LE DEVELOPPEMENT ET LA PROTECTION DES OEUVRES CULTURELLES SUR LES NOUVEAUX RESEAUX

Novembre 2007

RAPPORT AU MINISTRE DE LA CULTURE ET DE LA COMMUNICATION

Mission confiée à Denis Olivennes

Membres : Olivier Bomsel, *professeur d'économie et chercheur au Centre d'économie industrielle de l'Ecole des Mines*

Isabelle Falque-Pierrotin, *Conseiller d'Etat, déléguée générale et présidente du Conseil d'orientation du Forum des droits sur l'Internet*

Pascal Faure, *Vice-Président du Conseil Général des Technologies de l'Information*

Rapporteur : Damien Botteghi, *auditeur au Conseil d'Etat*

Suivi des séances : Olivia Bozzoni Fringant, *Docteur en droit*

INTRODUCTION

La France est aujourd'hui l'un des tous premiers pays du monde par le développement d'Internet, en particulier d'Internet à haut débit, la fibre optique annonçant encore de nouveaux progrès en termes de capacité. Dans le même temps, elle demeure exceptionnelle du point de vue de la vitalité de ses industries de création – qu'il s'agisse de l'audiovisuel, du cinéma, du livre ou de la musique. Au moment où les nations se livrent une concurrence féroce pour figurer en tête de l'économie mondiale de l'immatériel et de la société de l'information, notre pays peut tirer un grand parti économique et culturel de ces deux atouts majeurs.

Encore faut-il que les dynamiques d'Internet et de la création se conjuguent et que les acteurs de ces deux secteurs coopèrent. C'est leur intérêt respectif : Internet a besoin de contenus nombreux et attrayants ; les industries culturelles et les créateurs ont, avec Internet, un débouché nouveau et puissant. C'est également l'intérêt des consommateurs, qui disposeront de réseaux étendus et de contenus divers et de qualité. C'est enfin l'intérêt de la nation, en raison de la stimulation de la création, de la multiplication des contenus et du surplus de richesse économique engendrés par le développement de ces deux secteurs d'avenir.

Cependant, pour l'instant, tout semble pousser l'internaute à choisir la voie de la consommation illégale. Elle est à la fois facile, en raison d'un haut débit de qualité, gratuite et adaptée à tous les supports. En regard, l'offre légale est souvent verrouillée, par les mesures techniques de protection qui limitent la libre utilisation et la conservation de l'oeuvre achetée, ou par la disponibilité tardive de cette dernière. Nombre de consommateurs font état d'une insatisfaction face à l'offre légale, qui explique également qu'ils se détournent de tels achats.

Pourtant, cette consommation illégale est aujourd'hui une source de destruction de valeur : en affaiblissant la rémunération des créateurs, le financement de la production et l'efficacité économique de la distribution, elle compromet la diversité des œuvres et constitue une menace pour la vitalité de la création, donc pour l'identité de la France et de l'Europe. Il est désormais urgent d'inverser les signaux envoyés aux agents économiques, en particulier les consommateurs, et de faire prendre conscience que la généralisation du gratuit illégal a un coût collectif pour les industries culturelles, pour les créateurs et pour la nation.

Tout doit être fait pour désinciter au piratage, par des réponses proportionnées, pragmatiques, respectueuses des libertés individuelles et compatibles avec la rapidité d'évolution des technologies. Cela nécessite d'abord de continuer à informer et à sensibiliser, notamment les jeunes générations Cela passe ensuite par la promotion d'une offre légale attractive, aussi facile d'usage que l'offre illégale, car les études montrent que les consommateurs sont prêts à payer si une offre légale correspond à leurs attentes. Cela requiert enfin de compliquer sérieusement la violation de la propriété intellectuelle, en trouvant des réponses qui soient cependant mesurées, adaptées aux comportements et qui puissent, en particulier, dissuader la répétition des mêmes actes.

En d'autres termes, il s'agit de rendre plus difficile et plus coûteux le téléchargement illégal, et, inversement, plus facile et moins cher le téléchargement légal. Toute avancée en ce sens nécessite la coopération de tous les acteurs : ayants droit, pouvoirs publics et prestataires techniques. C'est dans un état d'esprit de responsabilité collective qu'acteurs privés et pouvoirs publics doivent converger vers des mesures de désincitation au téléchargement illégal et d'incitation au développement des usages légaux.

1 LE PIRATAGE NUMERIQUE EN FRANCE.

Face à un piratage massif des oeuvres numériques utilisant des techniques très évolutives et adaptées à tous les types d'oeuvres, les réponses juridiques et techniques qui se sont progressivement mises en place n'ont pas pour l'instant trouvé leur pleine efficacité.

