accès, les hébergeurs de toute sorte, les prestataires de paiement ou DNS.be. Dans ce dernier cas toutefois, on soulignera que les informations d'identification détenues par DNS.BE sont publiques[509], ce qui rend une demande d'information à son encontre sans réel intérêt pratique.

Les informations qui peuvent être demandées sont celles de l'article 8 de la directive, c'est-à-dire les noms et adresses des producteurs, fabricants, distributeurs, fournisseurs et autres détenteurs antérieurs des marchandises ou des services ainsi que des grossistes et des détaillants, ainsi que les quantités et les prix. En plus d'être adressée à l'auteur de l'atteinte, la mesure peut l'être à toute autre personne qui aurait été trouvée « en possession des biens contrefaisants à l'échelle commerciale », « en train d'utiliser des services contrefaisants à l'échelle commerciales », ou « en train de fournir à l'échelle commerciale des services utilisés dans des activités contrefaisantes ». Le

[509] Voir le registre « whois » dont les données sont accessibles via le site web http://www.dns.be

but étant la fourniture d'information dans le cadre de la collecte d'éléments utiles en vue d'entamer des poursuites, la personne visée par la mesure ne doit donc pas nécessairement avoir commis l'acte de contrefaçon[510]. L'injonction de l'article 86*ter* ne peut être ordonnée que lorsqu'il y a eu constatation préalable d'une atteinte par le juge[511], tel que cela ressort de l'objectif de ce droit, des termes de l'article 8 de la directive que cet article transpose et de son économie générale, même si cela n'est pas expressément mentionné dans la directive[512]. Ne pas suivre cette interprétation de l'article 8 de la directive reviendrait à glisser du droit d'information vers le droit de la preuve et entrainerait une confusion entre ces notions[513]. Le demandeur ne peut se fonder sur de simples allégations, ce qu'implique la nécessité de justification de la mesure[514]. L'exigence de constatation préalable de l'atteinte par le juge empêche de fait la contestation de la mesure[515]. En plus d'être justifiée, il faut que la mesure soit proportionnée.

La Cour de justice a eu l'occasion de se prononcer à propos de la compatibilité d'une loi nationale similaire, la loi suédoise IPRED[516]. En Suède, la directive 2004/48 a été transposée dans la législation suédoise par une loi du 26 février 2009. Cette loi insère un nouvel article dans la loi suédoise sur le droit d'auteur qui prévoit que lorsqu'une atteinte au droit de propriété intellectuelle est établie, il peut être ordonné par un tribunal la communication d'informations sur l'origine et les réseaux de distribution d'œuvres contrefaites, et ce même aux ayants droit. Les caractéristiques de cette obligation de communiquer sont que, premièrement, la demande peut émaner du titulaire du droit, son ayant droit ou quiconque qui jouit d'un droit légal d'exploitation de l'œuvre, et deuxièmement, cette communication ne peut être ordonnée que si les informations demandées sont susceptibles de faciliter l'enquête sur la violation du droit ou l'atteinte au droit en cause[517]. Cette injonction de communiquer ne peut être ordonnée que si les raisons la motivant sont d'un intérêt supérieur aux inconvénients ou autres préjudices qu'elle peut entrainer pour son destinataire ou tout autre intérêt qui s'y oppose[518].

La question que la Cour a eu à examiner était celle de savoir si cette disposition permet d'imposer à un fournisseur d'accès à internet de communiquer à un ayant droit, dans une procédure civile, l'identité de l'abonné à qui l'adresse IP suspectée a été attribuée[519]. Ce que vise la loi suédoise est donc la transmission de données, dans le cadre d'une procédure civile, dans le but de faire constater une atteinte aux droits de propriété intellectuelle[520]. Une demande de communication de données à caractère personnel pour assurer la protection effective des droits d'auteur relève de la directive 2004/48[521], cet article de la loi suédoise autorisant l'implémentation d'une obligation de

[510] B. MICHAUX, Commentaire de l'article 86ter de la LDA, in *Hommage à Jean Corbet. La loi belge sur le droit d'auteur – Commentaire par article*, Bruxelles, Larcier, 2008, p. 472.
[511] *Doc. Parl.*, Chambre, sess. ord., 2006-2007, n° 51-2943 et 2944/1, 33.
[512] Exposé des motifs du projet de loi relatif aux aspects civils de la protection des droits de propriété intellectuelle, 26 février 2007, Doc 2943/001, p. 33.
[513] *Idem*, p. 34.
[514] Avis du Conseil d'Etat, *Doc. parl.*, Chambre, sess. ord.2006/07, n° 51-2943 et 2944/1, 114.
[515] B. MICHAUX, *op. cit.*, p. 473.
[516] Voir premier chapitre du rapport.
[517] Article 53*quater* loi suédoise.
[518] Article 53*quinquies* de la loi suédoise.
[519] Arrêt *Bonnier*, § 36.
[520] *Ibidem*, § 44.
[521] Arrêt *Promusicae*, §58.

transmission de données à caractère personnel à des personnes privées pour leur permettre la poursuite des atteintes au droit d'auteur[522]. La Cour va juger que si la loi :

- exige que pour qu'une injonction de communiquer les données en cause puisse être ordonnée des indices réels d'atteinte à un droit de propriété intellectuelle sur une œuvre existent ;
- exige que les informations demandées soient susceptibles de faciliter l'enquête sur l'atteinte ou la violation du droit d'auteur ;
- exige que les raisons motivant cette injonction soient d'un intérêt supérieur aux inconvénients ou aux autres préjudices qu'elle peut entrainer pour son destinataire[523] ;
- s'applique aux personnes ayant qualité pour agir ;
- peut pondérer les intérêts opposés en présence, en fonction des circonstances de chaque espèce et en tenant compte des exigences résultant du principe de proportionnalité[524] ;

elle peut être considérée comme susceptible d'assurer un juste équilibre entre la protection du droit de propriété intellectuelle et la protection des données à caractère personnel[525]. Cette ligne de conduite donnée par la Cour de justice permet de savoir ce qu'il faut comme condition dans une loi qui prévoirait une injonction de communication envers les fournisseurs d'accès à internet au bénéfice des ayants droit pour s'assurer de la proportionnalité et de la validité de celle-ci.

L'article 124 de la loi du 13 juin 2005 sur les communications électroniques permet la communication des données d'identification des internautes uniquement si une loi le permet, ce que fait l'article 86*ter* de la LDA. Or, comme nous l'avons vu, le droit d'information de l'article 86*ter* ne peut être exercé que dans le cadre d'une action judiciaire, l'atteinte à un droit de propriété intellectuelle devant être constatée, ce qui empêche tout traitement de données à caractère personnel qui se déroulerait en dehors d'un tel cadre. L'article 8 de la directive rend possible d'exiger une communication de données sur base d'indices réels d'atteinte, et va donc moins loin que la loi belge. C'est ce qui ressort de l'arrêt Bonnier examiné ci-dessus[526].

Ce qui pose question dans l'implémentation d'un tel système d'injonction de communication dans le cadre de la mise en place d'un système répressif, est qu'une adresse IP n'assure pas le ciblage de la personne qui est réellement à la source de l'infraction aux droits d'auteur car cette adresse est en réalité reliée à l'abonné de la connexion qui n'est peut-être pas responsable de l'acte en cause. C'est en ce sens que s'est prononcé l'avocat général dans l'affaire *Bonnier.* En effet, selon lui, « dans l'affaire au principal, il s'agit des nom et adresse d'un abonné, qui sont à identifier sur la base d'une adresse IP. Il s'ensuit que nous nous trouvons dans le champ d'application des règles relatives à la protection des données à caractère personnel. Il convient néanmoins de rappeler que l'identité de la personne susceptible d'avoir commis une atteinte à des droits de propriété intellectuelle ne peut être établie sur la seule base de l'adresse IP lorsque plusieurs personnes peuvent utiliser l'accès au réseau identifié par cette même adresse IP. Cela est le cas concernant par exemple les réseaux sans fil dépourvus de protection efficace, le détournement d'ordinateurs connectés à Internet, ainsi que les situations dans lesquelles plusieurs personnes peuvent utiliser le même ordinateur. »[527]

[522] *Ibidem*, §§ 54 et 55.
[523] Arrêt *Bonnier,* § 58.
[524] *Ibidem*, § 59.
[525] *Ibidem*, § 60.
[526] Voir *infra* pour les développements en matière de protection des données.
[527] Conclusions avocat général, affaire *Bonnier*, §§ 42 et 43.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

La loi belge ne résout pas la problématique de la collecte des adresses IP avant toute introduction d'une action judiciaire, car il est nécessaire que l'atteinte au droit d'auteur soit préalablement constatée par un juge. Comme nous aurons l'occasion de l'étudier de manière approfondie au point suivant du présent rapport, les adresses IP constituent des données à caractère personnel au sens de l'article 2, point a), de la directive 95/46 sur le traitement des données à caractère personnel. Dès lors, « la surveillance des comportements des internautes et la collecte de leur adresse IP équivalent à une interférence dans leur droit au respect de la vie privée et de leurs correspondances »[528].

§6. Autre rôle des fournisseurs d'accès à internet

I. Dans le cadre du mécanisme de réponse graduée

Pour mettre en œuvre un tel mécanisme, il est nécessaire d'identifier les auteurs présumés des contraventions au droit d'auteur. Nous aurons l'occasion de voir dans le chapitre suivant ce que cela implique en termes de protection des données à caractère personnel et de vie privée. C'est au niveau de l'identification des internautes que les intermédiaires techniques auront un rôle à jouer. Il s'agit ici de procéder à une stratégie plus indirecte de coopération avec les fournisseurs d'accès à internet envers leurs clients et non plus une volonté de les rendre responsables de ce qu'il se passe via leurs services. Outre l'identification des clients à la demande des ayants droit ou d'une instance judiciaire ou administrative, il leur sera demandé d'envoyer des lettres d'avertissement – élément clé dans le mécanisme de réponse graduée – et de couper ou restreindre la connexion des internautes récidivistes selon que l'on se trouve ou non dans un mécanisme de réponse graduée intégral ou seulement d'avertissement.

L. EDWARDS relève trois moyens d'obtenir la coopération des fournisseurs d'accès à internet : une participation volontaire, une participation découlant d'un jugement intervenant dans une action en justice et la participation imposée par le législateur[529]. Nous avons vu dans la première partie du rapport des exemples de ces trois types d'intervention. Le degré d'implication des fournisseurs variera en fonction du choix de tel ou tel modèle, avec comme principales questions le coût de l'imposition d'un tel mécanisme, son imputation, et des considérations plus organisationnelles.

Dans le cadre de la réponse graduée limitée aux avertissements, une fois la récolte d'adresses IP d'internautes soupçonnés de télécharger illégalement réalisée, le fournisseur reçoit une notification l'enjoignant d'envoyer une lettre d'avertissement à ses clients dont il a levé l'anonymat. Selon le système en place, il aura parfois seulement à identifier le client qui se cache derrière l'adresse IP et de transmettre cette information à l'ayant droit qui se chargera lui-même de l'envoi des lettres. Il faut savoir que le fournisseur d'accès à internet est le seul qui peut faire correspondre l'adresse IP avec le nom et les coordonnées d'un internaute, raison pour laquelle il est fait appel à lui dans la réponse graduée.

[528] CEPD, Avis du 22 février 2010 sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC).
[529] L. EDWARDS, *op. cit.*, p. 26.

La charge du coût qui pèsera sur les fournisseurs va dépendre du choix de la méthode, le processus d'identification et d'envoi d'avertissements ayant un coût important, surtout pour les petites structures. Le Gouvernement anglais a estimé le coût pour les fournisseurs entre 290 et 500 millions de Livres sterling sur dix ans[530], coût qui inclut l'identification, l'envoi de notifications, la gestion de *call centers* pour répondre aux questions, et l'investissement dans des équipements pour gérer le système[531]. Toujours au Royaume-Uni, il a été décidé d'une clé de répartition 25/75 entre les fournisseurs et les ayants droit. En France, le gouvernement a prévu un budget annuel de 6,7 millions d'euros pour le fonctionnement de la Haute autorité. L'imposition de telles charges financières aux fournisseurs – et parfois pas sur tous en cas d'implication volontaire ou de participation imposée suite à un litige privé (cf. Eircom) – peut avoir des conséquences en terme de concurrence et de liberté d'entreprise[532].

Outre le problème de répartition des coûts, il faut pouvoir assurer au fournisseur d'accès des moyens suffisants pour contrôler si la demande des ayants droit d'envoyer des avertissements est bien fondée, et des garanties en cas d'erreurs qu'ils commettraient, lors de l'identification des internautes par exemple. Il faudrait pouvoir prévoir ici aussi une disposition qui sanctionnerait les demandes fausses ou illégitimes faites par les ayants droit comme cela est déjà le cas aux USA pour la procédure de *notice and takedown*[533] et dont nous avions déjà suggéré ce parallèle dans notre analyse de la procédure de notification et de retrait.

II. Dans le cadre d'un régime d'autorisation des échanges

Dans les modèles d'autorisation des échanges d'œuvres en *peer-to-peer* contre rémunération, les intermédiaires jouent généralement un rôle non négligeable, en tant que débiteurs de la rémunération perçue auprès des internautes à titre de compensation des communications et reproductions d'œuvres effectuées. Il est en effet généralement proposé que cette rémunération soit prélevée sur le prix des abonnements ADSL.

La justification économique de cette implication est fondée sur le fait que les fournisseurs de services de connexion fournissent un moyen indispensable de s'adonner aux échanges en *peer-to-peer*. Sans Internet à large bande, des téléchargements réguliers de musiques ou de films seraient impossibles. Certains économistes dénoncent même un détournement de l'utilité de l'industrie des contenus par celle des réseaux Internet haut-débit, qui ont pu se déployer grâce aux utilisations du *peer-to-peer*[534], ce qui pourrait justifier un retour économique sous forme d'une taxe ou d'une rémunération des auteurs par les fournisseurs d'accès.

[530] OECD, "The economic and social role of internet intermediaries", avril 2010, disponible sur http://www.oecd.org/internet/interneteconomy/44949023.pdf
[531] L. EDWARDS, *op. cit.*, p. 44.
[532] Voir *infra*.
[533] L. EDWARDS, *op. cit.*, p. 38.
[534] O. BOMSEL, *Enjeux économiques de la distribution des contenus,* CERNA, 2004, disponible sur http://www.cerna.ensmp.fr/Documents/OBetalii-P2P.pdf.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

A. Rôle des fournisseurs d'accès internet en cas de licence légale

Le rôle des FAI dans les propositions d'une licence globale autorisant les échanges d'œuvres en *peer-to-peer* dépend du type de régime d'autorisation proposé.

Dans le cas d'une licence légale ou non volontaire, la rémunération qui serait versée par le FAI est fondée sur une obligation légale par laquelle le législateur impose le versement d'une compensation pour le dommage subi par les ayants droit du fait des échanges de leurs œuvres.

A l'instar de la rémunération pour copie privée, les débiteurs de cette rémunération qui serait perçue sur le prix des abonnements à Internet, ne sont pourtant pas les personnes responsables des actes de reproduction et de communication des œuvres qui enclenchent la nécessité d'une compensation pour les auteurs. La Cour de Justice de l'Union européenne a récemment admis, s'agissant de la copie privée, que « compte tenu des difficultés pratiques pour identifier les utilisateurs privés ainsi que pour les obliger à indemniser les titulaires des droits du préjudice qu'ils leur causent (…), il est loisible aux États membres d'instaurer, aux fins du financement de la compensation équitable, une «redevance pour copie privée» à la charge non pas des personnes privées concernées, mais de celles qui disposent d'équipements, d'appareils et de supports de reproduction numérique et qui, à ce titre, en droit ou en fait, mettent ces équipements à la disposition de personnes privées ou rendent à ces dernières un service de reproduction »[535]. Les juges européens ajoutent que c'est l'activité de mise à la disposition d'équipements de reproduction qui « constitue la prémisse factuelle nécessaire pour que les personnes physiques puissent obtenir des copies privées [et que] rien ne fait obstacle à ce que ces redevables répercutent le montant de la redevance pour copie privée dans le prix de la mise à disposition desdits équipements »[536].

Par analogie, faire reposer la rémunération des auteurs pour les échanges *peer-to-peer* sur les fournisseurs d'accès Internet répondrait à une nécessité pratique. Cette rémunération étant en toute probabilité répercutée sur leurs abonnés[537], la charge de la redevance sera en définitive supportée par les personnes échangeant les œuvres, devenant les «redevables indirects» de la compensation équitable. Les opérateurs fournissant une connexion internet à leurs abonnés ne pourraient en conséquence se soustraire au paiement de la rémunération équitable qui leur serait imposée, dans le cadre d'une licence légale, au motif que celle-ci serait due uniquement et directement par les internautes utilisant leur service.

B. Rôle des fournisseurs d'accès dans une autorisation basée sur la gestion collective

Lorsque le modèle d'autorisation repose sur une gestion collective, qu'elle soit favorisée par une gestion collective obligatoire ou une licence collective étendue, un contrat de licence est proposé par les sociétés de gestion collective. Les propositions en ce sens envisagent généralement que les

[535] C.J.U.E., 21 octobre 2010, *Padawan*, C-467/08, § 46.
[536] *Ibidem*, § 48.
[537] Sauf dans le cas de la proposition de loi Ecolo/Groen qui refuse que les fournisseurs d'accès augmentent d'autant le coût de la connexion à Internet.

cocontractants des sociétés d'auteurs et de droits voisins soient les fournisseurs d'accès internet. Deux modèles sont en réalité possibles. Soit les FAI sont parties au contrat de licence conclu avec les sociétés de gestion collective, soit ce sont les internautes qui sont les preneurs de cette licence les autorisant à échanger les œuvres.

Dans le premier cas, le contrat entre fournisseurs d'accès et sociétés de gestion a pour objet de permettre à un tiers, non partie à l'accord, de bénéficier d'une autorisation consentie par l'un des cocontractants. Dans ce schéma, que l'on retrouve dans tous les modèles d'autorisation du *peer-to-peer* non basés sur la licence légale, le fournisseur d'accès à Internet sert de relais entre les sociétés de gestion et les abonnés Internet tout en s'obligeant à rétribuer les titulaires de droits. Il s'engage également au profit de ses abonnés Internet puisque le contrat crée la faculté, à leur profit, d'échanger des œuvres sur les réseaux *peer-to-peer*. De son côté, la société de gestion s'engage en effet à autoriser ce type d'échanges et donc à ce que les internautes soient autorisés à reproduire et communiquer au public des œuvres dans le cadre de ces échanges, dans les limites précisées par l'accord.

Il s'agirait toutefois d'un contrat un peu particulier. Alors que l'octroi d'une licence par une société de gestion collective a généralement pour objectif de donner l'autorisation nécessaire à l'accomplissement d'actes de reproduction et/ou de communication au public couverts par le droit d'auteur, ce contrat conclu avec les FAI n'a pas pour objectif d'autoriser ceux-ci à commettre de tels actes d'exploitation des œuvres. Les fournisseurs d'accès ne sont pas directement à l'origine d'actes de communication au public ou de reproduction des œuvres. Quant au droit de reproduction, il est vrai que toute diffusion en ligne d'une œuvre implique des fixations provisoires, aussi bien au niveau de l'internaute que des prestataires et des intermédiaires. Les œuvres échangées sont fixées temporairement sur les serveurs des fournisseurs d'accès à Internet afin d'être diffusées sur les réseaux *peer-to-peer*. Quoi qu'il en soit, la transposition (obligatoire) de l'exception de reproduction technique provisoire par le législateur belge[538] immunise quelque peu ces actes de copies techniques et transitoires pour autant qu'elles soient indispensables au processus technique de transmission des contenus sur Internet et n'aient pas de signification économique indépendante, ce qui paraît être le cas dans notre contexte. Ainsi, les fournisseurs d'accès à Internet, en l'état actuel du droit, ne paraissent pas effectuer d'actes requérant une autorisation des ayants droit pour la transmission des œuvres échangées en *peer-to-peer* par leurs abonnés.

En conséquence, la cause de leur présence comme cocontractants des titulaires de droit d'auteur peut difficilement être trouvée dans leur responsabilité propre pour les transferts de fichiers protégés.

Seule la figure de la stipulation pour autrui pourrait qualifier ce contrat entre ayants droit et FAI et justifier de la cause du contrat dans le chef de ces derniers[539]. Les conditions spécifiques de ce modèle contractuel sont que le stipulant et le promettant doivent avoir la commune intention de faire naître un droit au profit d'un tiers bénéficiaire (soit l'autorisation des échanges pour les

[538] Art. 21 § 3 de la LDA.

[539] Pour plus de développements sur l'application de la stipulation pour autrui à un tel régime d'autorisation, voir C. COLIN, Etude de faisabilité de systèmes de licences pour les échanges d'œuvres sur internet, Etude pour la SACD/SCAM, 2011, p. 68 et suiv.

internautes) et que les tiers bénéficiaire puissent être déterminés ou déterminables (ce sont les abonnés ou futurs abonnés du fournisseur d'accès).

En outre, la stipulation pour autrui doit nécessairement être accessoire par rapport au contrat principal signé entre le stipulant et le promettant, qu'il soit à titre gratuit ou onéreux (vente, donation, assurance…)[540], l'existence et la vie de ce contrat accessoire étant tributaires de celles du contrat principal[541]. Cette exigence d'un contrat principal risque de constituer un obstacle à l'application du modèle de la stipulation pour autrui à un contrat entre les titulaires de droit d'auteur et de droits voisins et les fournisseurs d'accès à Internet. La difficulté va résider dans la délimitation de l'objet du contrat principal entre les ayants droit et les fournisseurs d'accès à Internet puisqu'il faudrait qu'une obligation spécifique les lie et qu'intervienne seulement après, en tant qu'accessoire, l'objet de la stipulation pour autrui. Les ayants droit pourraient renoncer à poursuivre les abonnés des fournisseurs d'accès à Internet se livrant à des échanges illégaux sur les réseaux *peer-to-peer*, mais quelle serait la contrepartie contractuelle propre des fournisseurs d'accès ?

La jurisprudence a toutefois tendance à interpréter l'exigence d'un contrat principal entre le promettant et le stipulant de façon généreuse. Il ne serait en effet pas nécessaire que le promettant s'engage à exécuter une obligation au profit du stipulant. Il suffirait que le stipulant « joue un rôle juridique propre dans la relation contractuelle avec le promettant, fût-ce en qualité de débiteur »[542], comme par exemple « dans le cadre d'un contrat d'assurance sur la vie contracté au profit d'un tiers, [où] la condition est remplie du seul fait de l'obligation du stipulant de payer les primes d'assurance »[543]. En somme, il pourrait être concevable que le fournisseur d'accès à Internet s'engage seulement à rétribuer les titulaires de droits. Du seul fait de ce rôle de débiteur du fournisseur d'accès à Internet vis-à-vis des sociétés collectives, la stipulation pour autrui au profit des abonnés Internet pourrait être admise. On peut également imaginer que la stipulation pour autrui, sous forme de l'autorisation des échanges au bénéfice des abonnés, s'accroche à un contrat principal liant les fournisseurs d'accès et les sociétés de gestion pour une exploitation des œuvres que feraient ceux-ci dans un autre service proposé (vidéos à la demande, câblodistribution, etc.).

Une deuxième possibilité qui éviterait cette construction contractuelle hasardeuse basée sur la stipulation pour autrui consisterait en ce que les FAI restent un tiers au contrat de licence et se contentent de transmettre les contrats proposés par les ayants droit à leurs abonnés, en sus du contrat d'accès à Internet. Cette solution aurait le mérite de ne pas impliquer juridiquement et financièrement les fournisseurs d'accès – ils restent un tiers au contrat – et de laisser aux abonnés Internet la possibilité de choisir ou non le système mis en place par les sociétés de gestion collective. A première vue, ce système serait nécessairement optionnel pour les abonnés Internet, ce qui présente l'avantage de permettre aux internautes qui ne pratiquent pas les échanges d'œuvres sur les réseaux *peer-to-peer* de rester en dehors du mécanisme, le contrat de licence étant une option dans le contrat plus général d'abonnement à Internet[544]. Toutefois si la liberté de choix laissée à

[540] P. WERY, *Droit des obligations, Théorie générale du contrat*, Vol. 1, *op. cit*., n° 869, p. 736.
[541] *Ibid.,* n° 74, p. 93.
[542] S. BAR, « La stipulation pour autrui », *op. cit*., spéc. p. 264.
[543] S. BAR, « La stipulation pour autrui », *op. cit*., spéc. p. 264.
[544] Pour une opinion contraire, voir Ph. AIGRAIN, *Internet et Création, Comment reconnaître les échanges sur internet en finançant la création*, In Libro Veritas, 2008, spéc. p. 54, qui considère que tous les internautes doivent contribuer au financement de la création qui enrichit Internet.

l'abonné Internet permet d'éviter de mutualiser le financement de la rémunération des auteurs et autres titulaires de droits, il convient de rester prudent quant au succès de l'opération sur base du simple volontariat. Vont-ils délibérément souscrire à un système d'autorisation payant, alors qu'ils pensent que les risques de sanctions s'ils continuent les échanges illégaux sont minimes ? La proposition d'une solution contractuelle d'autorisation optionnelle pour les internautes ne devrait pas être exclusive d'éventuelles sanctions que le système belge mettrait en place à l'encontre des internautes.

Quel que soit le modèle contractuel plébiscité, l'implication des FAI repose sur leur seule volonté, soutenue, dans le premier cas, par le principe d'autonomie de la volonté et la liberté contractuelle. Le prélèvement d'une rémunération sur les abonnements Internet et son versement aux ayants droit comporteront des coûts administratifs. En outre, nombreux sont les FAI qui souhaitent développer leurs propres offres légales de contenus en ligne, ce qui ne les motiverait pas à faire la promotion du système d'autorisation proposé auprès de leurs abonnés, alors envisagé comme une concurrence à leurs propres services.

A défaut d'une implication volontaire des fournisseurs d'accès à Internet dans des négociations dans un système d'autorisation des échanges non-commerciaux en *peer-to-peer* contre rémunération, on peut songer à une intervention législative imposant une telle implication ou, à tout le moins établissant un cadre de négociation.

Le législateur pourrait-il imposer aux fournisseurs d'accès à Internet de négocier avec les sociétés de gestion collective ? Rappelons qu'on se trouve là dans une situation inédite où les fournisseurs d'accès à Internet ne sont pas demandeurs d'une licence et où il faudrait la leur imposer, et où ils ne sont pas davantage débiteurs d'une rémunération mise à leur charge par la loi. Les commissions existantes en matière de droit d'auteur ne sont pas d'un grand secours, car elles consistent généralement en un forum de négociation de la rémunération afférente à une licence non-volontaire. [545]

La proposition de loi relative au *peer-to-peer* déposée par le sénateur Richard Miller impose, en son article 12, la conclusion d'un accord entre fournisseurs d'accès et sociétés de gestion pour autoriser les échanges d'œuvres par les internautes dans certaines limites. En cas d'échec des négociations, trois médiateurs seraient désignés pour aider à l'aboutissement des celles-ci et formuler des propositions. Le rôle ainsi attribué aux fournisseurs d'accès à Internet n'est toutefois pas précisé : il peut être celui d'un débiteur des rémunérations envisagées en contrepartie des échanges qui seraient autorisés ou celui d'un intermédiaire dans le contrat d'autorisation conclu en réalité entre les ayants droit et les internautes.