1.1 Le piratage est massif et diversifié.

1.1.1 La France connaît une situation spécifique.

La situation en France est marquée par une offre illégale très forte, et inversement une consommation légale encore très faible, notamment pour la musique.

Pour les films, selon une récente étude du centre national de la cinématographie[1], 93,6 % des films piratés et déjà sortis en salles seraient disponibles sur les réseaux pair-à-pair avant leur sortie en DVD sur le territoire français. L'étude de 2005 et celle de 2004 présentaient des résultats légèrement moins élevés (respectivement 91,8 % et 91,0 %). Plus précisément, 40,5 % des films sortis en salles en France entre le 1er janvier et le 31 décembre 2006 sont disponibles en version française pirate sur les réseaux pair-à-pair sur cette même période ; ils étaient 37,9 % en 2005 et 36,4 % en 2004. Dans le domaine de la musique, les chiffres ne sont pas faciles à établir, et peuvent être discutés dans leur ampleur exacte. Le récent livre blanc du syndicat national de l'édition phonograhique (SNEP)[2] fait état d'un milliard de fichiers téléchargés, soit environ l'équivalent des ventes physiques de titres[3], dont seulement 20 millions sur des plate-formes de téléchargement légal. Ces chiffres très importants s'expliquent notamment par la qualité de l'offre d'accès en haut débit à internet à un coût parmi les plus faibles au monde. En France, la proportion des internautes pratiquant le téléchargement (musique, films, jeux vidéo et logiciels) est sans commune mesure avec celle recourant à un téléchargement de fichiers légaux, part au demeurant plus faible que celle constatée dans la plupart des autres pays, surtout dans le domaine de la musique. En matière d'offre VoD, cependant, la situation française est plutôt marquée par une avance : notre pays figure en tête du nombre de services IPTV et en seconde position pour le nombre de services VoD disponibles sur le web[4].

De fait, les produits culturels numérisables sont omniprésents sur le réseau internet et accessibles sous différentes formes. La dématérialisation des supports, associée à l'apparition du haut débit – et, bientôt, l'arrivée de la fibre optique, technologie offrant des débits symétriques et plus élevés, facilitant considérablement le téléchargement de fichiers denses, notamment vidéo – a bouleversé l'accès aux contenus culturels et multiplié les moyens et modalités de piratage. Plus particulièrement, l'échange de fichiers par des logiciels de pair-à-pair a pris, à partir de 2002, une ampleur considérable. On considérait en 2003 à plus de 150 milliards le nombre de fichiers musicaux[5] échangés dans le monde via ces logiciels. Une étude par protocoles avait été menée par la société CacheLogic[6] : publiée en 2004 et mise à jour en 2005 (hors données françaises), elle

[1] Etude CNC/ALPA, d'octobre 2007, disponible sur le site du CNC.
[2] Livre blanc sur le « peer-to-peer », Paris, 25 octobre 2007.
[3] Selon l'IFPI, les ventes physiques de disques en France en 2005 se sont élevées à 24,7 millions de *single* et 83 millions d'albums.
[4] Etude conduite par NPA Conseil pour la Direction du développement des médias et l'Observatoire européen de l'audiovisuel, mai 2007, disponible sur le site http://www.ddm.gouv.fr/.
[5] L'Idate estime qu'en 2003, près de 150 milliards de fichiers musicaux (contre 50 milliards vendus sur support physique), un milliard de films en DVD et 550 millions d'images ont été échangés sur les réseaux pair-à-pair.
[6] CacheLogic, « *P2P in 2005* ».

faisait apparaître que le trafic P2P représente 60 % du trafic. D'après l'OCDE[7], les utilisateurs simultanément actifs de ces réseaux dans le monde étaient près de 10 millions en avril 2004, en progression de 30 % par rapport au mois d'avril 2003. Les données recensées par Big Champagne confirment ces ordres de grandeur[8] : le cap des 10 millions a été franchi en 2005. En outre, de la musique, le phénomène s'est étendu aux films et aux programmes de télévision, notamment les séries.

1.1.2 Le piratage recourt à des techniques en évolution constante.

On peut considérer que le piratage utilise principalement deux types de techniques, en elles-mêmes neutres et qui peuvent ainsi également servir à des fins légales.