La proposition de loi écologiste impose également une négociation contractuelle entre sociétés de gestion collective et fournisseurs d'accès internet pour « permettre l'échange par leurs clients à [sic] des fichiers dont le contenu est protégé par le droit d'auteur »[546]. A défaut d'accord toutefois, les

[545] Voir par exemple la commission organisée par l'article 42 LDA en matière de droit de rémunération des titulaires de droits voisins. F. BRISON, « Commentaire de l'article 42 », in F. BRISON et H. VANHEES (eds.), *La loi belge sur le droit d'auteur – Commentaire par article – Hommage à Jan Corbet*, Larcier, 2ème édition, 2008, p. 240.
[546] Article 78-1 de la proposition de loi 5-590/1.

rémunérations seraient fixées par le Roi, ce qui emprunte davantage au système de licence non-volontaire qu'à une libre négociation contractuelle.

Dans ces deux propositions de loi, le législateur enclenche et impose le mécanisme de négociation entre les titulaires de droit d'auteur et de droits voisins et les fournisseurs de connexion Internet. L'idée est intéressante, mais elle bat en brèche un principe fondamental de notre droit, qui est la liberté de contracter ou de ne pas contracter. Y déroger suppose la poursuite d'un intérêt public important ou à tout le moins mérite d'être justifié.

Une autre solution serait que le législateur institue un cadre plus large aux négociations en créant une commission relative à Internet, qui rassemblerait des représentants des titulaires de droit d'auteur et de droits voisins, des internautes et consommateurs et des fournisseurs d'accès. Au sein de cette commission, des discussions pourraient avoir lieu sur une éventuelle légitimation des échanges *peer-to-peer*. Y inclure les consommateurs permet d'élargir la discussion aux réels utilisateurs des œuvres et éventuellement, de ne faire des fournisseurs d'accès à Internet que les intermédiaires à un contrat de licence conclu entre les ayants droits et les internautes (voir *supra*). L'association de consommateurs Test-Achat s'est d'ailleurs récemment déclarée favorable à la mise en place d'une licence négociée[547].

C. Rôle des fournisseurs d'accès dans un régime parafiscal pour la création sur Internet

En France, récemment, la SACEM a émis l'idée d'imposer une taxe aux fournisseurs d'accès à Internet en prélevant quelques euros sur les abonnements Internet. L'objectif est de compenser les pertes des filières musicale et cinématographique de manière proportionnelle au téléchargement illégal. Cette compensation aurait vocation à diminuer au fur et à mesure que le téléchargement illégal s'amenuiserait[548]. Il faut noter qu'en 2007, la France a déjà instauré une ressource fiscale prélevée sur les fournisseurs d'accès à Internet pour le compte de soutien géré par le CNC au profit de la production cinématographique[549]. Lors de sa campagne pour les élections présidentielles, François Hollande a également avancé l'idée d'une contribution financière des fournisseurs d'accès, moteurs de recherche et plateformes d'hébergement de contenu en faveur de la création.

La SABAM s'est elle aussi prononcée en faveur d'une implication financière des fournisseurs d'accès en guise de compensation du préjudice causé aux auteurs par l'utilisation de leurs réseaux pour les

[547] Audition concernant les propositions de loi Ecolo et MR, sénat de Belgique, 11 mai 2011. Voir également sur le site de Test-Achats : « Le débat ne fait que débuter et Test-Achats entend être partie prenante à celui-ci, dans la recherche d'un système équilibré où l'internaute puisse bénéficier d'une offre culturelle en ligne diversifiée et de qualité, mais également dans lequel les auteurs seraient équitablement rémunérés. »

[548] Se reporter à http://www.pcinpact.com/actu/news/62483-HADOPI-sacem-taxe-abonnement-internet.htm. Pour sa part, le rapport ZELNIK (Rapport remis au Ministre de la Culture et de la Communication par MM. Patrick ZELNIK, Jacques TOUBON et Guillaume CERUTTI, janvier 2010, disponible sur http://www.culture.gouv.fr/mcc/Actualites/A-la-une/Remise-du-rapport-de-la-mission-creation-et-internet) a écarté une telle hypothèse car elle « présente en effet un aspect rédhibitoire en ce qu'elle établit un surcoût pour les consommateurs sans leur apporter le moindre avantage » (spéc. p. 11).

[549] Cf. le rapport ZELNIK, *op. cit*., spéc. p. 8.

échanges en *peer-to-peer* en exigeant de ceux-ci le paiement d' « une juste rémunération pour la diffusion et l'exploitation sur internet des œuvres protégées »[550].

Cette contribution financière des fournisseurs d'accès – modèle développé par F. PATISSIER, consultant en études stratégiques pour la CISAC, pour la lutte contre le piratage de manière générale[551] – serait destinée à compenser certaines pertes dues aux échanges d'œuvres sur les réseaux *peer-to-peer*. Il ne s'agirait pas, comme dans les autres modèles envisagés *supra*, d'autoriser les échanges d'œuvres sur les réseaux *peer-to-peer*, mais simplement de faire participer financièrement les fournisseurs d'accès à la lutte contre cette forme de contrefaçon.

Une analogie peut être faite avec le secteur de l'audiovisuel dans lequel existe une obligation des chaines de télévision à investir dans la création audiovisuelle nationale et européenne. Le *ratio* d'une telle obligation est largement similaire, les acteurs retirant une valeur économique d'un contenu qu'ils transmettent ou hébergent. En conséquence, une contribution des FAI, de plateformes participatives ou d'autres acteurs d'internet dont on pourrait estimer qu'il retirent un bénéfice économique de contenus créatifs illicitement mis à disposition, pourrait être envisagée pour bénéficier à la création.

[550] *Apport de la Sabam au débat en faveur d'une juste rémunération pour la création sur internet*, SABAM, Mai 2010, disponible sur http://www.sabam.be/logbanner.php?link=website/data/SABAM_Position_Internet/Français.pdf.
[551] Se reporter à F. PATISSIER, « Réflexions sur de nouveaux modes de financement des industries culturelles », *World Copyright Summit*, CISAC, 9/10 juin 2009, Washington DC, disponible en ligne.

Section 3. La légitimité de tout traitement de données à caractère personnel effectué lors de la lutte contre le téléchargement

Quelle est l'incidence de tous les systèmes envisagés sur la **vie privée et la protection des données** personnelles des internautes ? Quelle est la légitimité de tout **traitement de données personnelles** effectué lors de la lutte contre le téléchargement ? L'identité du contrevenant présumé en matière de partage de fichiers est-elle communiquée au titulaire de droits, et si oui, comment ?

Quelles exceptions pourrait prévoir à cet égard la loi belge sur la protection des données personnelles ?

Les contraintes juridiques dans l'identification des individus qui téléchargent et partagent illégalement les contenus protégés constituent un obstacle significatif dans la lutte contre le piratage sur internet. Les ayants droit sont tentés de faire appel aux intermédiaires techniques pour que ceux-ci leur révèlent l'identité des abonnés qui contreviennent au droit d'auteur en partageant ou en téléchargeant des fichiers protégés. Outre la problématique de l'étendue de l'exonération de responsabilité des FAI que nous avons analysée *supra*, la question qui se pose est celle de savoir si les ayants droit, les FAI eux-mêmes ou une instance administrative, après avoir récolté les adresses IP des abonnés à internet peu scrupuleux, peuvent exiger des fournisseurs d'accès ou de tout autre intermédiaire, la communication de telles données à caractère personnel. Pour répondre à ces questions, il faut d'abord déterminer si une adresse IP est considérée comme une donnée à caractère personnel, et dans quelle mesure il y a traitement de données par les ayants droit dans la récolte de ces adresses IP.

La protection des données repose, entre autres droits fondamentaux, sur le droit fondamental à la vie privée, ainsi qu'il résulte en particulier de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la «CEDH»), qui a été signée à Rome le 4 novembre 1950. L'article 7 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), qui a été proclamée à Nice le 7 décembre 2000, a confirmé ce droit fondamental. Son article 8 a mis un accent particulier sur le droit fondamental à la protection des données à caractère personnel, en rappelant des principes fondamentaux importants de la protection des données. Selon l'avocat général de la CJUE, la communication des données à caractère personnel à un tiers porte atteinte au droit au respect de la vie privée des intéressés et constitue donc une ingérence au sens de l'article 8 de la Convention européenne des droits de l'homme[552].

[552] Conclusions de l'avocat général J. KOKOTT, 18 juillet 2007, aff. C-275/06, *Promusicae v. Telefonica de Espana SAU*, www.curia.eu, cons. 52.

§1. Les traitements de données à caractère personnel impliqués dans la lutte contre le téléchargement

Il s'agit de collecter les adresses IP dans le but d'identifier et de poursuivre les contrevenants, ainsi que de demander aux FAI la communication aux des données d'identification correspondant aux adresses IP collectées.

I. Question préliminaire : L'adresse IP est-elle une donnée à caractère personnel ?

Il est nécessaire de définir la nature de l'adresse IP, celle-ci étant l'information qui permet d'identifier les internautes commettant des actes contraires au droit d'auteur. Sont-elles des données à caractère personnel ? Si tel est le cas, se pose la question du respect de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui transpose en droit interne la directive 95/46/CE 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, dans le cadre de la collecte des adresses IP des internautes.

A. Aspects techniques

Une adresse IP, ou *Internet Protocol*, est une donnée d'identification qui est attribuée à chaque appareil connecté à internet – qu'il s'agisse d'un ordinateur, d'un téléphone, d'une tablette, *etc.* –, et qui se présente sous la forme d'une suite de quatre nombres compris entre 0 et 255, séparés par des points[553]. Pour qu'il puisse y avoir communication entre un client et un serveur, il faut que le serveur, pour répondre à la requête du client, connaisse l'adresse de celui-ci, et c'est là qu'intervient l'adresse IP, qui identifie alors de manière unique un abonné internet derrière une requête. A un moment donné dans le temps, une seule adresse IP correspond à un seul abonné internet – mais peut-être à plusieurs ordinateurs connectés à un même réseau local. Ce sont les fournisseurs d'accès à Internet qui sont chargés de l'attribution des adresses IP à leurs abonnés, et c'est donc vers eux qu'il faut se tourner pour obtenir le nom de la personne à laquelle cette adresse est assignée, les fournisseurs devant stocker l'adresse et le nom de la personne à qui est allouée telle adresse IP, à tel moment.

Concernant l'obtention des adresses IP sur les réseaux, plusieurs moyens sont mis à la disposition des personnes intéressées : lorsque plusieurs personnes sont connectées en même temps sur un même réseau – via un logiciel *peer-to-peer* par exemple – un logiciel d'analyse de trafic ou une simple commande Dos suffisent pour révéler les adresses IP[554]. Nous pouvons déjà préciser à ce stade que malgré la facilité de la collecte de ces adresses IP, il faut obligatoirement passer par le fournisseur d'accès à internet pour connaître l'identité de l'internaute – ou plutôt de l'abonné – qui

[553] Wikipédia, "Adresse IP", http://fr.wikipedia.org/wiki/Adresse_IP
[554] G. RUE et F. DE PATOUL, *op. cit.*, p. 18.

se cache derrière cette adresse, cette données brute, en tant que telle, ne fournissant pas une telle information.

B. Aspects juridiques

Selon l'article 1er, §1er de la loi vie privée, une donnée à caractère personnel est « toute information concernant une personne physique identifiée ou identifiable (…) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

Une adresse IP est donc un identifiant unique, souvent modifiée à chaque nouvelle connexion, d'un abonné internet, et les informations qui y sont contenues concernent une personne physique identifiable, c'est-à-dire qui peut être *identifiée, directement ou indirectement,* au regard de la loi vie privée. La simple connaissance d'une adresse IP, aussi aisée soit-elle à obtenir, ne permet pas d'établir à qui elle se rapporte pour un moment donné, il faut pour cela qu'elle soit couplée à la base de données des FAI qui permet alors une identification précise de l'abonné[555]. Les moyens d'identification existent donc. Dans ce cadre, « une information relative à une personne est considérée comme donnée à caractère personnel tant que quelqu'un est en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme 'données à caractère personnel' les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clés nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne »[556]. Dès lors qu'il existe un moyen raisonnable d'identifier les internautes, les données collectées tombent sous le champ d'application de la loi alors même que cette possibilité technique n'existerait qu'*in abstracto* dans le chef d'un tiers – le fournisseur d'accès –, le fait d'obtenir l'identité précise des internautes grâce à leurs bases de données automatisées étant de l'ordre du moyen raisonnable[557]. Mais en matière de communication électronique, il pourrait être considéré que le fait qu'un fournisseur d'accès à internet ne soit pas autorisé, en vertu de l'article 124 de la loi du 13 juin 2005, à divulguer les informations se trouvant derrière une adresse IP soit un moyen déraisonnable et ôte dès lors la qualité de donnée à caractère personnel de ce type de données. Or l'article 125 tempère cette interdiction en prévoyant une série d'exceptions qui permettent la divulgation des informations, une de ces exceptions étant qu'une loi autorise cette transmission. En Belgique, l'article 86*ter* de la LDA est une telle disposition, ce qui implique que le moyen d'identification reste raisonnable.

Certains auteurs de doctrine, principalement en France, ont par contre considéré que les adresses IP n'étaient pas des données personnelles, « puisque ces adresses ne permettent pas, par elles-mêmes, d'identifier leurs bénéficiaires », et que « ces adresses ont un caractère seulement indirectement

[555] G. Rue et F. De Patoul, *op. cit.*, pp. 17-18.

[556] Exposé des motifs de la loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, 1566/1, 97/98, p. 12.

[557] G. Rue et F. De Patoul, *op. cit.*, p. 20.

nominatif »[558]. Une certaine jurisprudence française a également mis à mal la reconnaissance de l'adresse IP comme donnée à caractère personnel, mais la C.N.I.L. a désapprouvé cette conception en estimant qu'une telle analyse « remet profondément en cause la notion de donnée à caractère personnel qui est très large. En effet, (la loi) vise toute information relative à une personne physique qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à des éléments qui lui sont propres. Ce qui est le cas d'un numéro de plaque d'immatriculation de véhicule, d'un numéro de téléphone ou d'une adresse IP »[559]. D'autres s'interrogent : serait-ce désormais « la fonction qui déterminerait la nature juridique de l'adresse IP » si l'on considère que l'adresse IP n'est une donnée à caractère personnel qu'entre les mains de la personne qui a les moyens de lever son anonymat[560] ? Nous pouvons légitimement constater que dès lors que des moyens existent pour « décoder » une donnée anonyme, même s'il y a disjonction entre la personne qui collecte et celle qui décode, cela ne change pas l'analyse relative à la qualification de donnée à caractère personnel, « une liste d'adresses IP ne constituerait donc pas des données anonymes non couvertes par la loi »[561].

Le groupe de travail de l'article 29 (ci-après « Groupe 29 ») sur la protection des données a également considéré les adresses IP comme étant des données à caractère personnel, protégées par la directive 95/46, car plusieurs acteurs disposent de moyens raisonnables pour associer ces adresses à l'identité de l'abonné. Le groupe 29 relève que « l'attendu 26 de la directive 95/46 précise que des données sont qualifiées de données à caractère personnel dès lors que le contrôleur ou toute personne utilisant des moyens raisonnables peut établir un lien avec l'identité de la personne objet des données (dans ce cas, l'utilisateur de l'adresse IP). Dans le cas d'adresses IP, le fournisseur de services Internet peut toujours faire le lien entre l'identité des abonnés et les adresses IP, et d'autres entités sont peut-être également en mesure de le faire par exemple en utilisant les registres des adresses IP attribuées ou d'autres moyens techniques existants »[562].

La Cour de justice quant à elle ne s'est pas prononcée sur la question de l'adresse IP en tant que donnée à caractère personnel dans son arrêt *Promusicae*, un tel moyen n'ayant pas été soulevé. L'analyse a plutôt porté sur la légalité de la communication de l'identité des internautes présumés coupables de contrefaçon, dont on ne conteste pas que de telles informations sont des données à caractère personnel, à un tiers, personne privée, lors d'une procédure civile[563]. Selon la Cour de justice, le fait de mettre à disposition les noms et adresses de certains utilisateurs de réseaux de *peer-to-peer* par un fournisseur d'accès à une organisation de défense des intérêts des auteurs tombe bien dans le champ d'application des directives 95/46/CE et 2002/58/CE[564].

---

[558] F. POLLAUD-DULIAN, "Du conflit entre l'accès à l'information nécessaire à l'action en contrefaçon et le droit au respect de la vie privée", *A&M*, 2008/4, p. 264.

[559] C.N.I.L., « L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes », 2 aout 2007, disponible sur http://www.cnil.fr/la-cnil/actualite/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/

[560] S. ROUJA, "La collecte des adresses IP par les agents assermentés, ou la fronde des tribunaux du 1er degré », *Juriscom.net*, 25 septembre 2007, disponible sur http://www.juriscom.net/actu/visu.php?ID=967.

[561] G. RUE et F. DE PATOUL, *op. cit.*, p. 19.

[562] Groupe de travail «article 29» sur la protection des données, Avis 4/2007 sur le concept de données à caractère personnel », 20 juin 2007.

[563] Arrêt *Promusicae*, § 45.

[564] *Idem.*

Dans son arrêt *Scarlet*, la Cour va suivre son avocat général sur le point de savoir si une adresse IP est bien une donnée à caractère personnel. Elle va estimer qu' « il est constant, d'une part, que l'injonction de mettre en place le système de filtrage litigieux 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* »[565]. Avant elle, son avocat général avait conclu qu' « une adresse IP peut être qualifiée de donnée à caractère personnel dans la mesure où elle peut permettre l'identification d'une personne, par référence à un numéro d'identification ou à tout autre élément qui lui soit propre »[566]. Dans l'affaire *Bonnier*[567], une précision a été apportée par l'avocat général dans ses conclusions : « Il convient de commencer par la question de savoir si les données demandées sont des données à caractère personnel. (…) Il s'agit des nom et adresse d'un abonné, qui sont à identifier sur la base d'une adresse IP. Il s'ensuit que nous nous trouvons dans le champ d'application des règles relatives à la protection des données à caractère personnel. Il convient néanmoins de rappeler que l'identité de la personne susceptible d'avoir commis une atteinte à des droits de propriété intellectuelle ne peut être établie sur la seule base de l'adresse IP lorsque plusieurs personnes peuvent utiliser l'accès au réseau identifié par cette même adresse IP. »[568] Cette précision est essentielle lorsqu'il s'agit de condamner une personne sur base de la collecte de son adresse IP, dans un mécanisme de réponse graduée par exemple.

Nous pouvons en conclure, sur base de cette analyse, que l'adresse IP doit être considérée comme une donnée à caractère personnel et est, dans ce cadre, soumise aux exigences de la loi vie privée.

II. Les différents traitements et leur légitimité

A. Notions générales

1. Traitement et responsable de traitement

Une fois l'adresse IP définie comme étant une donnée à caractère personnel, il faut se poser la question du traitement de cette donnée. Un traitement de données est défini dans la loi vie privée comme étant « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel »[569]. Cette notion a été définie largement, ce qui permet d'y faire entrer le traitement des données privées des internautes dans son champ d'application, car il y a au minimum collecte et conservation de ces données, en l'occurrence des adresses IP. Le traitement de données est réalisé par le responsable de traitement, qui est défini dans la loi vie privée comme étant « la personne physique ou morale, l'association de fait ou

[565] Arrêt *Scarlet*, § 51 (nous soulignons).
[566] Arrêt *Bonnier*, conclusions de l'Avocat général, § 78.
[567] C.J.U.E. (3e ch.), 19 avril 2012, *Bonnier Audio*, C-461/10, non encore publié au recueil.
[568] Arrêt *Bonnier*, conclusions de l'Avocat général, §§ 42 et 43.
[569] Article 1er, § 2 de la L.V.P.

l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »[570]. En raison également de la définition large de la notion, l'on peut aisément considérer les ayants droit, ou autres institutions qui se chargent d'enquêter sur les réseaux, les FAI ou une instance administrative, comme des responsables du traitement dans la mesure où les deux critères – à savoir la détermination des finalités et la détermination des moyens pour y parvenir – se retrouvent remplis dans leur chef. L'exigence de détermination des finalités et des moyens du traitement de données est remplie par la personne qui collecte, conserve et organise les données, ce qui sera le cas à chaque fois que l'une des personnes visées collectera des adresses IP d'internautes qui partagent illégalement des fichiers protégés par le droit d'auteur. Il peut arriver que ce soit un sous-traitant qui soit en charge de la collecte, l'organisation et la conservation des données à caractère personnel, le responsable de traitement restant la personne qui fixe les finalités du traitement.

2. *Principes de finalité et de transparence*

Un élément essentiel de la loi vie privée est le principe de finalité, le caractère explicite de celui-ci découlant du principe de transparence. Le premier est composé de deux principes que sont la légitimité et la conformité. Selon le principe de légitimité, « les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables »[571] ; le principe de conformité[572] consiste quant à lui en l'existence d'un lien suffisant entre les données et la finalité poursuivie, qui implique que les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement »[573]. La loi impose en outre une transparence des traitements et « interdit que la personne ne soit laissée dans la méconnaissance de l'utilisation des données la concernant »[574].

Lorsqu'il y a traitement des données à caractère personnel – en l'occurrence des adresses IP et des données de connexion – il faut que le responsable de ce traitement respecte le principe de transparence tel qu'il ressort de l'article 9 de la loi vie privée, et de l'article 10 de la directive 95/46. Selon ces dispositions, le responsable de traitement, lorsqu'il collecte des données auprès d'autres personnes que la personne concernée, doit « dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données »[575] informer celle-ci en lui fournissant les coordonnées du responsable de traitement, les finalités du traitement, le ou les destinataire des données, l'existence du droit d'opposition, d'accès et de rectification, etc. Et c'est là que le bât blesse. En effet, les ayants droit constituent des fichiers sur les internautes à leur insu, qui devraient normalement être avertis en

[570] Article 3 de la L.V.P. (nous soulignons).
[571] Article 4, §1er, 2° de la L.V.P.
[572] F. RIGAUX, *La vie privée, une liberté parmi les autres?*, Bruxelles, Larcier, 1992, p. 257
[573] Article 4, §1er, 3° de la L.V.P.
[574] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46 du 24 octobre 1995", *J.T.*, 1999, p. 20.
[575] Article 9, §2 de la L.V.P.

vertu du principe de transparence. Mais pour pouvoir les avertir, il faut les identifier et pour cela demander ces informations aux fournisseurs d'accès, qui n'ont pas le droit de leur fournir sous peine de violer le droit en la matière[576]. Mais le devoir d'information ne doit pas nécessairement être fait à titre individuel, l'obligation étant déjà remplie par le signalement sur un site internet que les données de navigation sont susceptibles d'être traitées. On ne doit pas non plus identifier nécessairement les individus pour pouvoir les informer, si un numéro de GSM a été fourni par exemple lors de l'inscription sur un site, on pourrait imaginer simplement l'envoi d'un SMS à cette personne et il n'est dès lors pas indispensable de connaître son nom. Dans la situation de la lutte contre le piratage en ligne, ces cas ne seront pas légion, mais sont malgré tout envisageables.

Par ailleurs, selon une recommandation du groupe 29, « la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée et à la liberté d'expression dans le cyberespace »[577]. L' avis 1/2008 du groupe 29 estime en outre que « la surveillance secrète du comportement des utilisateurs, un comportement assurément privé, tel que la visite de sites internet, va à l'encontre des principes de traitement loyal et légitime inscrits dans la Directive 95/46/CE »[578]. La Cour européenne des droits de l'Homme a considéré quant à elle que « la collecte et la conservation, à l'insu de la requérante, de données à caractère personnel se rapportant à l'usage qu'elle faisait du téléphone, du courrier électronique et de l'Internet ont constitué une ingérence dans l'exercice du droit de l'intéressé au respect de sa vie privée et de sa correspondance, au sens de l'article 8 »[579].

Concernant plus particulièrement le filtrage de toutes les communications électroniques, tant entrantes que sortantes, il ne peut constituer une surveillance secrète des internautes, qui doivent être informés des traitements les concernant, en vertu des dispositions précitées[580].

3. Intervention de la loi sur les communications électroniques

De plus, le traitement lui-même pourrait être illégal, dès lors qu'il pourrait être considéré comme violant l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques. L'article 124 prévoit que sans autorisation de la personne concernée, il est interdit de « prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique (qui) ne lui est pas destinée personnellement ; identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ; (…) prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ; modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non. » Les données dont il est question ici sont bien des données de trafic, qui relèvent de la loi de 2005 relatives aux communications électroniques. Par « donnée de trafic », il faut entendre « toute données traitée en vue de l'acheminement d'une communication par un réseau de

[576] G. RUE et F. DE PATOUL, *op. cit.*, p. 24.
[577] Recommandation 3/97 WP 6 du Groupe 29 du 3 décembre 1997.
[578] Avis 1/2008 du Groupe 29 du 4 avril 2008 sur les aspects de la protection des données liées aux moteurs de recherche.
[579] C.E.D.H., *Copland c. Royaume-Uni*, 3 avril 2007.
[580] D. GOBERT et J. JOURET, *op. cit.*, p. 30.

communication électronique ou de la facturation de ce type de communication »[581]. La protection offerte par l'article 124 s'appuie sur le concept de tiers à la communication, qui n'a pas la qualité de destinataire de la communication[582] – l'ayant droit par exemple[583]. L'article 124, 1° de la loi du 13 juin 2005 vise la prise intentionnelle de connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique. Le deuxième alinéa de cet article vise l'identité des personnes qui sont concernées par la transmission de l'information et son contenu, et le troisième les données de communication électroniques, y compris les données de trafic. Il est admis que la protection offerte par l'article 124 est applicable après que la transmission soit achevée, et non seulement durant celle-ci[584].

Il peut être dérogé à cet article « lorsque la loi permet ou impose l'accomplissement des actes visés ; lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communication électronique (…) » selon l'article 125 de la loi du 13 juin 2005 qui transpose l'article 15, §1er de la directive 2002/58. Il s'agirait de la seule disposition qui présenterait un intérêt dans le cadre de la lutte contre le partage illégal de fichiers sur internet pour permettre un traitement des adresses IP ou des moyens de surveillance des communications[585]. Il faut se poser la question de la précision de la disposition visée pour constituer une base légale adéquate. Relevons encore que selon l'arrêt *Bonnier* de la Cour de justice, l'article 15, §1er de la directive peut s'appliquer dans le cadre de procédures civiles.

B. La collecte des adresses IP

La loi vie privée « s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »[586]. Le traitement d'adresses IP entre dans cette définition du champ d'application de la loi, sans que cela ne pose plus de questions.

Ce même article 3 contient toute une série d'exceptions, totales ou partielles, au champ d'application matériel et personnel de la loi. La première est celle pour les activités personnelles ou domestiques (§2)[587]. Cette exception ne concerne que les personnes physiques. La constitution de fichiers par les ayants droit, seuls ou par le biais d'une association ou d'une société de gestion collective, en vue d'éventuelles poursuites judiciaires ne rentre pas dans le cadre de telles activités. De plus, le concept de « finalité domestique » exclut l'activité commerciale ainsi que la volonté de lucre. Une autre exception qui aurait pu être pertinente est celle concernant les services de police

[581] Article 2, 5° de la loi du 13 juin 2005 relative aux communications électroniques.
[582] K. ROSIER et R. ROBERT, « Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu de travail », in *Le droit du travail à l'ère du numérique*, Limal, Anthemis, 2011, p. 252.
[583] Article 124, al. 1 de la loi du 13 juin 2005 relative aux communications électroniques.
[584] K. ROSIER et R. ROBERT, *op. cit.*, p. 261.
[585] V. FOSSOUL, « La protection de la vie privée, obstacle à la lutte contre le téléchargement illégal ? », in *Le téléchargement d'œuvres sur Internet*, Bruxelles, Larcier, 2012, p. 331.
[586] Article 3, § 1er de la L.V.P.
[587] « La présente loi ne s'applique pas au traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

(§5)[588], mais dans le cas qui nous intéresse, le Parquet interviendrait effectivement dans un cas de demande d'informations à un intermédiaire technique par exemple, mais pas au titre de responsable du traitement.

Un régime spécifique est prévu pour les données sensibles, données qui jouissent d'une protection particulière, dont font partie les données judiciaires, ce que sont dans les faits les données récoltées sur internet dans un but de lutte contre le piratage, qui sont « des données relatives à des suspicions ayant trait à des infractions »[589], et qui sont interdites de traitement sous réserve d'exceptions strictement réglementées par la loi[590]. Le contrôleur européen de la protection des données est arrivé à la même conclusion pour les données récoltées dans un système de réponse graduée, considérant que ces données doivent être qualifiées de données sensibles[591]. Le traitement de ces données est donc interdit, sauf exception strictement définie. Ainsi, selon le paragraphe 2, c) de l'article 8 de la loi vie privée, une personne physique ou morale peut traiter des données judiciaires aux seules fins de gestion de son propre contentieux. La Commission de la protection de la vie privée estime que le contentieux doit, à tout le moins, se situer dans une phase préparatoire à un litige devant une cour ou un tribunal[592], et elle en conclut que si ces conditions permettent à une maison de disques, à l'IFPI ou à la Sabam par exemple, de traiter des données relatives à une infraction précise qu'elles ont pu constater, dans la mesure où elles se situent dans une phase au moins préparatoire à un litige, elles ne permettent pas de rechercher systématiquement et de façon proactive des données à caractère personnel sur internet dans le but de déceler des infractions au droit d'auteur, cette démarche étant en dehors de toute phase préparatoire[593]. En vertu du point b) du même article, le traitement de ces données peut être effectué « par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ». Un traitement de données réalisé pour lutter contre le téléchargement illégal ne pourra avoir lieu sans une loi qui autoriserait un tel traitement.

Dans le fonctionnement de la réponse graduée, qu'elle soit intégrale ou atténuée, il y a en premier lieu, et c'est la base du mécanisme, une collecte des adresses IP des internautes. Cette collecte peut être réalisée par un agent assermenté – c'est le cas de l'HADOPI –, par un ayant droit, ou encore une autorité administrative. Concernant le principe de nécessité, il apparaît qu'un mécanisme proactif de surveillance généralisée et systématique des internautes, tel que celui de la réponse graduée dans

[588] « Les articles 9, 10, § 1er, et 12 ne s'appliquent pas :
1° aux traitements de données à caractère personnel gérés par des autorités publiques en vue de l'exercice de leurs missions de police judiciaire (…) ».
[589] Article 8 de la L.V.P.
[590] Article 8, §1er de la LVP : "Le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté est interdit".
[591] C.E.P.D., « Avis du contrôleur européen de la protection des données sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC) », 22 février 2010, 2010/C 147/01, n° 51.
[592] Malgré la disparition dans la loi de la condition qu'il doit s'agir de "litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives", la Commission a estimé que l'intention du législateur n'avait pas changé.
[593] CPVP, Avis n° 44/2001, pp. 3 et 4.

son étape initiale, est contraire à ce principe[594]. Quant au principe de proportionnalité, il requiert que la collecte et le traitement soient adéquats, pertinents et non excessifs. L'*European Data Protection Service* considère que le fait que la surveillance affecte tous les utilisateurs d'internet, qu'ils soient ou non soupçonnés de piratage, que l'effet de ce traitement puisse aller jusqu'à la suspension de la connexion et enfin que ce soit à une instance non judiciaire, tels que les ayants droit, les FAI ou une autorité administrative à procéder à la collecte est contraire à ces trois composantes du principe de proportionnalité[595].

A noter que certains contestent la fiabilité de l'adresse IP en tant que méthode d'identification. Selon la CNIL, « la fiabilité des dispositifs techniques destinés à garantir la sécurité des connexions n'est pas acquise »[596]. En effet, le risque existe qu'il y ait une usurpation d'adresse IP, rendue possible par une « technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès »[597]. Il est possible pour un ordinateur d'usurper l'adresse IP de n'importe quel autre appareil connecté à internet, ce qui en fait une technique incertaine de repérage des internautes. Ce risque sera également présent dans le cadre des systèmes d'avertissements, où c'est également via la collecte des adresses IP que pourra se faire le repérage des internautes. Cela découle de la conception même du protocole IP et du routage sur internet qui ne prévoient pas de vérification de l'adresse source, et cela de par leur caractère décentralisé[598]. La *Computer Emergency Response Team*, organisme chargé d'assurer des services de prévention des risques, déconseille d'utiliser une adresse IP comme méthode d'identification d'ordinateur sur internet[599]. Diverses études ont été menées pour démontrer qu'il était aisé de falsifier des adresses IP, en détournant l'adresse de son voisin, même protégée par une clé WEP, en enregistrant des adresses IP d'imprimantes ou de routeurs sur des serveurs de *peer-to-peer*, qui ont alors reçu des lettres d'avertissements pour téléchargement illégal alors qu'aucun fichier n'avait été téléchargé…[600] Comme dernière considération sur la faiblesse de l'adresse IP comme moyen de repérer les internautes soupçonnés de téléchargement illégal, nous pouvons relever qu'une adresse IP ne permet pas de connaître l'adresse de courrier électronique de l'internaute abonné, ou alors si une adresse est attachée à un compte elle peut très bien être obsolète ; or c'est justement via le mail qu'est adressé le premier avertissement d'HADOPI. Il y a donc un risque que les abonnés qui changent d'adresse mail ne reçoivent jamais le premier avertissement, sans jamais prendre connaissance de l'avertissement préalable.[601] En revanche, une

[594] European Data Protection Service, « EDPS comments on selected issues that arise from IMCO report on the réview of Directive 2002/22/EC (universal service) & Directive 2002/58/EC (ePrivacy) », p. 6.
[595] *Ibidem*, p. 7.
[596] M. REES, « La CNIL critique la loi HADOPI, son président la vote deux fois », *PCINpact*, 25 mai 2009, disponible sur http://www.pcinpact.com/news/51019-alex-turk-cnil-hadopi-vote.htm.
[597] http://fr.wikipedia.org/wiki/Usurpation_d%27adresse_IP
[598] http://www.cert.org/advisories/CA-1995-01.html
[599] http://www.cert.org/advisories/CA-1996-21.html
[600] « Challenges and directions for monitoring P2P file sharing networks-or: why my printer received a DMCA takedown notice », http://dl.acm.org/citation.cfm?id=1496683
[601] http://fr.wikipedia.org/wiki/Loi_Création_et_Internet

étude commandée par HADOPI a considéré que la méthode utilisée par la Haute autorité pour identifier une œuvre et l'adresse IP ayant mis à disposition cette œuvre est fiable[602].

C. Demande d'identification à partir des données récoltées

Une fois les adresses IP – données à caractère personnel – récoltées (si tant est qu'une loi l'autorise, ce qui n'est pas le cas actuellement dans la législation belge), ainsi que la date et l'heure de la connexion, il s'agit de faire correspondre ces données avec l'identité de la personne qui se cache derrière. De manière générale, une communication de données à caractère personnel à un tiers constitue une ingérence dans le droit au respect de la vie privée des personnes concernées au sens de l'article 8 de la Convention européenne des droits de l'homme, et doit par-là respecter les critères de légitimité établis par le paragraphe 2 de cet article et par la Cour européenne des droits de l'homme. De plus, une telle communication porte atteinte au secret des communications. Il s'agit donc de rechercher une base légale appropriée autorisant à communiquer des données relatives au trafic à des tiers souhaitant intenter une action judiciaire civile à l'encontre d'un internaute souçonné de partage illicite de fichiers[603]. Pour lever l'anonymat d'une adresse IP, il faut faire appel aux fournisseurs d'accès à internet, mais comment faire la balance entre des intérêts qui paraissent à ce point contradictoires ? On ne peut communiquer des données que si cela est compatible avec la finalité de la collecte initiale, si la loi dans laquelle cette compatibilité est prévue est suffisamment précise, prévisible[604].

La poursuite des utilisateurs s'étant heurtée à l'obstacle de l'identification des internautes se livrant à ces échanges, cela a réduit ces poursuites dans de nombreux pays. En Belgique par exemple, aucune action n'a été intentée contre les internautes de manière systématique car la Commission de la protection de la vie privée a estimé qu'un fournisseur d'accès à internet ne pouvait délivrer à des tiers des données à caractère personnel concernant ses abonnés dans l'objectif de déceler des infractions au droit d'auteur, sauf dans le cadre d'une procédure judiciaire[605].

Quelques années plus tard, le 29 janvier 2008, la Cour de justice a eu à connaître d'une question préjudicielle sur le sujet[606]. Il s'agissait pour la CJCE de déterminer à quelles conditions le droit à la vie privée pouvait faire obstacle à la poursuite des infractions au droit d'auteur, en précisant l'étendue des dérogations prévues par la législation communautaire à l'obligation de confidentialité des communications[607]. La question qui lui était posée était celle de savoir si les directives n° 2000/31, 2001/29 et 2004/48 « lues aussi à la lumière des articles 17 ainsi que 47 de la charte, doivent être interprétées en ce sens qu'(elles) imposent aux États membres de prévoir, en vue d'assurer la protection effective du droit d'auteur, l'obligation de communiquer des données à caractère

[602] Rapport Znaty, 16 janvier 2012, disponible sur http://www.hadopi.fr/actualites/rapports/publication-du-rapport-dexpertise-de-david-znaty

[603] F. COUDERT et E. WERKERS, « La protection des droits d'auteurs face au réseau *peer-to-peer* : la levée du secret des communications est-elle justifiée ? », *R.D.T.I.*, n° 30/2008, p. 77.

[604] Il faut également tenir compte de la loi du 13 juin 2005 relative aux communications électroniques.

[605] Avis de la Commission de la protection de la vie privée n° 44/2001 du 12 novembre 2001, *Revue Ubiquité, Droit des technologies de l'information*, Larcier, n° 12, juin 2002, p. 103 et s.

[606] C.J.C.E., 29 janvier 2008, *Promusicae c. Telefonica de Espana*, C-275/06.

[607] F. COUDERT et E. WERKERS, *op. cit.*, p. 77.

personnel dans le cadre d'une procédure civile », et donc de savoir s'il faut limiter aux seules procédures pénales la possibilité d'obtenir les informations indispensables. Il s'agissait ici de la volonté de l'association de producteurs et éditeurs espagnole Promusicae d'obtenir communication des noms et adresses de certains utilisateurs de KaZaA par le fournisseur d'accès Telefonica.

La Cour de justice va estimer que cette communication d'informations « constitue un traitement de données à caractère personnel, au sens de l'article 2, premier alinéa, de la directive 2002/58, lu en combinaison avec l'article 2, sous b), de la directive 95/46. Il doit donc être admis que ladite communication relève du champ d'application de la directive 2002/58 (…) »[608]. C'est donc la directive 2002/58/CE du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électronique qui s'applique. Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance. Selon le considérant 26 de ladite directive, ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Or, la récolte d'adresses IP constitue bien une interception de communication[609], car elle est réalisée avec une finalité autre que l'acheminement de la communication et sa facturation, ce qui implique le respect des exigences de prévisibilité et de proportionnalité. La directive prévoit en son article 5 l'interdiction « à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, §1 ». L'article 15 vise les cas où une limitation est nécessaire, appropriée et proportionnée pour sauvegarder certains intérêts qu'il énumère, et donc permettre des exceptions au principe de la garantie de la confidentialité des données pour certains cas spécifiques. Ces cas spécifiques sont « sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État —, la défense et la sécurité publique, ou 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, §1 de la directive 95/46/CE ». Cet article renvoie à l'article 13 de la directive 95/46/CE qui contient d'autres motifs de dérogations, comme par exemple, et c'est celui-ci qui nous intéresse dans le cadre de cette étude, la protection des droits et libertés d'autrui. Cela implique que des exceptions à la confidentialité des données peuvent être envisagées pour sauvegarder les droits d'autrui (comme le droit d'auteur). Ainsi, « 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 ».

C'est dans ce cadre que la Cour de justice a estimé que « les directives 2000/31, 2001/29, 2004/48 et 2002/58 n'imposent pas aux États membres de prévoir (…) l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile »[610]. En effet, « l'obligation de protéger les titulaires de droits d'auteur qui incombe à l'État n'est pas telle qu'elle lui imposerait de mettre à leur disposition des moyens illimités lui

[608] Arrêt *Promusicae*, § 45.
[609] « La prise de connaissance par un tiers du contenu et/ou des données afférentes aux télécommunications privées entre deux ou plusieurs correspondants » voir position du Groupe 29.
[610] Se reporter aux commentaires de Ch. CARON, *CCE* mars 2008, comm. n° 32.

permettant d'élucider les violations de ceux-ci. Au contraire, rien ne s'oppose à ce que certains droits d'investigation soient réservés aux autorités publiques ou ne soient tout simplement pas disponibles. »[611] En revanche, si le législateur admet une dérogation à la protection des données personnelles pour faciliter la poursuite de violations de droit d'auteur par les ayants droit – une telle possibilité n'étant pas interdite par le juge européen – la Cour exige de rechercher un juste équilibre entre les différents droits fondamentaux tant par les législateurs au moment de la transposition des directives que par les juges lors des litiges[612]. L'ordonnance de la Cour dans l'affaire *LSG*, portant sur les mêmes questions, confirme ce que la Cour a énoncé dans l'arrêt *Promusicae* sur ce point.

Dans l'affaire *Bonnier*, la Cour précise ce qu'elle a précédemment édicté dans les affaires *Promusicae* et *LSG*. Elle relève que lorsqu'un Etat prévoit dans sa législation une obligation de transmission de données à caractère personnel, dans le cadre d'une procédure civile, à des personnes privées, il doit respecter des critères[613]. Ainsi, il est tout à fait possible de modifier une législation existante en ce sens à condition de respecter les principes énoncés par la Cour dans l'arrêt *Bonnier*. Il est néanmoins permis, grâce à l'article 86*ter* de demander à un juge que soient fournies les données d'identification sur la base des données récoltées.

Nous pouvons enfin relever que lorsqu'il s'agit d'une action prenant la forme d'un blocage de site par un fournisseur d'accès, un hébergeur ou DNS.be, il n'y a pas de traitement de données à caractère personnel, les mesures se limitant au blocage d'un site internet. Il en irait bien évidemment autrement si les ayants droit, outre le blocage, demandent la communication des adresses IP ayant voulu s'y connecter.[614]

D. La conservation des données

Un troisième traitement intervenant dans la poursuite des internautes soupçonnés de partager ou télécharger illégalement des œuvres protégées par le droit d'auteur. L'article 6 de la directive 2002/58 prévoit que lorsque les données de trafic ne sont plus nécessaires à la transmission d'une communication, leur effacement ou leur anonymisation est obligatoire, à moins qu'une loi qui prévoirait une telle conservation ne soit adoptée[615]. Les ayants droit risquent de se retrouver dans l'impossibilité d'exercer leur droit à obtenir des informations en raison de l'effacement ou de l'anonymisation des données[616]. L'article 1er de la directive 2006/24 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications prévoit la conservation des données « à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne ». L'avocat général dans l'affaire *Bonnier* a considéré que « Pour qu'une divulgation des données à caractère personnel soit possible, le droit de

[611] Arrêt *Promusicae*, § 121.
[612] L'arrêt de la CJCE du 19 févr. 2009 (ord., *LSG-Gesellschaft zur Wahrrnehmung von Leistungsschutzrechten GmbH c/ Tele 2 Telecommunication GmbH,* aff. C.557-07,) s'inscrit dans la même tendance : voir L. COSTES, *CCE* avr. 2009, comm. 1567, p. 22.
[613] Voir *supra*.
[614] V. FOSSOUL, *op. cit.*, pp. 325 et 326.
[615] Article 15, §1 de la directive 2002/58.
[616] V. FOSSOUL, *op. cit.*, p. 340.

l'Union exige qu'une obligation de conservation soit prévue par la législation nationale, afin de préciser les catégories de données à conserver, la finalité de conservation, la durée de la conservation et les personnes qui peuvent y avoir accès. Il serait contraire aux principes de la protection des données à caractère personnel de faire usage des bases de données qui existent à d'autres fins que celles ainsi définies par le législateur »[617].

En France, le 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[618] précise les informations d'identification de leurs clients qui doivent être conservées par les fournisseurs d'accès et d'hébergement en vertu de l'article 6, II et II*bis* de la LCEN, en proposant des définitions des données d'identification, par acteur et par situation[619]. La conservation des données d'identification est le corollaire du régime de responsabilité limitée dont bénéficient les intermédiaires quant aux contenus mis en ligne[620].

En outre, dans un système de réponse graduée, il est nécessaire de conserver les données d'identification de l'internaute pour vérifier les récidives éventuelles qui déclenchent l'étape ultérieure des sanctions. Cette conservation des données pour une telle finalité devra faire l'objet d'une autorisation légale.

E. Conséquences de la preuve recueillie sur base d'un traitement illicite

Il apparaît que des données récoltées dans le cadre de traitements illégitimes, en infraction à la loi sur la vie privée, ne sont pas légales et entraineraient *de facto* la nullité des poursuites. Toutefois, la jurisprudence de la cour de cassation apporte une certaine souplesse dans l'appréciation des preuves recueillies dans ce contexte.

Comme le signale D. MOUGENOT, « l'administration de la preuve est de plus en plus encadrée par des lois ou principes qui en délimitent le champ »[621]. Parmi ces lois et principes, on retrouve celui du respect de la vie privée, les règles relatives au secret des correspondances, la loi du 8 décembre 1992 concernant la protection des données, la loi du 13 juin 2005 relative aux communications électroniques. On le voit, le risque de recueillir une preuve en infraction d'une de ces lois est bien présent, ce qui en fera une preuve illicite. Une preuve, en plus d'être illicite, peut avoir été récoltée de manière déloyale, ce qui est le cas d'une preuve recueillie à l'insu de la personne observée[622]. Cela est clairement le cas lorsque l'on procède à la collecte d'adresses IP d'internautes sur Internet, et cela sans respecter les règles de traitement de ces données à caractère personnel (non-respect du principe de transparence par exemple).

---

[617] Conclusions de l'avocat général N. JÄÄSKINEN dans l'affaire *Bonnier*, 17 novembre 2011, § 60.

[618] Décret n° 2011-219, 25 févr. 2011 : *JO* 1er mars 2011, p. 3643. Pour une analyse détaillée du décret, voir I. CANTERO et P. AGOSTI, « Une Arlésienne enfin visible. 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 », *C.C.E.*, janvier 2012, pp. 13 et s.

[619] I. CANTERO et P. AGOSTI, *op. cit.*, pp. 13 et 16.

[620] *Ibidem*, p. 13.

[621] D. MOUGENOT, « Antigone face aux juges civils. L'appréciation des preuves recueillies de manière illicite ou déloyale dans les procédures civiles », *DAOR*, n° 2011/98, pp. 240 et 241.

[622] *Ibidem*, p. 241.

En matière pénale, depuis l'arrêt *Antigoon*, et la jurisprudence dite Antigone qui a suivi, les preuves recueillies de manière illégale, ainsi que tous les éléments qui se fondent sur celles-ci, ne sont plus écartées automatiquement des débats. L'arrêt de la Cour de cassation est clair à ce sujet : « la circonstance qu'un élément de preuve a été obtenu irrégulièrement a, en règle, uniquement pour conséquence que le juge, lorsqu'il forme sa conviction, ne peut prendre cet élément en considération ni directement, ni indirectement :

a. soit lorsque le respect de certaines conditions de forme est prescrit à peine de nullité ;
b. soit lorsque l'irrégularité commise a entaché la fiabilité de la preuve
c. soit lorsque l'usage de la preuve est contraire au droit à un procès équitable ».

La Cour a par la suite ajouté de nouveaux critères d'appréciation : « Lorsque l'irrégularité commise ne compromet pas le droit à un procès équitable, n'entache pas la fiabilité de la preuve et ne méconnait pas une formalité prescrite à peine de nullité, le juge peut, pour décider qu'il y a lieu d'admettre des éléments irrégulièrement produits, prendre en considération, notamment, la circonstance que *l'illicéité commise est sans commune mesure avec la gravité de l'infraction dont l'acte a permis la constatation* (c'est nous qui soulignons), ou que *cette irrégularité est sans incidence sur le droit ou la liberté protégés par la norme transgressée* (c'est nous qui soulignons) ». La question qui se pose est celle de la transposition de cette jurisprudence à la matière civile.

Un certain nombre de décisions ont plutôt été dans le sens d'une mise en balance des intérêts en présence, considérant que le droit à la vie privée n'était pas un droit absolu et que son invocation ne peut justifier un rejet systématique des preuves qui pourraient y porter atteinte. Un arrêt de la Cour de cassation du 10 mars 2008 a d'ailleurs été dans le sens de la jurisprudence Antigone : « sauf si la loi prévoit expressément le contraire, le juge peut examiner l'admissibilité d'une preuve illicitement recueillie (…) en tenant compte de tous les éléments de la cause, y compris de la manière suivant laquelle la preuve a été recueillie et des circonstances des lesquelles l'irrégularité a été commise ». Dans trois cas, la preuve sera rejetée par le juge : en cas de violation d'une formalité prescrite à peine de nullité, de présentation d'une preuve dont l'obtention est entachée d'un vice qui est préjudiciable à sa crédibilité, et donc non fiable, et si la preuve porte atteinte au droit à un procès équitable. De plus, le juge devra procéder à la mise en balance de la gravité du manquement et celle de l'irrégularité de la preuve[623], ce qui est en définitive l'élément central du pouvoir d'appréciation du juge en matière civile[624].

Comme le souligne D. MOUGENOT, « il est certains manquements qui ne peuvent être constatés que par surprise ou par ruse », qui lui-même cite R. PERROT qui exprime que « la concurrence déloyale ne se fait jamais au grand jour et la preuve devient impossible si l'on ne permet pas à celui qui s'en estime victime d'en percer certaines zones d'ombre qui, à la faveur des technologies modernes, empruntent des voies souterraines ». Ces réflexions nous font automatiquement penser à la recherche des internautes qui téléchargent et partagent des fichiers protégés par le droit d'auteur

[623] « Le juge qui procède à (l') appréciation peut notamment tenir compte d'une ou de plusieurs des circonstances suivantes : le caractère purement formel de l'irrégularité, sa conséquence sur le droit ou la liberté protégés par la règle violée, la circonstance que l'autorité compétente pour la recherche, l'instruction et la poursuite des infractions a commis l'irrégularité intentionnellement, la circonstance que la gravité de l'infraction excède manifestement celle de l'irrégularité, le fait que la preuve illicitement recueillie porte uniquement sur un élément matériel de l'infraction, le fait que l'irrégularité qui a précédé ou contribué à établir l'infraction est hors de proportion avec la gravité de l'infraction ».

[624] D. MOUGENOT, "Antigone face aux juges civils (…)", *op. cit.*, p. 253.

sur le réseau internet, et il peut être remarqué que certaines juridictions sont conscientes que dans certains cas, une preuve ne pourrait pas être administrée autrement qu'en infraction de la loi vie privée par exemple.

Quoi qu'il en soit de cette application de la jurisprudence Antigone en matière civile, il reste toujours la théorie de l'abus de droit par laquelle nous pourrions considérer que l'invocation du droit à la vie privée ne peut couvrir la commission d'une infraction, ou encore l'application de l'adage *fraus omnia corrumpit* par lequel la personne qui commet un manquement perd son droit à invoquer la protection de certains droits fondamentaux[625].

§2. La proportionnalité : un principe directeur pour toute modification législative

En l'état actuel des textes, il nous parait impossible d'effectuer les différents traitements nécessaires à la poursuite des internautes soupçonnés de porter atteinte au droit d'auteur sur internet. Une modification législative s'avèrerait nécessaire pour légitimer ces traitements, modifications qui seront fonction de l'option choisie.

Il est essentiel de toujours garder à l'esprit la problématique générale qui est de savoir dans quelle mesure des organismes privés peuvent chercher à faire respecter les droits d'auteur dont ils ont la gestion. Il faut assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire et qui n'entre pas en conflit avec les dits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité.

A ce titre, la Cour de justice, dans ses différents arrêts rendus en la matière, se penche sur les mécanismes permettant de concilier les exigences liées à la protection des droits fondamentaux en présence. En effet, il est de jurisprudence constante que les droits fondamentaux font partie intégrante des principes généraux du droit communautaire dont la Cour de justice assure le respect. Une limitation aux droits fondamentaux des personnes doit respecter trois conditions, dont le principe de proportionnalité. Dans son arrêt *Promusicae*, la Cour avait déjà exprimé que la protection du droit fondamental de propriété, dont font partie les droits liés à la propriété intellectuelle, doit être mise en balance avec celle d'autres droits fondamentaux[626], qu'il faut assurer un juste équilibre entre la protection de ce droit et celle des droits fondamentaux des personnes qui sont affectées par les mesures, tels que le droit de liberté d'entreprise[627] – des fournisseurs d'accès dans la plupart des cas – et le droit à la protection des données et la liberté de recevoir ou de communiquer des informations[628] – pour les clients de ces fournisseurs d'accès. Ainsi la Convention n° 108 du Conseil de l'Europe prévoit qu'une mesure d'ingérence par rapport à la protection des données n'est tolérée que lorsqu'elle constitue une mesure nécessaire dans une société démocratique à la protection des intérêts nationaux énumérés en son article 9, § 2, et lorsqu'elle est strictement définie au regard de cette finalité. L'arrêt *Lindqvist* de la Cour de justice a par ailleurs rappelé qu'en application du

[625] D. MOUGENOT, *op. cit.*, p. 254. Et plus spécialement F. HENDRICKX (n°3) et K. WAGNER (n°46).
[626] Arrêt *Promusicae*, §§ 62 à 68.
[627] Arrêt *Scarlet*, § 49.
[628] *Ibidem*, § 50.

principe de proportionnalité, il incombe à la juridiction de renvoi de prendre en considération toutes les circonstances de l'affaire dont elle est saisie, notamment la durée de la violation des règles mettant en œuvre la directive 95/46 ainsi que l'importance, pour les intéressés, de la protection des données divulguées[629].

Comme le relèvent F. COUDERT et E. WERKERS, « l'interprétation de la C.J.C.E. entraîne un élargissement considérable du champ des dérogations admises à la confidentialité des communications, amoindrissant de ce fait la protection accordée à ce droit au profit d'autres intérêts légitimes concurrents »[630]. De plus, en laissant le choix aux Etats membres, il y a un risque que cela conduise à des divergences entre l'interprétation qui sera faite par ceux-ci du principe de proportionnalité et dès lors poser problème en terme d'harmonisation du marché intérieur.

L'avocat général avait relevé dans ses conclusions dans l'affaire *Bonnier* que la protection des droits d'auteur est un intérêt social important, qui constitue un intérêt fondamental de la société, et que le partage illégal de fichiers compromet effectivement la protection des droits d'auteur, mais qu' « il n'est (…) pas certain que le partage de fichiers entre personnes privées, en particulier lorsque celles-ci agissent sans but lucratif, compromette la protection des droits d'auteur d'une manière à ce point grave qu'elle justifierait l'application de [l'exception pour sauvegarde de la sécurité publique] »[631], et c'est au législateur d'apprécier si tel est le cas. C'est ce motif qui est le plus à même de fonder une exception dans le cas de l'affaire *Promusicae*, car la protection des droits d'auteur est un intérêt social dont la Communauté a reconnu l'importance et qui peut être reconnu comme intérêt fondamental de la société. L'avocat général met toutefois en doute la nécessité et la proportionnalité d'une mesure visant à communiquer les données de trafic des utilisateurs par les FAI à des personnes privées. Il avait suggéré, mais n'a pas été suivi sur ce point par la Cour de justice, la mise en place d'une solution plus modérée qui prévoirait que les données à caractère personnel relatives au trafic soient communiquées à des autorités étatiques, plutôt que directement aux titulaires de droits lésés[632]. Cette solution offre la garantie que « la communication demeure dans de justes proportions par rapport aux positions juridiques protégées »[633] et les autorités étatiques sont directement tenues par les droits fondamentaux, contrairement aux particuliers, et elles doivent respecter les garanties de procédure, ce qui apparaît comme étant plus proportionné[634]. En effet, les données de trafic des utilisateurs ne devraient être communiquées que dans des contextes particuliers et ce afin de respecter la confidentialité des communications.

Dans l'affaire *Bonnier*, la Cour de justice, après avoir rejeté l'application de la directive 2006/24/CE pour la question de la communication par un FAI à un ayant droit de l'identité d'un abonné à qui une adresse IP a été attribuée et qui aurait servi à l'atteinte à un droit d'auteur, donne des éléments complémentaires d'interprétation à ce qu'elle a déjà annoncé dans les affaires *Promusicae* et *LSG*. En effet, la Cour relève que la Suède a décidé de se prévaloir de la faculté qui lui était offerte de prévoir une obligation de transmission de données à caractère personnel, dans le cadre d'une procédure civile, à des personnes privées, via sa loi IPRED. Alors que cela ne lui était pas demandé, la Cour a décidé de son propre chef d'évaluer la loi suédoise et s'est posée la question de savoir si elle

[629] C.J.C.E., 6 novembre 2003, *Lindqvist*, C-101/01.
[630] F. COUDERT et E. WERKERS, *op. cit.*, p. 83.
[631] Conclusions de l'avocat général J. KOKOTT dans l'affaire *Promusicae*, §§ 106.
[632] *Ibidem*, §§ 112 et 113
[633] *Ibidem*, § 113.
[634] *Ibidem*, § 114.

répondait aux exigences qui découlent des arrêts *Promusicae* et *LSG*, à savoir « assurer un juste équilibre entre la protection du droit de propriété intellectuelle, dont jouissent les titulaires de droit d'auteur, et la protection des données à caractère personnel dont bénéficie un abonné à Internet ou un utilisateur d'Internet »[635]. Selon la Cour tel est le cas car « cette législation permet à la juridiction nationale saisie d'une demande d'injonction de communiquer des données à caractère personnel, introduite par une personne ayant qualité pour agir, de pondérer, en fonction des circonstances de chaque espèce et en tenant dûment compte des exigences résultant du principe de proportionnalité, les intérêts opposés en présence »[636]. La Cour de justice nous donne ici une application pratique de ce qu'une loi nationale doit contenir pour respecter les prescrits en terme d'équilibre des droits fondamentaux en présence[637].

[635] Arrêt *Bonnier,* § 60.
[636] *Ibidem*, § 59.
[637] Voir *supra*.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Section 4. Autres droits fondamentaux

§1. La préservation de la liberté d'expression et du droit de recevoir des informations

La surveillance et le blocage de sites web ne sont-ils pas susceptibles d'entraver la liberté d'expression et son corollaire, le droit d'accéder à l'information ? A quelles **conditions** cette restriction peut-elle être admise et avec quelles **mesures de précaution ou garanties** ?

I. Généralités

Lorsque des mesures sont imposées pour mettre fin à ou prévenir des atteintes à un droit de propriété intellectuelle, il est essentiel de veiller à assurer un juste équilibre, une mise en balance entre les droits et libertés, équilibre qui constitue un des angles du « triangle diabolique » que nous avons rencontrés *supra*. Nous avons déjà étudié la balance à réaliser entre les droits de propriété intellectuelle et la protection de la vie privée, mais il faut également trouver un équilibre entre la propriété intellectuelle et le droit à la liberté d'expression.

Certains droits consacrés par la Convention européenne des droits de l'Homme sont « intangibles », tels que le droit à la vie ou le droit de ne pas être torturé, tandis que d'autres sont « conditionnels », parce qu'ils peuvent être l'objet de dérogations, de restrictions, ce qui est le cas du droit à la liberté d'expression. Cette dernière « constitue l'un des fondements essentiels d'une société démocratique »[638], et comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées, et ce sans considération de frontière[639]. Elle est garantie par l'article 19 de la Déclaration universelle des droits de l'Homme (non directement applicable en Belgique), l'article 19 du Pacte international sur les droits civils et politiques (ci-après « le PIDCP »), et l'article 10 de la Convention EDH.

L'article 10 de la Convention EDH prévoit en son paragraphe 1 que « toute personne a le droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière (…) ». Le second paragraphe ajoute que « l'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, condition, restrictions ou sanctions, prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ». La Charte des droits fondamentaux de l'Union européenne prévoit en son article 11, §1 que « (t)oute personne a droit à

[638] CEDH, *Christine Goodwin c. Royaume-Uni*, 11 juillet 2002, no. 28957/95, §
[639] CEDH, *Sunday Times c. Royaume-Uni*, 26 avril 1979, § 65.

la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières ». Dans la Charte est fait le lien avec la Convention EDH, via son article 52 : « Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ». Depuis l'entrée en vigueur du traité de Lisbonne en décembre 2009, est conférée à la Charte des droits fondamentaux une force contraignante.

Il est prévu que l'exercice du droit à la liberté d'expression comporte des « devoirs et des responsabilités », et peut être soumis à certaines restrictions. Pour restreindre ce droit, il faut que l'ingérence soit conforme à l'article 10, paragraphe 2 de la Convention EDH qui prévoit trois conditions cumulatives à respecter : les restrictions doivent être « prévues par la loi », légitimes et proportionnelles. Selon la Cour EDH, le principe de légalité signifie que la loi considérée doit répondre à au moins deux conditions[640] : premièrement, il faut que « la loi soit suffisamment accessible », « le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné »[641] ; deuxièmement, « on ne peut considérer comme une "loi" qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ». Le citoyen doit dès lors, « être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »[642]. Nous étudierons dans le point suivant ce que cette exigence de légalité implique comme conséquence en cas de prise de mesures préventives. Concernant la condition de légitimité, il est exigé que la restriction poursuive l'un des objectifs légitimes énumérés à l'article 10, qui sont limitativement énumérés : il faut que la restriction vise à « la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ». Le PIDCP prévoit quant à lui que les restrictions « doivent être expressément fixées par la loi et (…) doivent (être) nécessaires (…) au respect des droits ou de la réputation d'autrui », ou « à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques ». Dans le cadre de notre rapport, nous retiendrons principalement l'objectif de « protection de la réputation ou des droits d'autrui ». Une balance des intérêts doit être réalisée lorsqu'est prise en compte l'objectif de « protection de la réputation et des droits d'autrui », telle qu'elle ressort de la jurisprudence de la Cour EDH : « En l'espèce, le seul but invoqué par le Gouvernement pour justifier l'ingérence incriminée est celui de la 'protection des droits et libertés d'autrui'. Si ces 'droits et libertés' figurent eux-mêmes parmi ceux garantis par la Convention ou ses Protocoles, il faut admettre que la nécessité de les protéger puisse conduire les Etats à restreindre d'autres droits ou libertés également consacrés par la Convention : c'est précisément cette constante recherche d'un équilibre entre les droits fondamentaux de chacun qui constitue le fondement d'une 'société démocratique'. La mise en balance des intérêts éventuellement contradictoires des uns et des autres est alors difficile à faire, et les Etats contractants doivent disposer à cet égard d'une marge

[640] *Sunday Times c. Royaume-Uni*, § 48.
[641] *Ibidem*, § 49.
[642] *Idem*.

d'appréciation importante, les autorités nationales étant en principe mieux placées que le juge européen pour évaluer l'existence ou non d'un 'besoin social impérieux' susceptible de justifier une ingérence dans l'un des droits garantis par la Convention' »[643].

Enfin, la condition de proportionnalité, dite principe de nécessité dans une société démocratique, implique que la restriction soit « nécessaire dans une société démocratique », qu'elle réponde à un « besoin social impérieux ». Selon la Cour européenne des droits de l'Homme, « l'adjectif "nécessaire" (…) implique l'existence d'un "besoin social impérieux" » ; il « n'est pas synonyme d'"indispensable", il n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun" »[644]. Cette dernière condition se subdivise elle-même en trois sous-conditions : « (t)oute mesure (…) concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques qui serait susceptible de limiter les libertés et droits fondamentaux précités ne peut être instituée que si elle est appropriée, proportionnée et nécessaire dans le cadre d'une société démocratique »[645].

Appliquer ces diverses garanties à l'univers numérique ne pose aucun obstacle de principe[646], ce que confirme une Déclaration du Comité des Ministres du Conseil de l'Europe : « la liberté d'expression, d'information et de communication doit être respectée dans un environnement numérique tout comme dans un environnement non numérique. Elle ne doit pas être soumise à d'autres restrictions que celles prévues à l'article 10 de la Convention, pour la simple raison qu'elle s'exerce sous une forme numérique »[647]. Toujours selon le Comité, « le développement des technologies et des services de l'information et de la communication devrait contribuer à ce que toute personne jouisse des droits garantis par l'article 10 de la Convention européenne des droits de l'Homme, dans l'intérêt de chacun et dans celui de la culture démocratique de toute société »[648]. Dans l'un de ses arrêts récents, la Cour EDH a clairement énoncé que la liberté d'expression profite aux propos diffusés sur internet : « Grâce à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information ». Toujours selon la Cour, « compte tenu de son accessibilité et de sa capacité à stocker et à communiquer des quantités importantes d'informations, Internet joue un rôle important dans l'amélioration de l'accès du public à l'actualité et facilite la dissémination de l'information de manière générale »[649]. Selon le Parlement européen, le libre accès à internet, sans ingérence injustifiée ou même arbitraire, est un droit d'une considérable importance. Internet est « une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre

[643] CEDH, *Chassagnou c. France*, 29 avril 1999, § 113.
[644] *Sunday Times c. Royaume-Uni*, § 59.
[645] Nouvel article 1, 3*bis* de la directive « cadre ».
[646] P.-F. DOCQUIR, « Contrôle des contenus sur internet et la liberté d'expression au sens de la Convention européenne des droits de l'Homme », *CDPK*, 2002, p. 174.
[647] Déclaration sur les droits de l'Homme et l'état de droit dans la Société de l'information adoptée par le Conseil des Ministres le 13 mai 2005 lors de la 926ème réunion des Délégués des ministres, www.coe.int.
[648] *Idem*.
[649] C.E.D.H. (4e sect.), *Times Newspapers LTD (n° 1 et 2) c. Royaume-Uni*, 10 mars 2009, *R.D.T.I.*, n° 37/2009, § 27.

générations dans la société de l'information », et dont l'accès est protégé par le droit à la liberté d'expression[650].

A côté des obligations négatives des Etats, il existe une obligation positive pour ceux-ci de prendre toutes les mesures raisonnables pour empêcher les violations de la liberté d'expression. En effet, les ingérences à ce droit peuvent être le fait de l'Etat, mais pas seulement, il doit assurer la jouissance effective de ce droit aux personnes se trouvant sous sa juridiction[651]. La Cour EDH a affirmé que « l'exercice réel et efficace de cette liberté ne dépend pas simplement du devoir de l'Etat de s'abstenir de toute ingérence, mais peut exiger des mesures positives de protection juridique dans les relations des individus entre eux »[652]. Les Etats seraient dès lors contraints « à adopter un cadre réellement rassurant pour les intermédiaires afin d'éviter la censure privée qu'ils risqueraient d'opérer par crainte d'une action en responsabilité »[653].

II. Fournisseurs d'accès et liberté d'expression

La directive 2000/31 sur le commerce électronique fait explicitement référence en son considérant 9 à la liberté d'expression consacrée par l'article 10 de la C.E.D.H. Il dispose que « les directives couvrant la fourniture de services de la société de l'information doivent assurer que cette activité peut être exercée librement en vertu de l'article précité, sous réserve uniquement des restrictions prévues au paragraphe 2 du même article (…). La présente directive n'entend pas porter atteinte aux règles et principes fondamentaux nationaux en matière de liberté d'expression. »

Un des buts que le législateur avait à l'esprit en instaurant un régime d'exonération conditionnelle de responsabilité et en les épargnant de procéder eux-mêmes au contrôle de tout ce qui se passe sur leurs réseaux était la promotion de la liberté d'expression. Cela permet actuellement aux intermédiaires de développer des nouveaux services de la société de l'information, de favoriser les contenus créés par les utilisateurs, d'éviter toute censure préalable.[654] Il y a une volonté commune à l'Europe communautaire et au Conseil de l'Europe de promouvoir la société de l'information et, plus largement, la liberté d'expression à travers le développement des technologies de l'information et des réseaux de communication[655].

Comme nous l'avons vu *supra*, les intermédiaires techniques sont un passage obligé pour la transmission des informations sur internet. Il n'est pas contesté que les intermédiaires bénéficient de la liberté d'expression telle qu'édictée par l'article 10 de la Convention européenne des droits de l'homme. De plus, cette disposition vise également les informations de nature commerciale. Une lecture évolutive des arrêts de la Cour EDH nous amène à pouvoir leur transposer les arrêts de la Cour qui ont énoncé que les éditeurs qui fournissent un support aux auteurs bénéficient des garanties offertes par l'article 10 de la CEDH en ce qu'ils participent à la liberté d'expression. Dans un

[650] Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe, 2007/2153(INI), § 23, disponible sur http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//FR
[651] Q. VAN ENIS et E. MONTERO, *op. cit.*, p. 89.
[652] CEDH, *Appleby et a. c. Royaume-Uni*, 6 mai 2003, §§ 39-40.
[653] Q. VAN ENIS et E. MONTERO, *op. cit.*, p. 89.
[654] *Ibidem*, p. 87.
[655] *Idem*.

arrêt concernant plus particulièrement la réception d'émissions télévisées que « l'article 10 protège tant le contenu des informations que les moyens de les transmettre et de les capter, car toute restriction à ceux-ci touche le droit de recevoir et communiquer des informations »[656].

Nous avons vu au point précédent que les ingérences dans le droit à la liberté d'expression peuvent, non seulement être directement le fait de l'Etat, mais aussi résulter de demandes d'injonctions instrumentées par les titulaires de droit d'auteur ou de droits voisins. Il est nécessaire de s'assurer que les mesures imposées par injonction ne portent pas atteinte au droit à la liberté d'expression. Une ingérence dans ce droit ne serait admissible que si elle est prévue par la loi, orientée vers l'un des buts légitimes limitativement énumérés au paragraphe 2 de l'article 10 de la Convention, et proportionnée au but légitime poursuivi.

III. Blocage / filtrage et liberté d'expression

Comme nous l'avons vu, la liberté d'expression inclut le droit de communiquer et de recevoir des informations, y compris dans l'environnement numérique, par l'intermédiaire d'internet, et toute mesure de restriction qui empêcherait un individu d'accéder à un contenu, ou d'en fournir un, serait contraire à cette liberté. Imposer une mesure de filtrage risque de porter atteinte au droit à la liberté d'expression, en constituerait une restriction, du fait justement qu'il empêche l'accès ou la mise à disposition en ligne de/à l'information. Une injonction qui viserait à interdire un type d'atteinte – sans être un acte ponctuel – serait contraire à la fois à l'interdiction d'une obligation générale de surveillance, et à la liberté de « recevoir ou communiquer (sans censure) des informations ». L'interdiction d'imposer une obligation générale de surveillance aux prestataires se justifie au regard de la sauvegarde de la liberté d'expression ainsi que de la censure préventive. C'est d'ailleurs dans l'optique de la mise en place de mesures de filtrage et de blocage qu'une telle interdiction a été instaurée, comme cela ressort du premier rapport de 2003 de la Commission européenne sur la directive 2000/31 sur le commerce électronique[657]. Le considérant 9 de la directive 2000/31 sur le commerce électronique dispose quant à lui que « (…) les directives couvrant la fourniture de services de la société de l'information doivent assurer que cette activité peut être exercée librement en vertu de l'article précité, sous réserve uniquement des restrictions prévues au paragraphe 2 du même article (…) ». La première question qui va se poser est celle de savoir si la propriété intellectuelle peut être considérée comme suffisamment importante pour peser dans la balance.

A. Conciliation avec la propriété intellectuelle

Pour pouvoir faire le poids dans la balance des intérêts en présence, et donc permettre une ingérence au droit à la liberté d'expression, il est nécessaire que le droit à la protection des droits de propriété intellectuelle soit considéré comme suffisamment important. Ces droits sont protégés par un certain nombre de traités au niveau international, tel que la DUDH qui prévoit en son article 27, 2

[656] CEDH, *Khurshid Mustafa et Tarzibachi c. Suède*, 16 déc. 2008, § 32.

que « chacun a droit à la protection des intérêts moraux et matériel découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur », ainsi que le PIDCP et son article 15, 1. La Cour EDH a considéré que les droits de propriété intellectuelle ressortissent du champ d'application de l'article 1er du Protocole additionnel de la CEDH qui consacre le droit de propriété : « Au vu de la jurisprudence susmentionnée, la Cour fait sienne la conclusion de la chambre selon laquelle l'article 1 du Protocole no 1 s'applique à la propriété intellectuelle en tant que telle »[658]. Au niveau de l'Union européenne, la Charte prévoit en son article 17, 2 que « la propriété intellectuelle est protégée ». Le droit à la protection des droits de propriété intellectuelle est donc considéré comme un droit de l'Homme et une liberté fondamentale, et il peut en conséquence être invoqué en justification d'une mesure de restriction sur internet, comme le filtrage ou le blocage.

La question à se poser est celle de savoir si le droit d'auteur, ou la propriété intellectuelle en général, est en mesure d'être une raison suffisante pour justifier le blocage ou le filtrage de contenu, et par là porter atteinte à la liberté d'expression. La directive 2001/29 sur le droit d'auteur dans la société de l'information fait le lien avec la liberté d'expression en se rapportant au « respect des principes fondamentaux du droit et notamment de la propriété, dont la propriété intellectuelle, et de la liberté d'expression et de l'intérêt général »[659]. La liberté d'expression peut subir des restrictions, dans le but de garantir le droit d'auteur, ce droit étant lui-même « limité par la reconnaissance d'exceptions légales, elles-mêmes justifiées par la prise en compte de la liberté d'expression », et c'est donc « l'équilibre consacré par le droit d'auteur lui-même, entre la protection des droits des auteurs et la protection ''des intérêts tout aussi légitimes du public et de la société en général'' qui résout le conflit éventuel entre propriété littéraire et artistique et liberté d'expression. »[660] Le droit d'auteur offrant des droit exclusifs à ses bénéficiaires, sur de l'information, cela implique qu'un risque de conflit existe entre ce droit et le droit à la liberté d'expression[661]. Il importe que si le droit d'auteur est mis en œuvre délibérément en tant que moyen de censure pour empêcher la libre circulation d'informations, c'est la liberté d'expression qui doit nécessairement prévaloir[662].

B. Les conditions de l'article 10, § 2 de la Convention EDH

Il s'agit d'une liberté conditionnelle et non intangible, qui est susceptible de limitations, dans le respect d'un certain nombre de conditions que nous avons analysées au point I. Pour être admissible, une ingérence à la liberté d'expression doit donc respecter les trois conditions limitatives du paragraphe 2 de l'article 10, c'est-à-dire être prévue par la loi, légitime et proportionnée à l'objectif poursuivi[663]. Il s'agit maintenant de confronter ces différentes conditions avec l'imposition d'une mesure de filtrage ou de blocage de sites internet dans le cadre de la protection de la propriété intellectuelle.

---

[658] CEDH, gde. ch., arrêt *Anheuser-Busch Inc. c. Portugal*, 11 janvier 2007, § 72
[659] Considérant 3 de la directive 2001/29.
[660] S. DUSOLLIER, « Le géant aux pieds d'argile : Google News et le droit d'auteur », *Revue Lamy droit de l'immatériel*, avril 2007, n° 26, pp. 70 à 75.
[661] G. GATHEM et A. STROWEL, « Droit d'auteur versus liberté d'expression et responsabilité des fournisseurs de services sur l'Internet », *A&M* 2004/1, p. 51.
[662] *Idem*.
[663] Voir *supra*.

Concernant la première condition, dite de légalité, il est tout à fait raisonnable de considérer que la possibilité d'une injonction prenant la forme d'une mesure de filtrage ou de blocage soit effectivement prévue par la loi, en l'occurrence la législation européenne. Mais les intermédiaires et les internautes peuvent-ils suffisamment prévoir les conséquences qui pourraient découler de l'adoption par eux d'un comportement déterminé ? Les individus doivent en effet pouvoir déterminer, et cela avec un degré suffisant de prévisibilité, les conséquences de leurs comportements[664]. Il apparaît également que « même en s'entourant de conseils éclairés, les intermédiaires de l'internet ne semblent pas en mesure de prévoir, à un degré raisonnable, qu'une mesure de filtrage, fut-elle limitée à un contenu spécifique, puisse leur être imposée »[665]. Il est nécessaire de prévoir dans le droit national une disposition suffisamment claire et précise, et la question de savoir s'il est possible de prévoir le filtrage via un texte non législatif dépendra des dispositions constitutionnelles propres à chaque Etat[666].

La deuxième condition porte, elle, sur la nécessité de respecter l'un des objectifs légitimes énumérés au paragraphe 2 de l'article 10. Un de ces objectifs légitimes est « la protection de la réputation et des droits d'autrui », et c'est dans ce cadre que se place l'instauration de mesures de filtrage. De plus, la propriété intellectuelle a été établie par la Cour EDH comme tombant dans le champ d'application de l'article 1[er] du Protocole additionnel à la Convention EDH (voir *infra*). Le retrait ou la suppression de certains contenus illicites, protégés par la propriété intellectuelle, entre dans cet objectif de protection des droits d'autrui, la deuxième condition étant dès lors satisfaite dans la mise en place de mesures de filtrage. Si l'on prend l'exemple d'une mesure de filtrage instituée sur un réseau de *peer-to-peer* pour lutter contre les échanges illicites entre internautes d'œuvres protégées par le droit d'auteur, l'objectif est clairement la protection des droits des ayants droit, et par là répondrait au but de « protection des droits d'autrui »[667].

Enfin, la troisième condition, celle de proportionnalité, prévoit que la restriction doit répondre à un « besoin social impérieux », et être justifiée par des « motifs pertinents et suffisants »[668], c'est-à-dire pouvoir se justifier dans une société démocratique. Cette condition est elle-même subdivisée en 3 sous-conditions : la mesure doit être appropriée, nécessaire et proportionnée au sens strict. Ces conditions se retrouvent dans le nouvel article 1, 3*bis* de la directive cadre. L'implémentation d'une mesure de filtrage d'un réseau internet doit dès lors « correspondre à un besoin réel de la société, la satisfaction de ce dernier impliquant encore que la mesure soit efficace »[669]. Il faut donc se poser la question du caractère approprié d'une mesure, de son efficacité. La Cour de justice dans son arrêt Scarlet avait estimé que « (l') injonction 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

[664] *Sunday Times c. Royaume-Uni*, § 49.
[665] E. MONTERO et Q. VAN ENIS, *op. cit.*, p..98.
[666] C. CALLANAN, M. GERCKE, E. DE MARCO et H. DRIES-ZIEKENHEINER, Rapport – Filtrage d'Internet : Equilibrer les réponses à la cybercriminalité dans une société démocratique, 11 mai 2012, p. 216.
[667] Rapport filtrage d'Internet, *op. cit.*, p. 219.
[668] *Sunday Times c. Royaume-Uni*.
[669] Rapport filtrage d'Internet, *op. cit.*, p. 224.

la part des auteurs concernés. »[670] Scarlet avait elle-même souligné que « la licéité d'une transmission est une donnée inaccessible à la technique ». L'avocat général, dans ses conclusions dans ladite affaire, avait considéré que « l'imposition à un FAI d'une mesure de filtrage telle que celle en cause « ne représente pas, en elle-même, les caractéristiques de concrétude et d'individualisation qui sont normalement attendues de toute riposte ou réaction à une conduite supposée spécifique et déterminée ». La problématique du sur-blocage ou du sous-blocage, qui est inévitable dans la mise en place d'un tel mécanisme, implique que la condition d'effectivité sera difficilement remplie. En effet, les mesures de filtrage risquent inévitablement « soit de conduire à la suppression et au blocage de contenus qui ne portent nullement atteinte à des droits de propriété intellectuelle, soit de laisser passer des communications illicites »[671]. Il a été prouvé qu'outre les problèmes de sur- ou sous-blocage que cela implique, il y a un risque de voir les échanges en *peer-to-peer* chiffrés quelques mois après l'application d'une mesure de filtrage, ce qui conduirait en un empêchement de toute nouvelle tentative de filtrage, le rendant caduque et empêchant également toute surveillance des contenus échangés. Il y a également la problématique du contournement aisé des mesures mises en place, que ce soit par les internautes, mais également par le propriétaire du site lui-même.

Dans ces conditions, le téléchargement et les échanges illégaux risquent de continuer à se propager en toute impunité. Il ne s'agit donc pas de la mesure la moins préjudiciable à la liberté d'expression, ce qui implique qu'elle ne remplit pas la sous-condition de nécessité qui suppose que la mesure choisie doit être celle qui est la moins préjudiciable aux droits en cause. Il faudrait, enfin, qu'il y ait respect de la proportionnalité au sens strict, qui veut qu'il n'y ait pas de disproportion excessive entre l'intérêt légitime que l'on souhaite protéger par rapport aux autres intérêts juridiques en cause. C'est donc entre les mesures de filtrage qui seraient imposées aux intermédiaires – avec leurs conséquences sur les utilisateurs – et la protection des droits de propriété intellectuelle que cette balance doit se faire. Même s'il est décidé d'opter pour des mesures de filtrage limitées à un contenu spécifique, cela n'empêchera pas leur contournement et la réapparition de ce contenu, ni les erreurs en ce qui concerne l'appréciation de la légalité de ce contenu au regard des droits intellectuels – les techniques en la matière ne sont pas au point pour distinguer si tel ou tel contenu entre ou non dans le champ d'une éventuelle exception par exemple[672]. Et puis, peut-on décider du blocage d'un site entier alors que tous les contenus ne sont pas illicites ? A partir de quand dans ce cas-là y aurait-il disproportion ? Il ressort des discussions ayant précédé l'adoption de la Recommandation du Comité des Ministres que « si une partie importante du contenu bloqué est en fait inoffensive, la restriction imposée à la liberté d'expression peut être considérée comme disproportionnée au regard du but légitime poursuivi »[673].

Des précisions seront bientôt apportées par la Cour EDH à l'interprétation de l'article 10 de la Convention EDH relativement aux mesures de filtrage et de blocage, et donc au non accès à certains contenus sur internet, avec deux affaires qui sont pendantes devant elle. L'affaire *Yildirim c. Turquie* concerne une mesure de blocage de tous les sites hébergés par Google (https://sites.google.com), dont la page personnelle du requérant, aux fins de bloquer une URL précise mise en cause dans une

[670] Arrêt *Scarlet*, § 52.
[671] E. MONTERO et Q. VAN ENIS, *op. cit.*, pp. 98 et 99.
[672] *Ibidem*, p. 98.
[673] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, 26 mars 2008.

affaire pénale[674]. Dans l'autre affaire, *Akdeniz c. Turquie*, le requérant se plaint, en tant qu'utilisateur, du blocage d'un site de réseau social (myspace.com) et d'un site consacré à la musique (last.fm) prononcé au motif que ces sites diffusaient sans autorisation des œuvres protégées par le droit d'auteur[675]. Il est question ici de mesures qui ont une portée trop large et qui mettent à mal l'accès à l'information pour les utilisateurs d'internet.

Quoi qu'il en soit, filtrer du contenu suppose, pour celui qui l'exerce, d'avoir le droit de procéder à ce filtrage et donc de « priver certaines personnes de leur droit d'accéder à un contenu électronique, d'utiliser un protocole de communication particulier, ou de communiquer un contenu donné à certains individus ou d'une certaine façon »[676]. La Déclaration du Conseil de l'Europe sur la liberté de communication sur internet affirme qu' « à condition que les garanties de l'article 10, paragraphe 2, de la (CEDH) soient respectées, des mesures peuvent être prises pour supprimer un contenu internet clairement identifiable ou, alternativement, faire en sorte de bloquer son accès si les autorités nationales ont pris une décision provisoire ou définitive sur son caractère illicite »[677]. Mais « il ne faut pas que le filtrage devienne un incontournable outil de lutte généralisée et systématique contre les atteintes à des droits intellectuels, ce qui apparaît contraire à chacune des limitations assignées au pouvoir d'injonction, telles que découlant des directives 2000/31 et 2004/48 ainsi que des autres règles de droit auxquelles ces directives font référence. »[678]

Un outil intéressant pour évaluer les mesures de filtrage est la recommandation du Conseil de l'Europe à ce sujet, et ce même s'il ne s'agit que de *soft law*[679]. Il ressort des lignes directrices que le recours au filtrage n'est possible que pour poursuivre l'un des objectifs de l'article 10 de la Convention EDH, avec la possibilité de l'utiliser pour bloquer l'accès à des contenus protégés par le droit d'auteur qui seraient diffusés illicitement. Des mesures étatiques de filtrage ne devraient être prises que si le filtrage concerne un contenu spécifique et clairement identifiable, une autorité nationale compétente a pris une décision au sujet de l'illégalité de ce contenu et la décision peut être réétudiée par un tribunal ou entité de régulation indépendant et impartial[680]. Il faut également « veiller à ce que tous les filtres soient évalués avant et pendant leur mise en œuvre, et cela afin de vérifier que les effets du filtrage sont en adéquation avec l'objectif de la restriction (…) », pour éviter tout blocage excessif des contenus[681].

Enfin, la France a décidé d'abandonner la publication du décret relatif au filtrage des contenus pédopornographiques alors que l'article 4 de la loi d'orientation et de programmation pour la performance de la sécurité intérieure – dite LOPPSI 2 – prévoit l'instauration d'un système de blocage pour les sites diffusant du contenu pédopornographique, via l'intervention d'une autorité

[674] CEDH, *Yildirim c. Turquie*, affaire pendante (3111/10)
[675] CEDH, *Akdeniz c. Turquie*, affaire pendante (20877/10).
[676] Rapport filtrage d'internet, *op. cit.*, p. 161.
[677] Comité des Ministres, Déclaration du Conseil de l'Europe sur la liberté de communication sur l'internet, 28 mai 2003, principe 3, p. 5.
[678] *Idem*.
[679] Recommandation du Conseil de l'Europe, CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, 26 mars 2008.
[680] Recommandation du Conseil de l'Europe, III., ii.
[681] *Ibidem*, III., iv.

administrative pour procéder au blocage des sites en cause.[682] Le Conseil constitutionnel avait pourtant déclaré ce texte « conforme à la Constitution » et que « la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé »[683].

C. Le filtrage volontaire

La recommandation sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet fait la distinction entre le filtrage obligatoire imposé par l'intervention de l'Etat et le filtrage volontaire des acteurs[684]. Le filtrage qui résulte d'une intervention étatique doit toujours se conformer aux exigences de l'article 10, § 2 de la CEDH. Or, l'intervention de l'Etat aura lieu non seulement dans le cadre d'une action des pouvoirs publics directement imputable à l'Etat, mais aussi lorsque des organismes privés agissent sur instruction de l'Etat.[685]

Mais la mise en place de mesures de filtrage peut également être faite sur une base tout à fait volontaire, que ce soit par des acteurs privés ou publics – des individus, des institutions du secteur public ou privé, des établissements scolaire, des entreprises, *etc*[686]. Le filtrage volontaire n'est pas épargné par le risque d'atteinte à la liberté d'expression, mais il ne relève pas directement de l'article 10, paragraphe 2 de la Convention EDH. En plus des obligations négatives, les Etats sont tenus par ce que l'on appelle les obligations positives[687], ce qui implique qu'ils doivent s'engager à garantir la jouissance effective d'un droit fondamental à tous leurs citoyens, et cela sans qu'ils ne soient à la base de leur violation. Ils seront tenus par ces obligations positives même lorsque les mesures de filtrage ne proviennent pas de leur initiative. Il ressort des discussions qui ont précédé l'adoption de la Rec(2008)6 du Comité des Ministres que « (b)ien que les acteurs privés ne soient pas directement liés par l'article 10, la décision d'interdire à une personne l'usage d'un ordinateur pour accéder à certains contenus Internet soulève un problème de liberté d'expression et (…) devrait aussi faire l'objet d'une justification »[688].

La recommandation du Conseil de l'Europe comporte également des règles directrices concernant le filtrage volontaire, que ce soit un « auto-filtrage » ou via des accords volontaires négociés entre différents acteurs. Celles-ci prévoient qu'il faut veiller à évaluer et à réétudier régulièrement l'efficacité de la mise en place de filtres, et son caractère proportionnel[689] ; à renforcer les informations et les conseils aux utilisateurs concernés par des filtres sur des réseaux privés – leur existence, justification et critères de fonctionnement[690] ; à coopérer avec les utilisateurs pour

[682] « Loppsi 2 : Le gouvernement pourrait abandonner le blocage des sites sans juge », *Le Monde*, 25 juillet 2012, disponible sur http://www.lemonde.fr/technologies/article/2012/07/25/loppsi-2-le-gouvernement-pourrait-abandonner-le-blocage-des-sites-sans-juge_1738020_651865.html
[683] Décision Conseil constitutionnel
[684] *Idem*.
[685] C. ANGELOPOULOS, *op. cit.*, p. 7.
[686] *Ibidem*, p. 8.
[687] Voir *supra*.
[688] Rec(2008)6, § 45
[689] Recommandation du Conseil de l'Europe, III., § 2, i.
[690] *Ibidem*, III., § 2, ii.

améliorer la transparence, l'efficacité et le caractère proportionnel des filtres[691].

La directive 2000/31 sur le commerce électronique encourage le volontariat en la matière, en prévoyant dans son considérant 40 qu'il faut permettre « l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible » et qu' « 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 ». Les accords volontaires entre parties prenantes sont à encourager en matière de lutte contre le piratage en ligne.

En conclusion, il semble évident que toute mesure de filtrage limite le droit à la liberté d'expression, et cela dans une mesure plus ou moins grande en fonction des caractéristiques du filtrage et selon son degré d'efficacité – entendons s'il n'est pas excessif (*overinclusive*) – l'objectif étant clairement la limitation de l'accessibilité des contenus. L'enjeu est donc ici la détermination de la mesure dans laquelle une liberté peut être limitée dans l'objectif d'en préserver une autre, au regard des conditions du paragraphe 2 de l'article 10 de la Convention EDH Toute mesure de filtrage qui constituerait une ingérence dans l'exercice du droit à la liberté d'expression devra respecter les conditions énumérées dans cette clause d'ordre public.

IV. La suspension de l'accès à internet

Les considérations portant sur les mesures de filtrage et de blocage sont à transposer en matière de coupure de la connexion internet, et plus particulièrement en ce qui concerne les conditions du paragraphe 2 de l'article 10 qui permettent une ingérence au droit à la liberté d'expression. Cette question sera également traitée au point suivant du présent rapport.

Il est intéressant de soulever que le Conseil constitutionnel français a considéré que le droit d'accéder à internet est protégé sous le principe de la liberté d'expression : « en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services »[692]. Le Parlement européen considère également que la suspension de la connexion à internet est en contradiction avec les garanties accordées aux droits fondamentaux, mais sans préciser si c'est parce qu'internet permet l'exercice de ces libertés, ou si l'accès à internet est un droit fondamental en lui-même[693]. Par une résolution du 10 avril 2008, le Parlement engage « la Commission et les États membres à reconnaître qu'Internet est une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information, et, par conséquent, à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à Internet ». En lien avec le filtrage, il a été dit que le conflit entre protection de la propriété

[691] *Ibidem*, III., § 2, iii.
[692] Conseil constitutionnel français, décision n° 2009-580 DC du 10 juin 2009, considérant 12, disponible sur www.conseil-constitutionnel.fr.
[693] C. CALLANAN, M. GERCKE, E. DE MARCO, H. DRIES-ZIEKENHEINER, « Filtrage d'internet (…) », *op. cit.,* p 28.

intellectuelle et liberté d'expression « serait encore plus grand si la mesure préconisait la suspension d'un accès à Internet, prévenant ou empêchant par là même une personne d'utiliser l'ensemble du réseau Internet ou une partie de celui-ci »[694].

§2. La neutralité du net et le droit d'accès à internet

Existe-t-il un **droit fondamental d'accès à l'internet** ? Dans l'affirmative, une mesure de coupure d'internet ou de blocage d'un site Internet y porte-t-elle atteinte ?

La question qui se pose ici est de savoir si l'on peut bloquer l'accès à un site internet pour un utilisateur. Avec les techniques disponibles actuellement, il est tout à fait réalisable de discriminer[695] certains services et contenus, en les transmettant plus lentement, voire pas du tout[696]. Quelles sont les conditions pour qu'il puisse être demandé à un fournisseur d'un service de la société de l'information de procéder à un contrôle et une gestion du trafic ? Se posera également la question de la suspension de la connexion pour l'internaute qui aurait enfreint le droit d'auteur.

I. Définition

Il n'existe pas de définition établie de la « neutralité d'internet ». On retrouve malgré tout des définitions issues de la doctrine : la neutralité du net est « l'idée qu'un réseau d'informations public extrêmement utile tend à traiter tous les contenus, sites et plateformes de manière égale. Ceci permet au réseau de véhiculer chaque type d'informations et de soutenir toutes sortes d'applications »[697]. Il s'agit donc de « l'égal accès des internautes à tous les contenus, services et applications de la toile »[698]. Dans cette acceptation, la neutralité du net « est un principe selon lequel tous les contenus doivent bénéficier de la même qualité de service de transmission lorsqu'ils sont transmis sur les réseaux, et ce en excluant toute tentative de priorisation ou de préférence par les opérateurs de réseaux ».

En parallèle s'est développée ce que l'on appelle la « quasi-neutralité », conception selon laquelle « un traitement différencié serait autorisé, pour autant que ces exceptions soient en nombre raisonnable et fixées aux travers de critères objectifs ». Nous aurons l'occasion de nous intéresser plus loin dans l'exposé à quelles contraintes peut être soumise la neutralité, mais nous pouvons déjà

[694] *Idem*.
[695] La discrimination des contenus peut être opérées sur base de différents critères : selon le type de protocole (ex.: ralentir les données utilisant le protocole VoIP ou Peer-to-Peer), selon le type de contenu (ex.: bloquer les spams) ou selon l'origine (ex. : interdire l'accès à certains services en fonction de l'utilisation d'une connexion à l'Internet mobile ou fixe) ou la destination du contenu (ex.: bloquer l'accès à un site internet particulier).
[696] M. PIRON, « La neutralité des réseaux et la garantie de la fourniture de services de médias audiovisuels », *R.D.T.I.*, n° 45/2011, p. 71.
[697] M. PIRON, *op. cit.*, voir T. WU, « Network neutrality, FAQ », disponible sur http://timwu.org/network_neutrality.html.
[698] N. CURIEN et W. MAXWELL, « La neutralité d'Internet », Paris, La Découverte, 2011, p. 3.

préciser qu'une neutralité excessive, sans possibilité d'exceptions, serait nuisible au bon fonctionnement d'internet.

II. Le cadre européen

En Europe, c'est l'article 8 de la directive « cadre » qui fixe les objectifs de cette neutralité. En son paragraphe 4, il est prévu que « (l)es autorités réglementaires nationales soutiennent les intérêts des citoyens de l'Union européenne, notamment (…) en favorisant la capacité des utilisateurs finals à accéder à l'information et à en diffuser, ainsi qu'à utiliser des applications et des services de leur choix »[699]. Le considérant 28 de ladite directive prévoit qu' « il appartient aux utilisateurs finals de décider des contenus qu'ils veulent envoyer et recevoir, des services, applications, matériels et logiciels qu'ils veulent utiliser à cette fin, et ce sans préjudice de la nécessité de préserver l'intégrité et la sécurité des réseaux et des services (…) ». Toutefois, il faut souligner que cette disposition est applicable sans préjudice des mesures nationales ou supranationales destinées à lutter contre les activités illicites[700]. Quoi qu'il en soit, selon la directive, il s'agit d'un droit dont les citoyens peuvent réclamer l'exécution[701].

D'autre part, le considérant 34 de la directive « droit des citoyens » prévoit que « les utilisateurs finals devraient bénéficier de la qualité de service qu'ils demandent mais, dans certains cas particuliers, il peut être nécessaire de faire en sorte que les réseaux de communications publics atteignent des niveaux de qualité minimaux, de manière à prévenir la dégradation du service, le blocage des accès et le ralentissement du trafic sur les réseaux ». Il est donc possible de la moduler, de la soumettre à des exceptions, et cela pour éviter la congestion des réseaux, par un mécanisme de gestion des flux, les autorités réglementaires nationales décidant des conditions objectives et nécessaires pour autoriser une différenciation de traitement[702].

La position de la Commission européenne en la matière est la suivante : « La Commission attache la plus haute importance au maintien du caractère ouvert et neutre de l'internet, en tenant pleinement compte de la volonté des co-législateurs de consacrer désormais la neutralité de l'internet et d'en faire un objectif politique et un principe réglementaire que les autorités réglementaires nationales devront promouvoir, au même titre que le renforcement des exigences de transparence qui y sont associées et la création, pour les autorités réglementaires nationales, de pouvoirs de sauvegarde leur permettant d'éviter la dégradation du service et l'obstruction ou le ralentissement du trafic sur les réseaux publics »[703].

En novembre 2009, le cadre réglementaire européen en la matière a fait l'objet d'une profonde modification, par l'adoption du paquet de réformes des télécommunications de l'Union européenne :

[699] Article 8.4, g) de la directive cadre.
[700] Communication de la Commission du 19 mai 2011, L'internet ouvert et la neutralité d'Internet en Europe, COM (2011) 222, disponible sur: http://ec .europa.eu/information_society/policy/ecomm/doc/library/communications_reports/netneutrality/comm-19042011.pdf
[701] M. PIRON, *op. cit.*, p. 77.
[702] M. PIRON, *op. cit.*, p. 78.
[703] Communication de la Commission européenne du 19 mai 2011, *op. cit.*

« Le Paquet Télécom »[704]. Ce cadre modifié contribue à préserver le caractère ouvert et neutre d'internet. Il était nécessaire d'accorder des compétences aux autorités réglementaires nationales, et cela pour assurer le double objectif de la qualité de service et de la transparence des informations qui y sont liées. La qualité des services ainsi que la transparence des informations peuvent être conçues comme étant des buts à atteindre, permettant de s'assurer que l'utilisateur puisse faire le choix qui lui convienne le mieux en ayant une meilleure connaissance des offres présentes sur le marché et que ce dernier puisse bénéficier de la meilleure qualité d'expérience possible[705]. Ces derniers revêtent une grande importance dans la matière, objectifs qui se retrouvent à l'article 8.4, g) de la directive « cadre », mais également dans la directive « service universel ». Nous retrouvons également dans cet article 8.4, g) de la directive, le principe fondamental de la liberté d'expression lorsqu'il énonce qu'il faut favoriser « la capacité des utilisateurs finals à accéder à l'information et à en diffuser ».

En effet, l'accès à internet est un outil qui se trouve au centre de l'exercice de plusieurs libertés fondamentales, comme la liberté d'expression et le droit à l'information. Le Conseil de l'Europe s'est également exprimé dans une déclaration à propos de la liberté d'expression : « Pour autant que cela s'avère nécessaire dans le contexte décrit ci-dessus, la gestion du trafic ne doit pas être perçue comme contradictoire au principe de neutralité des réseaux. Cependant, toute exception à ce principe devrait être considérée avec beaucoup de circonspection et être justifiée par des raisons impératives d'intérêt public majeur. Dans ce contexte, les Etats membres devraient être attentifs aux dispositions prévues par l'article 10 de la Convention européenne des droits de l'homme et à la jurisprudence pertinente de la Cour européenne des droits de l'homme. Les Etats membres pourraient également trouver utile de se référer aux lignes directrices de la Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet. »[706]

Toutes les dispositions devaient être transposées par les Etats membres pour le 25 mai 2011, mais en Belgique cela n'est toujours pas le cas, ce qui place le pays dans le collimateur de la Commission européenne, et s'expose dès lors à une action en manquement. Les Pays-Bas sont le premier pays européen, et le deuxième au monde, à avoir adopté une loi contraignante imposant le strict respect de la neutralité d'internet.

[704] Ce Paquet Télécom est constitué de cinq directives : la directive « cadre », la directive « accès », la directive « autorisation », la directive « service universel » et la directive « vie privée et communications électroniques » ainsi qu'un nouveau règlement instituant l'Organe des régulateurs européens des communications électroniques (ORECE).

[705] La qualité d'expérience est une appréciation subjective de la qualité d'un service perçue par un utilisateur. Elle peut être qualifiée de « mauvaise », par exemple, lorsque le délai d'attente pour accéder à un service est beaucoup trop long. (18)

[706] Point 6 de la déclaration du Conseil des Ministres sur la neutralité du réseau.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

III. Questions posées

A. La gestion du trafic

Lors de l'adoption du Paquet Télécom a eu lieu une consultation publique et l'une des principales questions posées a été celle du blocage et de la limitation du trafic. Le blocage consiste « soit à rendre difficile l'accès à certains services ou sites Internet, soit carrément à en restreindre l'accès ». La limitation est « une technique employée pour gérer le trafic et le décongestionner », et peut être utilisée pour « dégrader (notamment ralentir) un certain type de trafic et ainsi affecter la qualité du contenu ». L'Organe des régulateurs européens des communications électroniques (ci-après « ORECE ») a pointé une situation préoccupante d'après elle : la réduction de la vitesse du partage de fichiers en *peer-to-peer* ou de la lecture vidéo en transit de la part de certains fournisseurs d'accès européens.

Se posent les questions suivantes : peut-on permettre aux opérateurs de réseaux de procéder à des gestions de trafic, ou 'priorisation de trafic' ? Si oui, à quelles conditions ? L'enjeu est en effet de taille : problèmes de concurrence, atteinte aux consommateurs, liberté d'expression, etc.[707]

Comme le souligne la Commission, c'est autour de la gestion du trafic, et de ce qui en constitue une gestion raisonnable, que le débat s'est tourné. Selon elle, « (i)l est largement admis que les opérateurs de réseau doivent adopter certaines méthodes de gestion du trafic pour veiller à l'utilisation efficace de leurs réseaux et que certains services (…) peuvent exiger une gestion spéciale du trafic pour garantir une qualité de service élevée, d'un niveau prédéfini »[708]. Gérer le trafic est donc indispensable, et il existe différentes techniques pour ce faire : la différenciation de paquets, le routage IP et le filtrage.

La différenciation de paquets, ou *deep packet inspection*, permet d'analyser le contenu des données qui transitent et, dès lors, de traiter différemment des catégories de trafic distinctes, que ce soit en fonction de leur contenu, de leur destinataire ou de leur émetteur[709]. Il s'agit plus spécifiquement d' « une technologie de réseau installée (…) pour surveiller quelles applications génèrent un trafic de données. Cette technologie est utilisée pour ralentir ou accélérer des données d'un contenu particulier généré par certaines applications de terminaux, tel que le *peer-to-peer* »[710].

Le routage IP permet aux fournisseurs de services de la société de l'information d'acheminer les paquets par des voies de communication différentes, et cela pour éviter la congestion[711].

Enfin, le filtrage permet à un fournisseur de faire la distinction entre le trafic « sûr » et le trafic « nuisible » et de le bloquer avant qu'il n'atteigne sa destination[712]. Peu importe la méthode choisie

---

[707] M. PIRON, *op. cit.*, p. 71.
[708] Communication de la Commission européenne du 19 mai 2011, *op. cit.*, p. 3.
[709] F. MCKELVEY, "Ends and ways: The algorithmic politics of network neutrality", *Global Media Journal – Canadian edition*, t. III, Ottawa, pp. 53 et 54, disponible sur http://www.gmj.uottawa.ca/1001/v3i1_mckelvey.pdf
[710] http://www.deeppacketinspection.ca/what-is-dpi/ : "*Deep packet inspection is a networking technology installed(…) to monitor what applications are generating datatraffic. This technology is used to delay, or 'throttle', particular data content generated by some computer applications, such as peer-to-peer applications".*
[711] Communication de la Commission européenne du 19 mai 2011, *op. cit*. p. 7.
[712] *Idem*.

pour procéder à une gestion du trafic, il s'agit bien d'un élément nécessaire et important du fonctionnement efficace de l'internet, et il est dès lors tout à fait admis qu'il soit utilisé pour remédier aux problèmes de congestion du trafic et de sécurité. Il a été convenu que des utilisations dans ce contexte sont « totalement légitimes et (ne vont) pas à l'encontre des principes de neutralité d'internet »[713]. Pour compenser ces éventuelles ingérences dans le trafic, il faut prévoir en contrepartie des mesures pour assurer la transparence et la qualité du service (voir article 8 de la directive « cadre »).

Le Sénat hollandais a adopté le 8 mai 2012 la loi sur les télécommunications, qui impose un traitement égalitaire de toutes les communications, et ce quel que soit le contenu, son origine et sa destination, et cela concerne tant l'internet fixe que mobile[714]. La loi autorise une ingérence dans le trafic par les fournisseurs d'accès à internet dans le cas de congestion, de sécurité du réseau, de restriction la transmission à un utilisateur final de communications non-sollicitées (les *spams*), ou pour donner effet à une disposition légale ou à une décision de justice[715], tant que ces mesures servent les intérêts des utilisateurs d'internet[716].

B. La suspension de l'accès à internet

Une des dispositions qui posait problème dans le cadre des discussions sur la réforme du Paquet télécom était le fameux « amendement Bono » qui porte sur les droits et libertés des internautes. Dans sa version initiale, il était prévu qu' « aucune restriction aux droits et libertés fondamentales des utilisateurs finals ne doit être prise sans décision préalable de l'autorité judiciaire en application notamment de l'article 11 de la Charte des droits fondamentaux, sauf en cas de menace à la sécurité publique où la décision judiciaire peut intervenir postérieurement ». Le Parlement en conclut, dans un communiqué de presse, que « l'accès à Internet ne peut pas être restreint sans décision préalable des autorités judiciaires »[717].

Cet amendement prévoit le recours obligatoire à une autorité judiciaire, et l'on peut imaginer le soulèvement engendré en France qui était alors en train de mettre en place un mécanisme de réponse graduée qui serait contrôlé par une autorité administrative. Alors que l'obligation de passer par une procédure préalable devant un juge pour toute suspension d'une connexion internet n'était pas remise en cause, c'était le fait de ne pas pouvoir recourir à une procédure administrative, assurant des sanctions plus efficaces, qui posait problème. Même le Conseil de l'Union européenne s'y est opposé, dans le cadre de la procédure de conciliation lancée après le second vote du Parlement. C'est suite à ces discussions qu'a finalement été adopté l'article 1.3 *bis* de la directive « cadre », inséré par la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre

[713] *Idem*.
[714] Wet van 10 mei 2012 tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, disponible sur https://zoek.officielebekendmakingen.nl
[715] Article 7.4a du Telecommunication Act.
[716] M. OOSTVEEN et F. ZUIDERVEEN BORGESIUS, « Pays-Bas : Modification de la loi relative aux télécommunications », *Iris 2012-7 :1/32*.
[717] « Pas d'accord sur le "paquet Télécom" », Société de l'information, Communiqué de presse, 6 mai 2009, disponible à cette adresse : http://www.europarl.europa.eu/news/expert/infopress_page/058-55086-124-05-19-909-20090505IPR55085-04-05-2009-2009-true/default_fr.htm.

2009 : « Toute mesure susvisée concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques qui serait susceptible de limiter les libertés et droits fondamentaux précités ne peut être instituée que si elle est appropriée, proportionnée et nécessaire dans le cadre d'une société démocratique, et sa mise en œuvre est subordonnée à des garanties procédurales adéquates (…). Les mesures en question ne peuvent être prises que dans le respect du principe de la présomption d'innocence et du droit au respect de la vie privée. Une procédure préalable, équitable et impartiale est garantie (…) ». Les termes « décision judiciaire » ont été remplacés par ceux, beaucoup plus larges, de « procédure préalable ». Les Etats membres peuvent donc prendre des mesures restreignant l'accès d'un utilisateur aux services, applications et leur utilisation via les réseaux de communications électroniques qui seraient susceptibles de limiter les droits fondamentaux[718], mais cela bien encadré par l'obligation de passer par une procédure juste et impartiale, respectant les droits de la défense.

Le Parlement européen considère que l'interruption de l'accès à Internet va à l'encontre « des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif»[719].

C. Internet : un droit fondamental ?

Plusieurs auteurs et membres du Parlement européen considérèrent que l'adoption de l' « amendement Bono » était une reconnaissance de l'accès à Internet en tant que droit fondamental[720]. Dans un communiqué de presse du 26 mars 2009, le Parlement européen expliqua, que « la Charte des droits fondamentaux de l'Union ne mentionne pas directement l'accès à Internet, mais le "droit à la liberté d'expression". Ce droit comprend "la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques, et sans considération de frontières" ».

Dans une recommandation, le Conseil des ministres du Conseil de l'Europe se dit « conscient de la valeur de service public de l'Internet, comprise comme étant le fait pour les personnes de compter de manière significative sur l'Internet comme un outil essentiel pour leurs activités quotidiennes (communication, information, savoir, transactions commerciales, loisirs) et de l'attente légitime qui en découle que les services de l'Internet soient accessibles et abordables financièrement, sécurisés, fiables et continus, et rappelant sur ce point la Recommandation Rec(2007)16 du Comité des

[718] M PIRON, *op.cit*, p. 81.
[719] Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe (2007/2153(INI), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//FR, n° 23 : « engage la Commission et les États membres à reconnaître qu'Internet est une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information, et, par conséquent, à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à Internet ».
[720] La Quadrature du Net, « Amendement 138/46 réadopté, Internet est un droit fondamental en Europe », 6 mai 2009, http://www.laquadrature.net/fr/amendment-138-46-r%C3%A9adopt%C3%A9-Internet-est-un-droit-fondamental-en-Europe

Ministres sur des mesures visant à promouvoir la valeur de service public d'Internet »[721]. Cette recommandation peut être considérée comme une reconnaissance de l'accès à internet comme droit fondamental[722].

L'article 1, 3*bis* de la directive « cadre », en son 1er alinéa, est une reconnaissance de l'internet comme droit fondamental, en tant qu'il est essentiel pour l'éducation et pour l'exercice pratique de la liberté d'expression et l'accès à l'information. L'alinéa 2 prévoit, comme souvent dans les articles ayant trait à la protection d'un droit fondamental, les cas dans lesquels ce droit pourrait être restreint / coupé par une autorité publique : si cela s'avère nécessaire et proportionné, seulement après une procédure juste et impartiale tenant compte du droit pour l'internaute d'être entendu, et un contrôle judiciaire doit être assuré « en temps utile ». Remarquons que les Etats membres peuvent être plus restrictifs par rapport aux possibilités de couper l'accès, l'article 1, 3*bis* établit une harmonisation minimale à ce niveau, et donc être plus protecteurs du droit d'accès à internet.

Il faut analyser cette disposition législative à la lumière de la stratégie numérique de la Commission européenne, qui prévoit dans une communication la « stratégie numérique pour l'Europe » 7 initiatives phares, dont la stratégie numérique pour l'Europe qui a pour objectif pour 2013 un accès garanti pour tous les européens à internet à un haut débit « de base », et pour 2020, un accès pour tous à un très haut débit (30 Mbps ou plus)[723].

Le Parlement considère que la solution de la France pour lutter contre le piratage en ligne, en suspendant la connexion internet des internautes, serait contraire à un internet comme droit fondamental, sans la garantie du passage devant une autorité judiciaire. Selon lui, « si l'accès à Internet était considéré comme un droit fondamental dans l'Union, la France pourrait se trouver en contradiction avec le droit européen[724]. Mais cet amendement n'a en définitive jamais été adopté. Le Conseil Constitutionnel français, dans sa décision du 10 juin 2009, a néanmoins précisé que « considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; […], dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins. »

[721] Comité des Ministres, Recommandation CM/Rec (2007)16 pour promouvoir la valeur de service public de l'Internet, 7 novembre 2007.
[722] C. CALLANAN, M. GERCKE, E. DE MARCO, H. DRIES-ZIEKENHEINER, « Filtrage d'internet (…) », *op. cit.*, p. 205.
[723] Communication de la Commission, « Europe 2020 – Une stratégie pour une croissance intelligente, durable et inclusive », COM(2010) 2020, 3 mars 2010.
[724] Parlement européen, communiqué de presse, 26 mars 2009, « Les droits fondamentaux doivent aussi s'appliquer sur Internet », disponible sur http://www.europarl.europa.eu/news/expert/infopress_page/017-52613-082-03-13-902-20090325IPR52612-23-03-2009-2009-false/default_fr.htm.

§3. Le droit à un procès équitable

De nombreux systèmes proposés (réponse graduée, blocage de sites internet) sont parfois confiés à des **autorités administratives**, sans recours à l'ordre judiciaire. Est-ce légitime au regard du droit à un procès équitable ?

Dans les systèmes proposés, qu'ils soient administratifs ou judiciaires, quelles sont les garanties en termes de **droit à la défense**, **principe du contradictoire** et autres règles de droit à un procès équitable ?

Quels sont enfin les **moyens de défense et de réaction** garantis aux internautes ou aux titulaires de sites web visés par les mesures proposées ? Quels recours leur sont offerts et quelle réparation en cas d'éventuelle erreur ?

Le droit à un procès équitable est consacré par deux textes internationaux, la Convention EDH et le PIDCP. L'article 6, § 1er, CEDH dispose que "toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle (...)". L'article 14, § 1er, PIDCP énonce quant à lui que "toute personne a droit à ce que sa cause soit entendue équitablement et publiquement par un tribunal compétent, indépendant et impartial, établi par la loi, qui décidera soit du bien-fondé de toute accusation en matière pénale dirigée contre elle, soit des contestations sur ses droits et obligations de caractère civil (...)".

L'exigence de l'équité de la procédure implique que chacune des parties puisse soutenir sa cause dans des conditions qui ne la désavantagent pas de manière substantielle par rapport à la partie adverse[725].

Le droit à un procès équitable comprend des questions telles que le droit de se faire entendre dans des conditions équitables, les critères en matière de preuve, la présomption d'innocence, le droit de faire appel, *etc*. Ce sont ces questions qui seront analysées dans la présente partie du rapport.

I. Droits de la défense

A. Le principe du contradictoire

En vertu du principe du contradictoire, chaque partie doit pouvoir être entendue et pouvoir réagir sur les arguments et éléments de preuve avancés par la partie adverse. On considère également que le juge ne peut fonder sa décision sur des éléments qui n'ont pas pu faire l'objet d'un débat

[725] F. GÖLCÜKLÜ, "Le procès équitable et l'administration des preuves dans la jurisprudence de la cour européenne des droits de l'homme", in *Présence de droit public et des droits de l'homme. Mélanges offerts à Jacques Velu*, Bruxelles, Bruylant, 1992, tome 3, p. 1366.

contradictoire.[726] Au stade de l'introduction de la procédure, le principe de la contradiction des débats requiert une convocation en bonne et due forme de la partie défenderesse. En ce qui concerne le déroulement de la procédure proprement dite, l'exigence du contradictoire impose une communication complète et loyale des pièces versées au débat[727]. Lors de sa prise de décision, il est fait interdiction pour le tribunal de se fonder sur des éléments n'ayant pas pu faire l'objet d'un débat contradictoire[728].

Lorsqu'est mis en place un système électronique automatisé de récolte des preuves destinées à fonder une accusation, et cela sans intervention initiale d'un juge, il n'est pas laissé à l'internaute la possibilité de se défendre et de faire valoir ses intérêts. Or, il y a une atteinte au principe du contradictoire s'il n'est prévu de possibilité de recours pour l'internaute que lorsqu'il a déjà été sanctionné.

En matière de procédure de *notice and takedown*, la directive 2000/31 ne prévoit aucun mécanisme curatif permettant aux fournisseurs de contenus, clients de l'hébergeur qui a procédé à leur retrait, de faire restaurer ces contenus, et cette carence a été analysée comme une violation du principe du contradictoire[729]. Une procédure de contre-notification comme cela est prévu aux Etats-Unis permet de pallier cette carence, mais pas complètement. Il faudrait en effet pouvoir inclure le propriétaire du contenu en cause dans la procédure, au stade précédent celui du retrait, et ce dans le respect du contradictoire. Il en va de même lorsqu'il est procédé au blocage ou à l'inaccessibilité d'un site internet.

B. La présomption d'innocence et le renversement de la charge de la preuve

L'article 11 de la DUDH prévoit que « Toute personne accusée d'un acte délictueux est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie au cours d'un procès public où toutes les garanties nécessaires à sa défense lui auront été assurées. » Elle est également reconnue à l'article 14, 2 du PIDCP, à l'article 48 de la Charte des droits fondamentaux de l'Union européenne ainsi qu'à l'article 6 de la Convention EDH. Cette présomption d'innocence implique que c'est à celui qui allègue un fait à le prouver. C'est donc au Ministère public d'établir l'infraction et non au défendeur de devoir prouver son innocence.

En droit civil, l'article 1315 du code civil prévoit que c'est à celui qui réclame l'exécution d'une obligation de la prouver.

Dans un système de réponse graduée, il y a collecte des adresses IP des internautes suspectés de partage ou de téléchargement illégal. Un lien est réalisé entre un acte commis sur un réseau et sa correspondance avec l'appareil qui en est à l'origine, et ce sera alors à l'internaute visé de démontrer qu'il n'est pas à l'origine du fait qui a révélé son adresse IP. Il y a donc sur cette base renversement de la charge de la preuve, preuve qui se rapproche de la simple présomption de responsabilité au vu du risque que la personne à qui l'adresse IP a été attribuée ne soit pas celle qui a effectivement

[726] A. CRUQUENAIRE, « Sources du droit à un procès équitable », *Cahiers du CRID*, n° 21, p. 153.
[727] CEDH, *Feldbrugge c. Pays-Bas*, 23 avr. 1986, § 44.
[728] I. ZAKINE, *op. cit.*, pp. 75-77.
[729] R. HARDOUIN, « La jurisprudence, les textes et la responsabilité des hébergeurs », *RLDI*, 2008/39, n° 1313.

commis l'acte répréhensible. Il n'est pas interdit au législateur d'alléger les règles relatives à la charge de la preuve dans certaines matières, dans un but d'allègement des règles dans des matières où les preuves sont difficiles à rapporter[730]. En Belgique, l'on retrouve ces présomptions en matière d'infractions contraventionnelles[731]. Un exemple intéressant pour notre propos peut être pris en matière de circulation routière : l'article 67*bis* de la loi relative à la police de la circulation routière fait peser une présomption de culpabilité sur le titulaire de la plaque d'immatriculation lorsque le véhicule est immatriculé au nom d'une personne physique et que le conducteur n'est pas identifié sur place. Cette présomption étant réfragable[732], « il suffit de créer un doute raisonnable quant à l'identification du conducteur »[733]. Cet exemple peut être rapproché du cas de la présomption de culpabilité qui pèse sur le titulaire d'une connexion internet.

Selon les cas prévus dans la loi française pour renverser cette présomption de culpabilité, il y a même un risque que cette présomption devienne irréfragable de fait, car il deviendrait impossible pour l'internaute d'apporter la preuve contraire. Nous pensons aux exonérations prévues dans la loi HADOPI, qui ne permettent de s'exonérer de la responsabilité que dans trois cas (voir *supra*), qui sont difficilement invocables par l'internaute accusé. L'internaute aura dans les faits à prouver l'absence de téléchargement illégal à partir de sa connexion internet.

C. Personnalité de la peine pénale

Hors les cas de responsabilité pour le fait d'autrui, on ne peut être condamné que pour ses propres faits.

Dans un mécanisme de réponse graduée avec collecte des adresses IP, nous avons vu que ce n'est pas toujours l'abonné à internet titulaire de l'adresse IP en cause qui est la personne qui a effectivement téléchargé ou partagé illégalement un fichier. Ce principe permettrait donc d'éviter la sanction de la coupure de son accès à internet, s'il n'a pas pu être prouvé que l'abonné est bien l'auteur de l'acte contrefaisant.

En France, la parade a été trouvée en condamnant non pas le téléchargement en tant que tel mais bien le défaut de sécurisation de sa connexion internet.

D. Le prononcé de la sanction par une autorité judiciaire

Pour la Cour EDH, c'est la nature de l'organe investi du pouvoir de sanction qui importe, ce qui la conduit à inclure dans le champ du procès équitable des organes de type administratif au regard de

[730] N. COLETTE-BASECQZ et N. BLAISE, *Manuel de droit pénal général*, Louvain-la-Neuve, Anthemis, 2010, p. 267.
[731] *Ibid.*, p. 268.
[732] Cass. (2e ch.), 11 juin 2002, *Pas.*, 2002, I, p. 350.
[733] N. COLETTE-BASECQZ et N. BLAISE, *op. cit.*, p. 268.

leur droit national dès lors qu'ils statuent sur des accusations en matière pénale »[734]. C'est donc une conception matérielle de la fonction juridictionnelle que la Cour EDH retient.

En France, mais cela a également été le cas en Espagne, il était prévu que ce soit une autorité administrative qui se chargerait des sanctions à prononcer. Il était prévu que la Haute autorité française puisse suspendre, pour une période déterminée, l'accès à internet, dans son ensemble. En Espagne, il était prévu que la Commission de la Propriété intellectuelle, organe administratif, procède elle-même au blocage de sites internet. Dans les deux pays les contestations ont été très fortes à ce sujet, et le passage par un juge a été rendu obligatoire pour respecter les garanties du procès équitable.

Le Conseil constitutionnel français, lorsqu'il a validé la loi HADOPI, a estimé que « c'est à la justice de prononcer une sanction lorsqu'il est établi qu'il y a des téléchargements illégaux », en se basant sur la considération qu' « Internet est une composante de la liberté d'expression et de consommation », et qu' « en droit français c'est la présomption d'innocence qui prime », et conclut que « le rôle de la Haute autorité est d'avertir le « téléchargeur » qu'il a été repéré, mais pas de le sanctionner ». Même si la seconde loi HADOPI prévoit une nouvelle contravention pour « négligence caractérisée » qui permet, si l'abonné, après la seconde recommandation, n'a pas sécurisé son accès internet et a donc laissé faire les téléchargements illégaux, une ordonnance pénale simplifiée qui permet une sanction plus rapide par le juge. Mais il reste dans les mains du juge, et le Conseil constitutionnel l'a rappelé, le pouvoir de décider de la suffisance ou non des éléments de preuves – jugement qui se fera au cas par cas, de refuser le prononcé d'ordonnances pénales en cas d'incertitude, de prendre en compte toutes les circonstances empêchant éventuellement qu'une peine soit applicable, de décider d'appliquer ou non une peine complémentaire et de contrôler les éléments pouvant constituer une « négligence caractérisée »[735]. La Haute autorité sera donc essentiellement un intermédiaire entre les ayants droit – qui sont chargés de lui fournir les adresses IP collectées – et le fournisseur d'accès à internet – qui sera alors chargé de l'identification des internautes et de la suspension de leur accès à internet si cela est décidé par le juge. La Commission européenne avait d'ailleurs interrogé la France sur la manière dont était « justifiée le fait qu'un organe administratif et non un organe judiciaire dispose du pouvoir de décider s'il y aurait violation ou non d'un droit d'auteur ou droit voisin », car en effet, la Haute autorité a pour mission de statuer sur la matérialité d'une contrefaçon[736] : elle analyse les opérations informatiques qui peuvent être qualifiées de reproduction d'une œuvre protégée par le droit d'auteur, recherche si une autorisation a été donnée par son auteur pour une telle utilisation, que cette utilisation n'entre pas dans l'une des exceptions énumérées par la loi[737].

Les mêmes considérations ont eu lieu en Espagne, concernant la procédure de blocage de sites, lors des discussions sur l'adoption de la loi *Sinde*, qui avait pour objet notamment de créer un organe administratif – la Commission de la Propriété intellectuelle – qui aurait été en charge de bloquer ou fermer des sites offrant des contenus illégaux, et cela sur sa simple intervention. Après de nombreuses critiques, l'exécution de ces mesures nécessite l'autorisation d'un juge, ces mesures

[734] J.-F. BRISSON, « Les pouvoirs de sanction des autorités de régulation : les voies d'une juridictionnalisation », *AJDA*, 1999, p. 847.
[735] Conseil constitutionnel, Décision n° 2009-590 DC du 22 octobre 2009.
[736] E. DE MARCO, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », juriscom.net, p. 4.
[737] *Ibidem*, p. 6.

portant atteinte à divers droits fondamentaux[738]. C'est à l'autorité administrative d'introduire les plaintes, une fois saisie par les ayants droit lésés, mais ce sera finalement au juge d'entendre les parties et de décider d'imposer ou non une mesure de blocage de sites.

Il avait été prévu au départ que l'HADOPI puisse obliger les fournisseurs d'accès au filtrage, mais cela a été estimé contraire aux droits fondamentaux, une telle mesure ne pouvant en effet n'être décidée que par le président du tribunal de grande instance. Une disposition de ce type « comporte un risque d'atteinte aux libertés individuelles, au rang desquelles figure la liberté d'expression, dans la mesure où elle donnerait la possibilité à l'HADOPI de demander à un intermédiaire technique de procéder au filtrage de contenus considérés comme portant atteinte aux droits d'auteur. », a estimé la Commission. Tout ce que pourra faire HADOPI, ce sera saisir le président du tribunal de grande instance pour que lui décide d'imposer ou non une mesure de filtrage[739].

Le problème en cas de procédure de *notice and takedown* est qu'il y a un abandon de la procédure à des acteurs privés en ce qui concerne le retrait de contenus illégaux. Or, « dans tout État de droit, seul un juge est en mesure de prononcer l'illégalité d'une situation juridique donnée »[740]. Si l'on décide de confier ce pouvoir à des opérateurs de réseau, cela revient à mettre en place une « justice privée et automatisée », contraire au droit à un procès équitable prévu à l'article 6 de la Convention EDH[741]. Si l'hébergeur est amené à devoir faire le choix entre retirer un contenu notifié et voir sa propre responsabilité mise en jeu en cas d'inaction, il ira naturellement vers la première option, sans se poser plus de questions… Il serait intéressant de prévoir des moyens de défense dans de telles situations.

II. Les moyens de défense garantis

Il est essentiel de prévoir des moyens de défense pour les parties en cause dans les cas où seraient mis en place des mécanismes de blocage de site, ou de notifications et de retrait, le risque dans ce type d'actions étant que des contenus tout à fait légitimes se retrouvent retirés ou rendus inaccessibles.

Lors de la transposition de la directive 2000/31 sur le commerce électronique, certains Etats ont choisi de créer un système de « contre-notification », comme la Lituanie et la Finlande. Le DMCA américain prévoit cette procédure de « contre-notification » depuis longtemps dans son système de *notice and takedown*, en offrant la possibilité de remettre sur le site le contenu qui aurait été bloqué

[738] Speech 09/551 de Viviane Reding, « Regulation in a convergent environment », Barcelone 23 novembre 2011, disponible sur : http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/551&format=HTML&aged=0&language=EN&guiLanguage=en. Viviane Reding avait d'ailleurs sollicité de l'Espagne qu'elle revoie cette approche : "Spanish measures that would allow for the cutting off of internet access without a prior fair and impartial procedure in front of a judge is certain to run into conflict with European law. The case of France has shown that national constitutional law may raise even more immediate barriers to such proposals. I therefore invite the Spanish authorities to consult very closely with the European Commission before heading into a direction which could soon turn out to be a blind alley"

[739] Délibération n°2008-101 du 29 avril 2008 portant avis sur le projet de loi relatif à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

[740] La Quadrature du Net, « Garantir la neutralité du Net », p. 12.

[741] *Idem*.

ou rendu inaccessible[742]. Dans le système américain, il y a d'abord retrait du contenu, sans entendre son propriétaire, et ce n'est qu'après que celui-ci peut demander sa réinsertion, avec les risques que cela pose en matière de liberté d'expression et de droits de la défense.

Pour préserver les prestataires intermédiaires lorsqu'ils procèdent au retrait ou au blocage d'un contenu de la mise en cause de leur responsabilité par le propriétaire dudit contenu, il faudrait qu'un mécanisme d'exonération de responsabilité soit prévu, exonération qui s'opérerait si le prestataire a agi de bonne foi, dans le respect de la loi. Ce critère du respect des règles légales sera à apprécier dans le chef du prestataire, dans des cas où il y aurait erreur lors d'un retrait ou d'un blocage, ou inaction de sa part, ou encore une lenteur dans son action (non-respect de l'exigence de promptitude dans la procédure de notification et de retrait). La loi américaine en matière de *notice and takedown* prévoit une telle exonération de responsabilité. Prévoir des sanctions en cas de notifications abusives permet également de préserver les prestataires intermédiaires. Il faut pouvoir prévenir aussi le risque pour les intermédiaires visés par la directive 2000/31 que leur exonération conditionnelle de responsabilité ne se voit pas remise en cause lorsqu'ils reçoivent une notification et que celle-ci est très laconique ; cela créerait une grave insécurité juridique dans leur chef. Ce bénéfice de l'exonération ne pourrait être perdu que dans le cas où la notification qu'ils reçoivent serait suffisamment complète pour pouvoir fonder une connaissance effective.

Le fait pour un intermédiaire technique de pouvoir procéder automatiquement au retrait d'un contenu, sans devoir apprécier sa licéité ou non, est une garantie importante pour éviter qu'ils ne se transforment en « juges de l'illicite ». Si une analyse de licéité par les hébergeurs reste prévue avant un retrait, ils pourraient se retrouver devant des contenus protégés par le droit d'auteur mais dont il serait difficile pour eux de déterminer l'existence d'exceptions ou de licences. Pour cela, il faudrait leur donner la possibilité de pouvoir corriger leurs erreurs ou de confirmer l'illicéité du contenu litigieux en sollicitant l'aide d'un juge. Cela permettrait de diminuer la pression qui reposerait sur les épaules de l'hébergeur.[743]

Outre la préservation des intérêts des prestataires lors du retrait ou du blocage d'un contenu qui serait parfaitement légitime, il faut également prévoir des moyens de défense garantis pour les propriétaires de ces différents contenus qui auraient été rendus inaccessibles[744]. Le juge doit pouvoir tenir compte également de ces différents intérêts.

[742] Article 512, du Digital Millenium Copyright Act.
[743] E. De Marco, *op. cit.*, p. 15.
[744] Voir *supra*.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

§4. La garantie de la liberté d'entreprise

Toute demande **d'intervention des intermédiaires d'internet** dans la lutte contre le téléchargement ne contrevient-elle pas à la liberté d'entreprise, notamment si elles emportent les contraintes techniques, organisationnelles ou empêchent le développement de certains services ?

L'intervention directe sur le contenu de sites web (blocage du site, cessation de l'hébergement) est-elle aussi susceptible d'avoir un effet sur la liberté d'entreprise si le contenu illicite visé n'est pas l'activité principale du site ? Quels garanties et moyens de défense doivent-ils être prévus ?

La liberté d'entreprise est reconnue par l'article 16 de la Charte des droits fondamentaux qui dispose que « la liberté d'entreprise est reconnue conformément au droit communautaire et aux législations et pratiques nationales ».

Dans son arrêt *Scarlet c. Sabam*, la Cour de justice de l'Union européenne invoque cette liberté fondamentale qui doit être prise en compte dans la mise en place de mesures de lutte contre la contrefaçon et rappelle que « dans des circonstances telles que celles de l'affaire au principal, 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 opérateurs tels que les FAI en vertu de l'article 16 de la charte »[745].

L'injonction de mise en place de systèmes de filtrage a été considérée, dans cette affaire, comme entrainant « une atteinte caractérisée à la liberté d'entreprise du FAI concerné puisqu'elle l'obligerait à mettre en place un système informatique complexe, coûteux, permanent et à ses seuls frais »[746]. Les juges communautaires en ont déduit que l'équilibre entre protection des droits intellectuels et liberté d'entreprise était rompu[747].

En conséquence, toute mesure imposée aux FAI dans la lutte contre la contrefaçon au droit d'auteur sur internet devra être mesurée à l'aune de ses effets quant à cette liberté fondamentale des opérateurs économiques. La Cour de justice a déjà stipulé que le coût ou la complexité des mesures, ainsi que leur caractère durable, seront des critères à prendre en compte. Si la décision concerne des mesures de filtrage, il n'est pas exclu qu'une telle analyse doive également être faite pour d'autres implications des FAI, que ce soit sur injonction de cessation ou dans des mécanismes de réponse graduée. Dans tous ces cas, il faudra veiller à l'impact de ces mesures pour la liberté économique d'entreprendre des intermédiaires concernés. Par exemple, le coût en termes de ressources techniques ou humaines qu'impliquerait l'intervention des FAI dans les envois de courriers aux internautes dans un système de type HADOPI ne saurait être tel que leur liberté d'entreprendre en serait affectée de manière significative.

[745] Arrêt *Scarlet*, § 46.
[746] Arrêt *Scarlet*, § 48. La même conclusion vaut pour les prestataires de services d'hébegement, voir C.J.U.E, 16 février 2012, *Sabam c. Netlog*, C-360/10, §47.
[747] Voir sur ce point, D. GOBERT et J. JOURET, « L'arrêt *Scarlet contre Sabam* : la consécration d'un juste équilibre du rôle respectif de chaque acteur dans la lutte contre les échanges illicites d'œuvres protégées sur Internet », *op. cit.*, pp. 48-49.

La liberté d'entreprise pourrait également être atteinte par des mesures trop larges de suspension ou de retrait d'une connexion à Internet, dans le cadre de systèmes de réponse graduée. Les moyens de communication étant indispensables à l'heure actuelle à l'exercice d'une activité professionnelle ou économique, empêcher une personne de bénéficier d'un accès à Internet pourrait être considéré comme ayant un effet disproportionné sur la liberté d'entreprendre de cette personne, soit directement soit par le biais de l'atteinte à la liberté d'accéder et de recevoir des informations, dont l'exercice de la liberté d'entreprise dépend.

Chapitre 3. Analyse des options envisageables pour lutter contre les atteintes au droit d'auteur sur Internet

Ce dernier chapitre a pour objectif, sur base des considérations juridiques développées au chapitre précédent, d'analyser les trois options principales de lutte contre les téléchargements non autorisés d'œuvres sur Internet. Cette analyse se fera en considérant les obstacles et difficultés juridiques soulevées par chaque option, ainsi que leur coût en termes d'opportunité ou de proportionnalité.

§1. Autorisation des échanges

I. Modalités pratiques

Un système d'autorisation des échanges peut revêtir deux formes principales :

- la licence non volontaire, soit licence légale ou licence obligatoire
- l'autorisation par les ayants droit eux-mêmes par la voie d'une gestion collective de leurs droits

L'intervention législative dans ces deux modèles diffère :

- La licence non volontaire nécessitera l'introduction dans la loi sur le droit d'auteur d'une nouvelle exception autorisant les échanges d'œuvres sur Internet, ainsi que la mise en place d'un régime de droit à rémunération pour ces utilisations.
- Aucune intervention législative n'est *a priori* requise pour l'autorisation de ces actes par la gestion collective qui relève de l'exercice du droit exclusif des titulaires de droit d'auteur et de droits voisins, mais celle-ci peut être facilitée par l'imposition, par la loi, que cette gestion collective se réalise dans un modèle de gestion collective obligatoire ou de licence collective étendue.

Certaines décisions quant aux modalités de ces divers mécanismes sont communes à l'ensemble de ceux-ci :

- quant au ***caractère optionnel de l'autorisation pour les internautes*** : il peut être décidé que tous les usagers bénéficiant d'une connexion internet accomplissent potentiellement des actes d'échange ou de téléchargement d'œuvres et à ce titre, contribuent à la rémunération des ayants droit perçue sur le coût de leur abonnement à Internet. Cette logique de « rough justice » est normalement applicable en matière de licence légale[748], mais le législateur pourrait considérer que les utilisateurs qui ne téléchargent pas d'œuvres ne soient pas soumis à cette redevance. Cela peut concerner les abonnements professionnels à Internet mais également les utilisateurs privés qui déclareraient ne pas procéder à de tels actes d'utilisation. Dans ce dernier cas, un mécanisme de contrôle doit pouvoir être mis en place,

[748] Et est admise par la CJUE, dans sa décision *Padawan*, voir C.J.U.E., 21 octobre 2010, C-467/10.

ce qui pose de nouvelles questions (en matière de vie privée, de sanctions, etc…). La question se pose également pour les autorisations accordées par la gestion collective. Les FAI peuvent vouloir réserver cette autorisation à leurs seuls abonnés qui souhaitent en bénéficier, ce qui entrainera pour ces premiers un coût de gestion supplémentaire, et pour les sociétés de gestion collective un coût en terme de contrôle. Le caractère optionnel du système sera plus aisé à gérer si les FAI ne sont pas les preneurs de la licence accordée par les ayants droit mais se limitent à offrir ce contrat à leurs abonnés.

- Quant à ***l'étendue des actes visés*** : le législateur devra indiquer précisément quels actes d'utilisation des œuvres et prestations protégées sont visés par une licence légale (upload/download, échanges commerciaux/non commerciaux, …). Dans les modèles basés sur la gestion collective, seuls les ayants droit ont le pouvoir de déterminer les actes qu'ils entendent autoriser. Toutefois, l'imposition d'une gestion collective obligatoire devra préciser quels actes d'exploitation des œuvres entrent dans le mandat de la gestion collective obligatoire. Une solution de licence collective étendue devra plus encore déterminer les actes autorisés par une société de gestion collective représentative des ayants droit concernés, qui seront étendus par l'effet de la loi aux titulaires de droit non représentés.
- Quant à la ***répartition des sommes perçues*** : dans les modèles basés sur la gestion collective, cette répartition est du ressort des sociétés de gestion collective, mais le législateur peut intervenir pour garantir que cette répartition se réalisera sur base d'études des flux d'œuvres réellement téléchargées. Cette intervention sera nécessaire dans un modèle de licence légale.

D'autres modalités sont spécifiques au régime de licence non-volontaire :

- quant à ***l'étendue des actes visés*** : le législateur devra préciser les limites de l'autorisation accordée par la nouvelle exception. Afin de ne pas être radicalement contraire au test des trois étapes, seuls les actes d'accès aux œuvres et d'échanges non commerciaux pourraient faire l'objet de la licence légale. Il pourrait également être décidé que seul l'acte de téléchargement est couvert par l'exception, mais cela laisserait les systèmes *peer-to-peer* dans une situation ambiguë où une partie des échanges continue à relever de la contrefaçon, alors que son pendant devient légitime. Une clarification pourrait être faite sur l'éventuelle application de la copie privée (et de son régime de compensation) aux actes de simple téléchargement d'œuvres à des fins privées, particulièrement en précisant si la source licite est une condition au bénéfice de la copie privée en droit belge. Dans l'affirmative, cette condition devrait être introduite dans la loi sous la forme d'une notion de « source manifestement licite ».

- quant à ***l'assiette et au taux de la perception de la compensation*** prévue pour les ayants droit : la plupart des modèles proposés de licence globale perçoivent une compensation à destination des ayants droit sur les abonnements Internet. Le taux de la perception fait l'objet de nombreuses propositions qui visent généralement un maximum de 10 euros par mois. La détermination de ce montant n'est pas aisée, car si l'on opte pour la licence légale, il

doit être suffisant pour rémunérer les ayants droit et pour ne pas nuire aux offres légales, tout en ne constituant pas un montant qui viendrait augmenter de manière excessive le coût de l'accès à Internet (surtout pour les abonnés ne procédant pas à de tels téléchargements mais inclus dans le régime de mutualisation de la licence légale).

II. Questions juridiques

A. La voie de la licence légale ou non volontaire

1. Légitimité d'une exception au droit d'auteur

L'obstacle principal à l'autorisation des échanges d'œuvres sur les réseaux *peer-to-peer* est l'admissibilité de l'introduction d'une nouvelle exception dans la loi belge pour couvrir cette hypothèse. L'opinion majoritaire relève qu'une licence légale couvrant les échanges non-commerciaux en *peer-to-peer* serait manifestement contraire au test des trois étapes, tel qu'il a été interprété par les législateurs internationaux et la jurisprudence.

En outre, le législateur belge ne peut prévoir une hypothèse d'exception ou de limitation au droit d'auteur qui ne soit pas prévue par la directive 2001/29 sur le droit d'auteur dans la société de l'information.

2. Implication des FAI

Dans le modèle de licence légale, l'implication des FAI sous la forme de la perception dans leur chef d'une rémunération sur le coût des abonnements internet est imposée par le législateur et est légitimée par la difficulté pratique de prélever cette rémunération auprès des internautes, réels bénéficiaires de l'exception et auteurs du préjudice des ayants droit que cette rémunération vise à compenser. Un tel système de compensation indirect a été validé par la Cour de justice européenne en matière de copie privée.

B. La voie de la gestion collective

L'intervention du législateur dans la gestion collective se justifie par la nécessité que l'autorisation donnée aux internautes de procéder à des échanges non commerciaux couvre un répertoire le plus large possible, sous peine de rendre cette autorisation peu attractive pour ces derniers. Ainsi un mécanisme de gestion collective obligatoire ou de licence collective étendue permet d'inclure dans la gestion collective un répertoire le plus large possible. Certains obstacles juridiques subsistent néanmoins.

1. Conformité aux textes législatifs

Les mécanismes de gestion collective obligatoire ou de licence collective étendue ne paraissent pas contraires aux textes internationaux ou européens en vigueur. S'agissant de la satisfaction au test des trois étapes, le fait que les licences soient issues de société de gestion collective qui agissent dans l'exercice du droit exclusif de leurs membres permet sans aucun doute de remplir les différentes conditions du test et principalement, l'absence d'atteinte à l'exploitation normale des œuvres et l'absence de préjudice injustifié aux intérêts des auteurs.

Il faut toutefois souligner que le mécanisme de licence collective étendue reste étranger à notre tradition juridique de droit d'auteur et que son introduction méritera un examen plus approfondi.

2. Globalité de la licence

En dépit de la gestion collective obligatoire ou la licence collective étendue, le choix d'autoriser ou non les échanges reste du ressort des ayants droit. Une licence ne sera globale que si les différentes catégories de titulaires de droit, auteurs, producteurs, artistes-interprètes, par le biais de leur société de gestion collective, acceptent d'octroyer cette autorisation. En pratique, cela paraît peu probable. En outre, seule une autorisation portant sur un répertoire mondial est susceptible de rencontrer l'adhésion des internautes. Or les sociétés de gestion collective belges ne sont pas mandatées, soit explicitement, soit par le biais d'accords de représentation réciproque, pour ce type d'exploitation des œuvres.

Seule une licence collective étendue pourrait valoir pour des auteurs étrangers mais une question subsiste sur la nécessité que la société de gestion collective jugée représentative de ces auteurs, doive démontrer qu'elle représente une part significative d'auteurs nationaux ou également d'auteurs étrangers pour lesquels elle a autorisé les échanges non commerciaux sur Internet. Dans cette deuxième hypothèse, la question de la légitimité de cette société à engager son répertoire étranger dans ce type de négociation subsiste.

3. Implication des FAI

Tout système d'autorisation des échanges *peer-to-peer* par une licence globale prévoit de prélever une rémunération sur les abonnements Internet ce qui implique la coopération des fournisseurs d'accès internet auprès de qui ce montant sera perçu. Si cette implication sera imposée par le législateur dans un système de licence légale, elle est moins évidente dans une autorisation résultant de la gestion collective. Les FAI n'étant pas responsables des actes de reproduction et de communication des œuvres, ils n'ont aucun motif à contracter ce contrat de licence auprès des intermédiaires mais ne peuvent être concernés que sur base volontaire afin d'offrir cette licence à leurs abonnés. Cette incertitude quant à l'intervention contractuelle des FAI rend plus incertaine une autorisation des échanges d'œuvres en *peer-to-peer* par les ayants droit.

Une alternative parfois invoquée est de mettre à contribution certains acteurs d'Internet qui bénéficient indirectement des contenus mis illicitement sur Internet, par le biais d'une mesure fiscale ou parafiscale.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

III. Questions d'opportunité

A. Effet sur les offres légales

Autoriser les échanges d'œuvres en *peer-to-peer* ou par tout autre moyen technique, même à des fins commerciales et contre rémunération, aura un impact sur les offres légales. Il ne faut sans doute pas en conclure que l'instauration d'une licence globale, que ce soit par la voie d'une exception ou de la gestion collective, viendra remplacer l'offre légale, celle-ci présentant des avantages en termes de qualité ou de contenus additionnels ou exclusifs qui restent recherchés par les internautes. En outre, il n'est pas à exclure qu'une licence globale puisse avoir des répercussions positives sur les offres légales, les internautes complétant leurs échanges par des acquisitions sur les plateformes commerciales de téléchargement. Afin de soutenir les offres légales, des systèmes de bons ou de réductions sur le coût de la licence globale pourraient être offerts aux internautes ayant acquis une certaine quantité de contenus sur les plateformes commerciales.

Une étude économique analysant les effets d'une éventuelle autorisation des échanges d'œuvres devrait pouvoir quantifier et mesurer ces effets.

B. Dimension pédagogique

La licence globale, du moins lorsqu'elle prend place dans une licence légale, transmet un message d'accessibilité de la création à un moindre coût, message qu'il faut encadrer avec soin pour éviter que les œuvres artistiques soient perçues comme un contenu accessible au rabais. Certes, la licence légale a le mérite de fixer un coût à la création, à l'opposé des téléchargements illicites d'œuvres qui ne rapportent rien aux ayants droit, et de battre ainsi en brèche l'impression de gratuité du contenu créatif. Mais elle pourrait prendre le relais, surtout auprès des jeunes générations, d'une perception de la création comme d'un simple flux de contenus accessible comme tout autre service, ce qui mettrait à mal l'idée même du droit exclusif.

§2. Mesures de neutralisation des contenus illicites mis à disposition

I. Modalités pratiques

Tarir ou empêcher la diffusion et la mise à disposition d'œuvres sans l'autorisation des ayants droit peut reposer sur des actions diverses et complémentaires à l'encontre de différents acteurs. On peut regrouper ces prestataires de services auprès desquels une action peut être entreprise en cinq catégories, les modes d'interventions différant pour chacune d'entre elles :

Acteur visé	Type de mesure sollicitée
Fournisseurs d'accès Internet	mesures de blocage mesures de filtrage demande d'information
Hébergeurs (incl. *cloud computing*, réseaux sociaux, plateformes type YouTube, …)	mesures de notification et de retrait mesures de filtrage demande d'information
DNS.be	mesures de blocage d'un nom de domaine demande d'information
Moteurs de recherche	déréférencement d'un site
Services de paiement	suspension des paiements à un site contrefaisant demande d'information sur titulaires des comptes saisie des fonds

Plusieurs scénarios sont envisageables. Le premier consiste à ce que les demandes formulées à destination de ces acteurs émanent directement des titulaires de droit, que ce soit lors d'une action en justice (cessation ou action en dommages et intérêts), préalablement à celle-ci ou de manière indépendante. C'est la solution qui prévaut à l'heure actuelle, bien que l'ensemble des mesures citées ci-dessus ne soit pas accessible aux ayants droit dans tous les cas.

Certaines mesures sont en effet réservées aux autorités de recherche des infractions ou au juge dans une action en cessation ou en dommages et intérêts.

Une alternative serait de confier l'initiative de certaines mesures prises en amont des téléchargements à une autorité administrative, travaillant de concert avec les autorités judiciaires, en complément des efforts individuels des ayants droit. Une telle autorité, que l'on retrouve dans le système espagnol ou norvégien, centraliserait les demandes des ayants droit, établirait des listes de sites dont le blocage serait désirable ou interviendrait d'initiative auprès des intermédiaires.

L'analyse qui suit, organisée par type d'intermédiaires, envisagera les deux options, non exclusives l'une de l'autre, examinant d'une part les possibilités de renforcement des moyens mis à la disposition des ayants droit et suggérant d'autre part les avantages possibles d'un recours administratif centralisé.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

II. Questions juridiques

A. Questions transversales de responsabilité des intermédiaires

1. Obligations de collaboration et de surveillance temporaire

Si les intermédiaires bénéficient pour certaines des fonctions qu'ils assurent (fourniture d'un accès internet et transport des informations, hébergement, *caching*) d'un régime d'exonération conditionnelle de responsabilité, ils peuvent être sollicités par les autorités pour leur communiquer les informations dont ils disposeraient sur des actes illicites commis à travers leurs services ou sur leurs auteurs, pour surveiller de manière limitée ce qui se passe sur les réseaux. Ils sont aussi obligés de signaler aux autorités judiciaires tout acte illicite dont ils auraient connaissance.

Il est à noter que ces obligations ne peuvent être fournies qu'aux autorités judiciaires et administratives. Elles ne sont donc d'aucune utilité pour les ayants droit souhaitant disposer d'informations dans le cadre d'une action civile pour lutter contre des contrefaçons commises sur Internet. Ils peuvent toutefois bénéficier du droit d'obtenir des informations prévu par l'article 86*ter,* §3 de la LDA qui peut être actionné dans le cadre d'une action portée devant le juge pour une atteinte au droit d'auteur ou aux droits voisins.

2. Droit d'information

Le droit d'information permet d'enjoindre aux intermédiaires (la loi parle de personne qui a été trouvée en train de fournir, à l'échelle commerciale, des services utilisés dans des activités contrefaisantes) de fournir les informations utiles pour entamer des poursuites. A priori, cette notion englobe de nombreux acteurs de l'Internet dont les services (de communication, d'hébergement, de paiement, etc…) sont utilisés par des sites mettant des œuvres à disposition du public en toute illégalité.

L'article 86*ter*, §3 de la LDA autorise la communication des informations et données d'identification des internautes à la partie qui a introduit l'action dès lors qu'une atteinte au droit d'auteur a été constatée par un juge. La Cour de justice a eu l'occasion d'apprécier la loi suédoise de transposition de l'article 8 de la directive 2004/48 et a pu décider qu'une telle disposition était considérée comme susceptible d'assurer un juste équilibre entre la protection du droit de propriété intellectuelle et la protection des données à caractère personnel sous réserve du respect de certaines conditions. Elle accepte la légitimité de cette loi, considérant que les garanties encadrant ce transfert, et notamment le fait que le juge dispose d'un pouvoir d'appréciation quant aux différents intérêts en présence[749], satisfont à la condition de proportionnalité. La Cour accepte la légitimité d'un transfert des données personnelles aux ayants droit (ce qui est prévu dans la loi belge), pour autant que le juge conserve un pouvoir d'appréciation au cas par cas.

Cet article ne résout pas la problématique de la collecte des adresses IP avant toute introduction d'une action judiciaire, car il est nécessaire que l'atteinte au droit d'auteur soit préalablement constatée par un juge. En effet, les adresses IP constituent des données à caractère personnel au

[749] Plus précisément la loi requiert l'exigence d'indices réels d'atteinte à un droit de propriété intellectuelle, la démonstration que les informations demandées sont susceptibles de faciliter l'enquête et que les raisons motivant cette injonction sont d'un intérêt supérieur aux inconvénients pour le destinataire.

sens de l'article 2, point a), de la directive 95/46 sur le traitement des données à caractère personnel. Une adaptation de la loi belge pour faciliter la collecte des adresses IP par les ayants droit, les FAI eux-mêmes ou une instance administrative serait opportune.

3. *Action en cessation à l'encontre des intermédiaires*

La directive 2001/29 sur le droit d'auteur dans la société de l'information ainsi que la directive 2004/48 sur la mise en œuvre des droits de propriété intellectuelle imposent qu'une action en cessation soit possible contre les intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou aux droits voisins. Cette obligation a été transposée aux articles 86*ter*, §1 et 87 de la LDA. Nous reviendrons sur les questions spécifiques que pose cette action en cessation selon les intermédiaires visés.

La notion d'intermédiaires visés par ces textes est très large et est susceptible de concerner tout prestataire de services utilisés pour héberger, diffuser, référencer un site comprenant des atteintes au droit d'auteur. Les prestataires de paiement peuvent également être compris dans cette définition. Quant au type de mesures qui peuvent être sollicitées par cette voie judiciaire, ce sont tout type de mesures jugées utiles par le juge pour faire cesser l'atteinte (positives ou négatives, préventives, …), sous la seule limite de la proportionnalité imposée par la Cour de justice dans l'arrêt *Scarlet*, qui oblige à tenir compte de l'effet des mesures sur la protection de la vie privée et les autres libertés fondamentales, exercice que nous ferons dans l'analyse des mesures qui pourraient être imposées à chaque type d'intermédiaires.

4. *Compétence territoriale*

Les mesures envisagées ici peuvent être introduites contre des intermédiaires belges. Ce sera le cas de toute action contre des fournisseurs d'accès internet et contre DNS.be. La question est plus difficile pour des injonctions que les ayants droit voudraient imposer à des moteurs de recherche ou des hébergeurs dont le siège social serait à l'étranger. Ce sera souvent le cas pour des services tels que Google, YouTube, Facebook ou autres réseaux sociaux, ou des services de *cloud computing*. Le juge de cessation et le juge du fond auquel une injonction de cessation serait demandée ne seront compétents qu'en vertu des règles de droit international privé. Peu importe que les faits de contrefaçon soient localisés à l'étranger, mais il faudra sans doute qu'une connexion quelconque avec le territoire belge soit établie pour obtenir une injonction de cessation devant les juridictions belges.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

B. Actions contre les hébergeurs

1. Notification et retrait des contenus

a. Questions relatives à la procédure de notification et retrait

Dans la mesure où l'exonération de responsabilité des hébergeurs est conditionnée à leur réaction rapide en cas de connaissance d'atteinte au droit d'auteur ou aux droits voisins[750], la directive sur le commerce électronique encourage la conclusion d'accords entre les parties intervenantes pour organiser des procédures de notification et de retrait des contenus litigieux. En Belgique, aucun accord-cadre ou législation n'organise de telles procédures de *notice and take down* qui varient selon les intermédiaires sollicités. Les questions qui résultent de ce défaut d'une procédure standardisée sont notamment :

- l'incertitude pour l'ayant droit quant à la procédure à suivre pour notifier une atteinte à ses droits à un intermédiaire ;
- l'absence de réglementation concernant l'auteur d'une notification, sa forme, son contenu ;
- l'incertitude quant à la prise en considération de sa demande ;
- l'absence de définition du critère de promptitude ;
- la possibilité de demandes abusives d'ayants droit qui seraient suivies d'effet par l'intermédiaire, sans plus d'examen, de crainte de voir sa responsabilité engagée ;
- l'absence de recours pour l'auteur du contenu ou du site web dont le contenu est retiré ;
- l'incertitude quant aux recours envisageables pour l'ayant droit si le contenu est remis en ligne, ainsi que les limites de l'intervention de l'hébergeur face à de telles *notice and stay down*.

Eclaircir l'étendue et la forme des procédures de notifications serait nécessaire en droit belge. Les questions suivantes devraient être réglées :

- l'auteur, la forme, les mentions requises de toute notification ;
- les critères permettant de définir la promptitude de la réaction requise de l'hébergeur ;
- l'existence d'un recours pour l'auteur du contenu retiré, à des fins de protection de la liberté d'expression;
- un principe d'absence de responsabilité des intermédiaires pour tout contenu retiré pour autant qu'ils agissent conformément à la loi ;
- l'étendue de l'obligation des hébergeurs de veiller à ce que le contenu retiré ne réapparaisse pas, dans les limites du principe d'interdiction d'une surveillance généralisée ;
- les éventuelles sanctions pour les notifications abusives émanant des ayants droit.

Une discussion est en cours à l'échelon européen pour définir des critères communs en matière de procédures de notification et de retrait et une consultation des parties intéressées a été lancée. Toute intervention législative belge sur ce point devra en tenir compte.

[750] Le niveau de connaissance n'est pas le même selon que l'on se trouve au pénal ou au civil.

b. Impact sur les droits fondamentaux

L'absence de réglementation des procédures de *notice and take down* peut avoir deux conséquences en matière de droits fondamentaux. La première concerne la liberté d'expression et d'accès à l'information qui subit une restriction lors des retraits de contenus d'Internet. A défaut d'un encadrement légal, les hébergeurs réagissent aux demandes qui leur sont adressées par les titulaires de droit de manière à éviter toute mise en œuvre de leur responsabilité. Aucun recours n'est prévu pour les auteurs des contenus, opinions ou sites faisant l'objet de la mesure de retrait et leurs intérêts ne sont pas pris en compte, ce qui peut légitimement poser des questions en terme de proportionnalité des pratiques de notification et de retrait. L'impact en termes de liberté d'expression se double d'une carence sur le plan du droit à un procès équitable, qui implique le principe du contradictoire et le respect du droit à la défense, l'auteur du contenu n'ayant aucun moyen de faire valoir sa position quant à la légitimité éventuelle du contenu retiré du web.

Tout encadrement légal de ces procédures devrait envisager des voies de recours pour les auteurs des contenus retirés et une éventuelle obligation de remettre le contenu en ligne si la légitimité de celui-ci est démontrée.

Un nombre trop important de notifications, non encadrées légalement, est aussi susceptible d'avoir un impact en termes de liberté d'entreprise des hébergeurs, pour lesquels la mise en place de mécanismes de réponse à ces notifications constitue une charge. La Cour de justice a reconnu une atteinte possible à cette liberté dans les cas d'un filtrage généralisé. Une conclusion similaire n'est pas exclue en cas d'un nombre excessif de notifications, risque qui peut être accru si les formes et la précision de celles-ci ne répondent à aucun cadre précis.

c. Intervention d'une autorité administrative

La difficulté des procédures de notification et de retrait en terme d'impact sur la liberté d'expression et le droit à un procès équitable est que le prestataire d'un service d'hébergement se trouve pris en tenaille entre les demandes des ayants droit et les intérêts légitimes des auteurs de contenus retirés. Pour éviter sa responsabilité, il a intérêt à accéder aux demandes des premiers, sans tenir compte des protestations des seconds, particulièrement si la loi lui assure une absence de responsabilité pour les décisions prises suite à une notification.

Si un encadrement plus précis de ces procédures ouvre un espace de réclamation pour les auteurs des contenus soustraits du réseau en permettant à ceux-ci de se plaindre auprès des hébergeurs postérieurement au retrait effectué, les hébergeurs seront les seuls juges de la légitimité du contenu concerné. La complexité des règles de droit d'auteur quant à la légitimité d'une reproduction ou mise à disposition d'une œuvre (définition de la durée de protection, du titulaire des droits, des droits enfreints, du bénéfice d'une exception, …) rend encore plus hasardeux le rôle qui serait dévolu aux hébergeurs en cas de procédure dite de *notice and put-back*. Confier cet exercice à un juge rendra en revanche le recours moins accessible et effectif pour les internautes.

Une autre solution, à l'instar de la loi américaine, est d'imposer à l'hébergeur en cas de plainte du propriétaire du site retiré, de remettre le contenu en ligne ; si l'ayant droit réagit et précise qu'il intente une action en justice contre l'auteur du contenu, l'intermédiaire doit à nouveau retirer le contenu dans l'attente d'une décision judiciaire. L'hébergeur n'a dans ce modèle aucune obligation d'évaluer la licéité du contenu.

Une alternative serait de confier à une autorité administrative le pouvoir d'évaluer les réactions des auteurs de contenus qui ont fait l'objet d'un retrait d'internet, dans le respect de leurs droits de la défense et de leur droit à une libre expression. Il ne nous paraît pas opportun de charger cette autorité de traiter des notifications adressées par les ayants droit, mais uniquement de la faire intervenir comme instance de recours pour les contre-notifications des propriétaires de contenus retirés. Cette autorité devra appliquer les principes de procès équitable, mais un recours contre les décisions qu'elle prendrait devrait pouvoir être intenté, que ce soit par les ayants droit ou par les internautes, devant les tribunaux ordinaires.

2. *Mesures de filtrage*

Un filtrage généralisé des contenus hébergés sur un site, une plateforme de type YouTube ou un réseau social, ne pourrait être imposé conformément à l'interdiction d'une surveillance généralisée prévue à l'article 21, § 1er, alinéa 1 de la loi du 11 mars 2003 sur la société de l'information. De plus, la Cour de justice a décidé, dans l'affaire *Netlog*, qu'un tel filtrage ne pouvait être admis en raison des atteintes à la liberté d'expression, à la liberté d'entreprise et à la protection des données personnelles potentiellement englobées dans la surveillance des contenus hébergés que le filtrage induit. Un filtrage limité à certains contenus et proprement délimité, comme cela est prévu par l'article 21, § 1er, alinéa 2 de la loi du 11 mars 2003 sur la société de l'information, est toutefois envisageable s'il respecte les exigences de proportionnalité mises en avant par la juridiction européenne.

3. *Obligation de communiquer des informations*

Aucune spécificité par rapport aux questions générales relevées *supra* n'est à relever sur ce point quant aux hébergeurs.

C. Action contre les fournisseurs d'accès à internet

1. *Mesure de blocage*

Dans de nombreux pays ainsi qu'en Belgique, les juges ont accepté d'enjoindre les FAI de bloquer l'accès à des sites internet mettant à disposition des œuvres protégées sur base des noms de domaine ou des adresses IP fournis par les ayants droit. Un blocage sur base des adresses IP a parfois été considéré comme pouvant s'étendre à des sites légitimes partageant la même adresse IP ; dans d'autres instances, notamment devant la cour d'appel d'Anvers, ce risque a conduit le juge à préférer un blocage sur base du nom de domaine.

Le blocage par noms de domaine comporte pourtant le même risque, des contenus illicites pouvant être inclus dans le même nom de domaine que les contrefaçons et leur accès être excessivement obéré par des mesures de blocage visant les atteintes au droit d'auteur. Afin de conserver une certaine proportionnalité, le juge devrait pouvoir considérer la part des activités illégitimes dans un site lié à un nom de domaine déterminé et n'admettre de blocage que si cette part est significative.

Un ordre de cessation obtenu au terme d'une procédure contre certains intermédiaires ne peut normalement être étendu à des FAI non parties à la cause, sans qu'une nouvelle instance soit introduite, ce qui peut diminuer l'effectivité de l'injonction prononcée. Une première décision obtenue pourrait toutefois être prise en compte dans la deuxième instance par le juge de cessation pour évaluer la légitimité de la demande.

Dans l'état actuel du droit, il n'est pas certain que l'on puisse étendre un ordre de cessation obtenu à l'encontre de sites hébergés sur d'autres noms de domaine ou d'adresses IP que celles définies par l'ordre de cessation. Une clarification législative serait sans doute utile pour permettre une certaine souplesse tout en l'encadrant par une définition des critères permettant de déterminer les sites dont le blocage pourrait être demandé ultérieurement sur base du même ordre de cessation, une responsabilité des ayants droit en cas d'élargissement abusif de l'objet des mesures de blocage et un recours possible des FAI sollicités devant le juge de cessation. Une solution intermédiaire serait de prévoir la possibilité d'une nouvelle demande des ayants droit devant le juge des cessations pour une extension à d'autres adresses IP ou noms de domaine, dans le cadre d'une procédure plus rapide, par exemple sur base d'une requête unilatérale, sans que les FAI soient entendus.

a. Impact sur les droits fondamentaux

Une injonction de bloquer l'accès à un site illicite n'a en principe aucun impact en matière de protection des données personnelles. En revanche, la liberté d'expression de propriétaires de sites ou de contenus légitimes soit bloqués par erreur, soit absorbés dans le blocage d'un ensemble plus vaste comprenant des contrefaçons, peut être restreinte de manière substantielle, ainsi que, par répercussion, la liberté d'entreprise si les contenus bloqués relèvent de l'exercice d'une activité professionnelle. Les auteurs des contenus bloqués, que ce soit par erreur ou par absorption, n'étant pas présents dans l'instance en cessation, leur droit de défense et leur droit à un procès équitable sont pareillement affectés.

Cet effet indésirable des demandes de blocage d'accès devrait pouvoir être évité par l'intervention du juge de cessation qui doit pondérer les intérêts en présence et assurer que la demande est légitime et proportionnée. Il ne devrait accéder à la demande que si le site visé comprend une part significative de contenus illicites et garder un pouvoir d'appréciation sur la réalité de l'atteinte. Les moyens de recours des auteurs des sites bloqués sont en effet difficiles à mettre en œuvre dans le cadre d'une action en cessation puisque l'instance est clôturée au moment du blocage du site et de ses effets.

b. Intervention d'une autorité administrative

Certaines des difficultés évoquées dans le cadre des demandes de blocage de site pourraient être atténuées par le recours à une autorité administrative. Celle-ci pourrait être chargée de l'établissement d'une liste évolutive des sites à bloquer et une imposition de cette liste à tous les FAI, parant ainsi à la limitation des injonctions en cessation quant aux destinataires et aux adresses de sites à bloquer.

Les auteurs de contenus auquel l'accès se verrait bloqué, soit par erreur, soit par absorption, pourraient intenter un recours devant cet organisme, garant d'un équilibre entre les droits intellectuels et les droits fondamentaux à la liberté d'expression et à un procès équitable.

2. *Mesure de filtrage*

Un filtrage généralisé des contenus échangés par les internautes ne pourrait être imposé aux fournisseurs d'accès internet conformément à l'interdiction d'une surveillance généralisée prévue à l'article 21, § 1er, alinéa 1 de la loi du 11 mars 2003 sur la société de l'information. à la décision de la Cour de justice dans l'affaire *Scarlet*, en raison des atteintes à la liberté d'expression, à la liberté d'entreprise (des FAI) et à la protection des données personnelles potentiellement englobées dans la surveillance des communications que le filtrage induit. Un filtrage peut également porter atteinte au principe de neutralité de l'internet.

Un filtrage limité à certains contenus et proprement délimité dans son étendue et dans le temps, comme cela est prévu par l'article 21, § 1er, alinéa 2 de la loi du 11 mars 2003 sur la société de l'information, est toutefois envisageable s'il respecte les exigences de proportionnalité mises en avant par la juridiction européenne.

3. *Obligation de communiquer des informations*

Aucune spécificité par rapport aux questions générales relevées *supra* n'est à relever sur ce point quant aux fournisseurs d'accès internet.

D. Actions contre DNS.be

L'organe de gestion de l'extension .be en matière de noms de domaine peut être considéré comme un intermédiaire visé par les articles 86*ter* et 87 de la loi sur le droit d'auteur. Une action en cessation peut donc légitimement être intentée à son encontre pour lui demander de bloquer le nom de domaine utilisé pour diffuser des œuvres protégées sans autorisation des ayants droit. Une injonction de communiquer les informations dont DNS.be disposerait est également applicable mais sans réelle pertinence dans la mesure où les informations relatives au titulaire d'un nom de domaine en .be sont rendues publiques.

Par analogie avec ce qui a été développé pour les mesures de blocage sollicitées des FAI, les questions soulevées sont également d'application dans le contexte du DNS.be, et notamment la question de la délimitation de l'ordre de cessation et l'impact sur la liberté d'expression et le droit d'accès à l'information des sites bloqués par erreur ou par absorption (étant partie d'un nom de domaine bloqué). Sur le premier point, se pose la question de la possibilité d'enjoindre DNS.be de bloquer tout nom de domaine lié à une adresse IP identifiée.

Ici également, l'intervention d'une autorité administrative pourrait pallier ces difficultés en établissant une liste régulière des noms de domaine que DNS.be devrait désactiver et en ayant compétence pour traiter des recours des sites bloqués par erreur.

E. Actions contre les moteurs de recherche

Les titulaires de droit adressent de nombreuses requêtes aux moteurs de recherche pour supprimer des liens dans les résultats d'une recherche. Les moteurs de recherche obtempèrent généralement et déréférencent les sites spécialisés en contenus illicites. Il est à noter que les moteurs de recherche ne bénéficient pas *a priori* en droit européen d'une exonération de responsabilité claire quant à leurs fonctions de moteurs de recherche, mais qu'on ne peut pas leur imposer d'obligation de surveillance généralisée. L'effet d'une suppression d'un lien dans les sites référencés par les moteurs de recherche, s'il n'équivaut pas à un retrait du site de l'internet, le rend néanmoins largement invisible des utilisateurs.

Les demandes des ayants droit se réalisent sur base de notification, à l'instar des demandes adressées aux hébergeurs et les mêmes incertitudes quant à l'absence d'un format et d'une procédure standardisés pour ces *notice and take down* se reposent ici.

De même l'impact de l'intervention systématique des moteurs de recherche d'une part, sur la liberté d'entreprise de ces acteurs et d'autre part sur la liberté d'expression et le droit à un procès équitable des auteurs de contenus qui sont ainsi déréférencés n'est pas éloigné du contexte de la suppression de contenus hébergés.

En outre, la question de l'extension d'un ordre de cessation obtenu à l'encontre d'un moteur de recherche à d'autres moteurs de recherche par identité de motifs se repose dans les mêmes termes que pour les injonctions de blocage obtenues contre certains fournisseurs d'accès internet.

En conclusion, tout comme pour les hébergeurs, les entreprises opérant des moteurs de recherche gagneraient à une clarification des règles en matière de notification. Celles-ci devraient comprendre des garanties et voies de recours pour les auteurs des sites déréférencés.

L'opportunité d'instituer une autorité administrative, doublée d'un recours devant les tribunaux judiciaires, pour établir une liste de sites à déréférencer et accueillir les plaintes éventuelles des sites n'apparaissant plus dans les résultats de recherche, devrait également être examinée.

F. Actions contre les services de paiement

Les services de paiement peuvent être considérés comme des intermédiaires dont les services sont utilisés par des sites mettant à disposition des œuvres sans autorisation et se faisant rémunérer pour celles-ci. A ce titre, les ayants droit peuvent demander à ces intermédiaires de communiquer au juge des informations sur les contrefacteurs ou intenter une action en cessation à leur encontre, qui aurait pour effet de bloquer les paiements à destination des auteurs des atteintes au droit d'auteur.

La cessation des paiements n'aura pas d'impact sur les droits fondamentaux sauf sur la liberté d'entreprise en cas de site internet licite visé par erreur. L'hypothèse sera peu probable dans la mesure où un juge vérifiera la réalité de l'atteinte avant d 'ordonner une cessation des paiements. La question de la communication des données personnelles se pose de la même manière que pour les autres intermédiaires.

Sur le plan territorial, des organismes de paiement situés en Belgique (tel ATOS) traiteront des paiements par cartes de crédit détenues par les internautes belges ayant téléchargé des contenus illicites contre rémunération. Il sera donc facile d'intenter une action en cessation devant un juge belge. Quant aux paiements par Paypal, les opérations européennes de cette société américaine se font par l'entremise d'une filiale installée au Luxembourg et contrôlée par les organismes financiers de ce pays.

III. Autres questions

A. Coût de l'implication des intermédiaires

Dans la mise en œuvre des mesures prises en amont du téléchargement d'œuvres illicitement mises à disposition, le rôle des intermédiaires est essentiel. Il faudra veiller à évaluer le coût financier que représente cette implication dans leur chef. Une participation des ayants droit aux frais engendrés par l'instauration de ces mesures de blocage, de retrait, de déréférencement ou de communication de données, pourrait être envisagée.

B. La légitimité d'une autorité administrative

L'intervention d'une autorité administrative dans la centralisation de certaines mesures à enjoindre aux intermédiaires a le mérite de rendre ces mesures plus aptes à s'adapter à la rapidité de réaction des contrefacteurs, ainsi que de constituer une instance de recours pour les auteurs des contenus supprimés.

Toutefois la légitimité et l'opportunité de ce rôle central dévolu à un organe administratif et non juridictionnel peuvent être discutées.

Sur le plan juridique, dans la mesure où cette autorité pourrait définir les sites devant être bloqués ou déréférencés et des restrictions de droits fondamentaux que ces blocages sont susceptibles d'emporter (liberté d'expression, droit à un procès équitable principalement), il est plus prudent de confier ce rôle à une autorité juridictionnelle ou à tout le moins de limiter le rôle de l'autorité administrative à la constitution de ces listes et à la saisine d'un juge. La délimitation de la compétence d'une telle autorité administrative et les garanties qu'elle doit offrir en matière de respect des droits de la défense et des autres droits fondamentaux devrait être analysée plus avant.

En matière de sites pédopornographiques, le Conseil Constitutionnel français a validé un tel système, considérant que « les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif

de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 »[751].

En sus des questions juridiques de légitimité d'un tel organe administratif, la popularité d'une telle institution, qui pourrait être perçue comme un organisme de censure central, n'est pas garantie si l'on se réfère à l'opposition très forte qu'a suscité le projet espagnol qui comprenait une Commission de la Propriété Intellectuelle, chargée entre autres d'un rôle d'injonction auprès des intermédiaires sur demande des ayants droit (et ce en dépit du fait que cette autorité soit spécialement chargée de garantir les intérêts et droits des auteurs des sites).

§3. Système de réponse graduée

I. Modalités pratiques

La mise en place d'un régime de réponse graduée peut prendre différents degrés. La solution la plus maximale, à l'instar de la loi française HADOPI, est de couper la connexion de l'internaute multirécidiviste. Sans aller jusqu'à la coupure, une suspension peut être envisagée, ou une limitation du volume de bande passante. Un régime plus léger consiste à n'adopter que les premières étapes de la réponse graduée, sans coupure ou suspension des moyens de communication, mais utilisant l'envoi successifs d'avertissements et de rappels à l'ordre à des fins dissuasives et pédagogiques.

Un mécanisme de réponse graduée ne peut que reposer sur une autorité centralisée en charge de détecter les échanges non autorisés, d'identifier les internautes responsables, de leur envoyer les emails de remontrance, et éventuellement d'enclencher, en cas de récidive, une procédure de suspension ou de coupure de l'accès à Internet. Cette dernière étape peut être confiée à un juge ou rester une compétence de l'autorité administrative (assortie le cas échéant d'un recours devant les tribunaux).

II. Questions juridiques

A. Protection des données personnelles

Les ayants droit qui collectent les adresses IP en surveillant les réseaux *peer-to-peer* effectuent un traitement de données à caractère personnel. Il en serait de même pour une autorité administrative qui serait en charge d'une telle surveillance.

[751] Conseil Constitutionnel, décision n° 2011-625 DC du 10 mars 2011 sur la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, §8.

Si l'on considère que les adresses IP étant récoltées en lien avec la commission d'une atteinte au droit d'auteur doivent être qualifiées de données judiciaires au sens de la loi sur la protection des données personnelles, soit de « données relatives à des suspicions ayant trait à des infractions », leur traitement est interdit. Les titulaires de droit ne pourraient bénéficier de l'exception permettant le traitement des données judiciaires aux seules fins de gestion de leur propre contentieux, dans la mesure où la Commission de protection de la vie privée estime que cette exception ne couvre que des données relatives à une infraction précise et ne permet pas une surveillance et une collecte de données proactive et systématique, dans le but de déceler des atteintes au droit d'auteur.

Un autre motif d'illégalité du traitement réside dans l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques qui interdit de « prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise pas voir de communication électronique (qui) ne lui est pas destinée personnellement ; identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ; (…) prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ; modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non ».

Toute collecte des données par les ayants droit, dans un contexte de surveillance des échanges sur internet, serait donc interdite, ce qu'a confirmé le Conseil constitutionnel français dans son analyse du projet de loi HADOPI. En conséquence, la preuve ainsi obtenue serait illégale ce qui entacherait les poursuites fondées sur de telles preuves, même si la jurisprudence s'est quelque peu assouplie et ne rejette plus systématiquement les preuves collectées de manière irrégulière.

Le Contrôleur Européen de la Protection des Données Personnelles a également considéré qu'une surveillance de tous les internautes, indépendamment de toute suspicion d'une atteinte au droit d'auteur à leur égard, l'effet potentiel de cette surveillance, soit la coupure de la connexion, ainsi que le fait que la surveillance soit effectuée par des personnes privées ne permettaient pas de conclure au respect du principe de proportionnalité.

La communication par le FAI de l'identification de ses données aux titulaires de droit disposant des adresses IP constitue également un traitement de données personnelles. L'arrêt *Bonnier* admet un élargissement de l'obligation de communication, pour permettre la communication de ces données non aux autorités nationales compétentes mais aux titulaires de droits pour autant qu'un équilibre soit préservé entre les intérêts en présence. En l'espèce, la Cour valide la législation nationale en question dans la mesure où elle exige que « des indices réels d'atteinte à un droit de propriété intellectuelle sur une œuvre existent, que les informations demandées soient susceptibles de faciliter l'enquête sur la violation du droit d'auteur ou l'atteinte à un tel droit et que les raisons motivant cette injonction soient d'un intérêt supérieur aux inconvénients ou aux autres préjudices qu'elle peut entraîner pour son destinataire ou à tout intérêt qui s'y oppose ». La loi belge, et plus particulièrement l'article 86*ter* de la LDA semble correspondre aux exigences de la Cour. Le juge saisi d'une demande d'injonction de communiquer les données peut donc pondérer les intérêts opposés en présence en fonction des circonstances de chaque espèce.

Dans le même sens, le Conseil Constitutionnel français a admis le traitement des données personnelles pour autant que les données collectées ne servent qu'à permettre d'exercer les recours juridictionnels nécessaires relatifs aux atteintes au droit d'auteur. Le Conseil enjoint toutefois que ces données ne soient transmises qu'à la commission de protection des droits (en charge de la

réponse graduée) ou aux autorités judiciaires et fait interdiction aux agents assermentés des sociétés de gestion collective de surveiller ou d'intercepter des échanges ou correspondances privées. Les décrets d'application de la loi HADOPI ont mis en œuvre ces principes permettant la collecte des adresses IP des internautes.

En conclusion, un système de réponse graduée ne peut fonctionner que si la loi offre les garanties nécessaires à la protection de la vie privée : les données collectées doivent être adéquates, pertinentes et non excessives ; une obligation de sécurisation des données repose sur le maître du fichier ; et un délai raisonnable et limité de conservation des données doit être appliqué. Ce délai ne peut sans doute dépasser le délai de récidive prévu par la loi pour enclencher les étapes successives de la réponse graduée. Confier l'envoi des emails d'avertissement aux fournisseurs d'accès, à l'instar de la loi française, évite également que les données identifiées des internautes soient transmises aux ayants droit mais restent seulement connues des intermédiaires. Dans tous les cas, un contrôle judiciaire doit être maintenu.

B. Droit fondamental d'accès à internet

Le droit d'accès à Internet a été qualifié, par de multiples instances (Conseil constitutionnel français, parlement européen et plus implicitement Cour européenne des droits de l'homme) de droit fondamental qui ne peut être restreint qu'à l'intervention d'un juge. La dernière phase d'une réponse graduée devrait en conséquence relever de la compétence des cours et tribunaux, celle-ci ne pouvant toutefois être effective que dans un régime de réponse rapide. La France a confié cette compétence à des juges dans le cadre d'une procédure accélérée, que nous ne connaissons pas en droit belge. La sanction de la coupure de l'accès à Internet pourrait en outre être disproportionnée dans le cadre des offres combinées (TV, téléphone, Internet,...).

Si la sanction finale consiste en une limitation du débit de la connexion, l'atteinte au droit fondamental d'accès à l'Internet est plus réduite ce qui pourrait justifier que cette sanction ne passe pas par un juge mais puisse être prononcée par une autorité administrative, pour autant qu'elle soit limitée dans le temps. Il faudrait également s'assurer que la coupure d'accès ne touche en aucun cas les services de courrier électronique.

En cas de limitation du débit, comment toutefois inciter le retour de l'internaute vers les offres légales, qui requièrent une certaine capacité de téléchargement ? Il serait utile de vérifier si techniquement le téléchargement d'œuvres sur des plateformes légales peut être comptabilisé dans le débit autorisé.

C. Droit de la défense et procès équitable

Un autre argument plaidant en défaveur de la solution d'une autorité administrative en charge d'un mécanisme de réponse graduée est la prise en compte des droits de la défense et du droit à un procès équitable dont bénéficie tout internaute visé par les sanctions. Ce dernier doit pouvoir disposer de recours en cas d'accusations inexactes, a le droit de connaître les accusations précises

portées contre lui et de pouvoir les contester dans une procédure contradictoire. Les constatations d'atteinte se basant sur des données techniques peu probantes (l'utilisation d'une adresse IP à un moment donné), le risque d'accusations inexactes est grand, particulièrement parce que la connexion (surtout car il s'agit d'un wifi) peut être partagée par de nombreuses personnes, utilisée sans autorisation par des tiers, voire piratée à la faveur d'introduction de virus ou chevaux de Troie à l'insu du propriétaire de l'ordinateur.

Dans le système français, l'internaute n'a aucun moyen de connaître les atteintes qui lui sont reprochées ni de les contester lorsqu'il reçoit les premières notifications avant coupure de l'accès. Or ces notifications qui émanent d'une autorité administrative et ont pour effet de constituer des étapes préliminaires à une véritable sanction doivent être considérées, non comme des simples rappels de la loi, mais comme des actes administratifs pour lesquels un recours doit être ouvert.

Il faut donc prévoir à tout stade de la réponse graduée (des premiers avertissements à la suspension ou coupure éventuelle de la connexion) une possibilité pour l'internaute visé de pouvoir contester ce qui lui est reproché.

Un deuxième écueil des mécanismes de réponse graduée sur le plan du droit à un procès équitable réside dans le fait que le titulaire d'une adresse IP n'est pas forcément le contrefacteur. Poursuivre celui-ci pour atteinte au droit d'auteur est en contradiction avec la présomption d'innocence. C'est ce qui a conduit le législateur français à considérer que l'infraction pour laquelle les sanctions peuvent aller jusqu'à la coupure d'internet est le fait d'avoir manqué à une obligation de sécurisation de sa connexion internet, qu'elle qualifie de « contravention de négligence caractérisée ». On peut estimer que cette solution est artificielle car elle fait reposer un mécanisme de sanctions assez lourdes et impopulaires sur un manquement relativement léger et peu répréhensible en soi. Cette définition de l'infraction comporte également son lot de conséquences. La première est que l'HADOPI a été chargée de déterminer quels outils de sécurisation pouvaient être employés par les internautes et de leur décerner un label. Jusqu'à ce jour, la Haute Autorité n'a pas désigné un tel outil qui constitue pourtant une pierre importante de l'édifice HADOPI.

III. Autres questions

A. Opportunité et popularité des mécanismes de réponse graduée

Les régimes de réponse graduée ont une cote de popularité très basse auprès des internautes et ont suscité une large opposition citoyenne et politique dans les pays qui les ont adoptés. Cette opposition a également débordé dans les discussions européennes sur le Paquet Télécom et sur l'ACTA. L'HADOPI est devenue un thème important de la dernière campagne présidentielle française. S'engager dans cette direction comporte des risques politiques non négligeables. Une solution atténuée sans suspension ni coupure internet serait certainement moins impopulaire mais il s'agira de se poser alors la question de son effectivité, même si un rappel aux internautes de leurs obligations en matière de droit d'auteur peut avoir un certain effet.

B. Coût

Le coût d'un régime de réponse graduée est important. Le budget prévu pour l'HADOPI en France est de 6,7 millions d'euros annuels auxquels doivent être ajoutés les frais d'identification et d'envoi des courriers électroniques aux internautes. L'intervention des fournisseurs d'accès internet dans le mécanisme (identification des adresses IP, envoi des courriers, collaboration avec l'autorité en charge, investissement en termes d'équipements) a également un coût significatif qui a été estimé en France et en Angleterre à plusieurs dizaines de millions d'euros par an. Au Royaume-Uni, ce coût sera pris en charge à 75% par les titulaires de droit d'auteur ou de droits voisins. Il faut y ajouter le coût propre de ces procédures pour les ayants droit.

Au total, il n'est pas évident que les retombées –qu'on espère positives–, d'un tel système sur les offres légales justifie ce coût pour les ayants droit et pour les finances publiques.

Il est à préciser que dans le système français aucune rémunération des ayants droit ne peut être imposée aux internautes sanctionnés en l'absence de toute possibilité pour les premiers de demander des dommages et intérêts pour les contrefaçons réalisées.

C. Les conséquences techniques et sociales d'une obligation de sécurisation des connexions internet

Le mécanisme de réponse graduée obligera, soit directement à l'instar de la loi française, soit par voie de conséquence pour les internautes soucieux de ne pas se voir accusés d'actes d'échange accomplis par autrui, de sécuriser leur connexion internet.

Alors que les connexions internet par wifi se multiplient, on peut s'interroger sur l'opportunité de ces obligations de sécurisation. Techniquement, il ne fait pas de sens de multiplier les connexions wifi alors que plusieurs personnes pourraient s'en partager l'usage. Les wifis ouverts se sont en outre développés dans les espaces publics et constituent des biens publics ayant une valeur sociale importante, particulièrement dans le cadre des bibliothèques, institutions d'enseignement, lieux publics. Cadenasser ces wifis serait un retour en arrière et nuirait à l'inclusion numérique et au développement d'une économie numérique. Ce coût social devrait être analysé.

§4. Mesures additionnelles : mesures éducatives et promotion des offres légales

Quelle que soit l'option choisie, elle devra être accompagnée de mesures éducatives sur la valeur de la création et l'importance du droit d'auteur. Les offres légales devront également être soutenues. Le système HADOPI comporte par exemple de nombreuses mesures de promotion des offres légales : la liste des plateformes offrant des contenus en toute légalité est disponible sur le site internet de l'Autorité et celle-ci délivre des labels certifiant que l'offre est légale (Label PUR – Promotion des

Usages Responsables). Diverses études ont également été confiées à l'HADOPI pour promouvoir la protection et la diffusion des œuvres sur Internet.

De manière plus générale, les obstacles juridiques, techniques ou pratiques au développement de services mettant légalement les œuvres à disposition des internautes devraient être identifiés et analysés plus avant.

Conclusion

La diminution des offres illégales d'offres sur Internet ne passe pas par une solution unique. Au terme de cette étude, on ne peut proposer un système clé en mains qui pourrait résoudre l'accès aux œuvres en streaming ou par voie de téléchargement sur des sites ou par des échanges non autorisés. Des trois options principales que nous avons étudiées, la voie de la légitimation des échanges ne peut sans doute pas prospérer en raison de multiples obstacles légaux et pratiques. La licence légale, véritable exception au droit d'auteur pose de sérieux doutes quant à sa légitimité et la voie de la licence résultant de la gestion collective se heurte à des difficultés d'implication des FAI et de globalité du répertoire donné en licence.

Quant aux mécanismes de réponse graduée, s'ils se répandent sur le plan international, ils n'en suscitent pas moins de nombreuses questions en matière de protection des données personnelles, de droits de la défense et d'accès à l'information... sans parler de la forte opposition populaire que ces systèmes engendrent.

La lutte contre l'offre illicite d'œuvres protégées passe donc surtout par un renforcement et une simplification des moyens de lutte contre les sources de telles contrefaçons, sites de stockage ou de *streaming*, sites de Torrent, listes d'hyperliens, etc. Dans le respect du principe d'exonération de responsabilité des intermédiaires, une collaboration accrue de ceux-ci peut certainement être poursuivie et il peut leur être demandé de retirer des contenus litigieux, de bloquer l'accès à des sites illicites, de suspendre tout paiement vers les exploitants de ceux-ci, de fournir l'identité des personnes suspectées de contrefaçon. L'initiative pourrait utilement être partagée entre les ayants droit et une autorité administrative qui pourrait jouer un rôle utile de centralisation et de détection des noms de domaine ou adresses IP de sites consultés en Belgique pour accéder à des œuvres sans autorisation. De manière additionnelle, la compétence du juge des cessations de pouvoir agir sur requête unilatérale pourrait être étendue à des actions visant uniquement à étendre les mesures prononcées par une injonction coulée en force de chose jugée, à toute manœuvre de contournement ou de migration entreprise par l'opérateur du site web condamné, moyennant un encadrement légal strict.

Ce renforcement des moyens judiciaires et des actions à l'encontre des intermédiaires n'est pas sans dommages collatéraux éventuels et il faudra en tenir compte. L'on songe à un blocage ou à un retrait indu de sites ou contenus légitimes, à un éventuel impact sur la protection des données personnelles, et sur les libertés d'expression, d'accès à l'information ou d'entreprise, du coût engendré pour les intermédiaires sommés de collaborer, à l'obligation de ne pas transformer ceux-ci en juges de l'illicite trop zélés. L'intervention d'une autorité administrative pourrait offrir certaines garanties sur tous ces points, même si le recours à un juge doit toujours subsister en dernier ressort.

Un rôle subsidiaire peut certes être conservé pour des mécanismes d'autorisation ou de réponse graduée. D'une part, les ayants droit pourraient convenir, sur base collective, d'autoriser certains échanges d'œuvres, lorsque l'effet sur l'exploitation de celles-ci est réduit, par exemple en matière d'œuvres épuisées. Mais le coût du contrôle du respect de telles licences serait important. D'autre part, l'avertissement des internautes qui s'adonnent aux échanges de fichiers en *peer-to-peer* et le

renvoi de ceux-ci vers des offres légales peut comporter des vertus bien qu'il ait un coût significatif, tant en termes financiers que sociaux.

En parallèle de toute option qui serait choisie, le renforcement des offres légales et de l'intérêt des consommateurs pour celles-ci s'avère indispensable. Outre la facilitation des obtentions de licences pour la mise à disposition légale de contenus musicaux, audiovisuels, littéraires et autres, à l'échelon national et paneuropéen, à laquelle s'attelle notamment l'Union européenne, il faut s'engager dans un changement des pratiques, à la fois des titulaires de droit et exploitants d'œuvres littéraires et artistiques et des utilisateurs et consommateurs de celles-ci. Les premiers devront varier leurs modèles économiques, leurs offres et leurs conditions d'utilisation pour répondre au mieux aux nouveaux usages et demandes du public numérique. Quant aux internautes et consommateurs, ils devront en revanche réaliser que la création a une valeur que l'ayant droit a le pouvoir et la liberté d'exploiter (même dans un modèle de libre accès éventuellement). Plus de pédagogie est certainement au programme et doit s'affranchir du message principalement répressif que l'on a destiné jusqu'ici aux internautes.

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
http://economie.fgov.be