- Le téléchargement par un réseau de *peer to peer*, qui constitue un procédé d'échange de fichiers directement entre des postes individuels d'utilisateurs connectés à Internet, lesquels mettent à disposition leurs bibliothèques multimédias et, réciproquement, téléchargent des fichiers rendus disponibles par d'autres utilisateurs. Les contributeurs (membres apportant du contenu nouveau) représentent une part mineure dans la communauté ; les utilisateurs, majoritaires, se contentent de télécharger des fichiers mis à disposition sans avoir d'ailleurs nécessairement conscience que, ce faisant, ils mettent souvent automatiquement à disposition des autres utilisateurs les fichiers qu'ils ont eux-mêmes récupérés sur leur propre ordinateur.

- La mise à disposition de contenus illégaux, par le recours à des sites hébergeant des contenus, chacun présentant des variantes dont les caractéristiques diffèrent parfois sensiblement. Dans ce cas, des éditeurs ou des hébergeurs stockent sur leurs serveurs des fichiers multimédias, soit envoyés par des utilisateurs ayant créé le contenu piraté, soit récupérés à partir d'un support ou d'une offre légale. Il s'agit principalement de serveurs dédiés, des sites communautaires et de partage, ou enfin des *newsgroups*.

L'attention s'est d'abord portée sur les sites internet « classiques », avec une mise à disposition centralisée (type Napster), puis sur les réseaux de pair-à-pair qui, fondés sur un réseau en étoile, permettent d'éviter le risque de fermeture du site central. Désormais, ces supports de la distribution d'offre illégale sur le réseau tendent à diminuer au profit des mises à disposition, tels les *newsgroups* et les systèmes *usenet*. Or les solutions permettant de désinciter à la contrefaçon sur ces différents types de support ne sont pas identiques.

1.1.3 Le piratage a des effets économiques négatifs.

Selon les chiffres publiés par le SNEP, le chiffre d'affaires des producteurs de disques, qui était en 2002 de 1 302 millions d'euros, a chuté à 819,2 millions d'euros en 2006. Au premier semestre 2007, les ventes physiques ont baissé de – 20 %. Si le marché de l'offre musicale légale dématérialisée commence à croître – pour la musique, par exemple, on passerait de 43,5 millions d'euros pour la France en 2006 à 100 à 120 millions en 2010 – cette progression est loin de compenser la perte de revenus liée à l'effondrement du support physique.

Ce qui est vrai de la musique depuis cinq ans est également vrai aujourd'hui des œuvres audiovisuelles et cinématographiques. Cette situation remet en cause le financement de la production et donc de la création culturelles.

---

[7] « OECD, Information Technology Outlook 2004 : Peer-to-peer networks in OECD countries ».

[8] V. rapport du Conseil supérieur de la propriété littéraire et artistique sur « le Peer-to-Peer », décembre 2005.

1.2 Plusieurs outils, tant juridiques que techniques, peuvent déjà être mis en oeuvre pour désinciter au piratage numérique.

1.2.1 La loi prévoit sanctions et recours préventifs.

Tout acte de contrefaçon numérique – qui est une atteinte à un droit de propriété – est considéré comme un délit (art. L. 335-2 à L. 335-4 du code de la propriété intellectuelle), passible au maximum d'une peine de 3 ans de prison et de 300 000 euros d'amendes[9]. Le volet du dispositif prévu par la loi dadvsi du 1er août 2006 qui prévoyait que le téléchargement réalisé à des fins personnelles ainsi que la communication au public opérée à des fins non commerciales échappaient aux sanctions prévues en cas de contrefaçon pour être considérés comme de simples contraventions a été censuré par le Conseil constitutionnel au nom du principe d'égalité devant la loi pénale. En outre, aux termes de l'article L. 335-2-1 du code de la propriété intellectuelle (article 21 de la loi dadvsi), le fait « de mettre à disposition du public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés » est susceptible des mêmes peines.

Plusieurs mécanismes permettent aux ayants droit de prévenir la présence de contenus illégaux sur des sites légaux, ou même de fermer certains sites hébergeurs en cas de mise à disposition illégale d'oeuvres sur des sites communautaires ou de partage. L'article 6-I-8 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 ouvre aux ayants droit la possibilité de saisir l'autorité judiciaire pour prescrire en référé à un prestataire technique toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. La voie du référé de droit commun est donc ouverte, et tout mode de preuve est accepté si elle est obtenue loyalement, sans fraude et débattue contradictoirement devant le juge.

Par ailleurs, l'article 8 de cette loi a élargi les possibilités de saisie-contrefaçon, régies par l'article L. 332-1 du code de la propriété intellectuelle, en prévoyant que le président du tribunal de grande instance peut, par ordonnance sur requête, décider de la suspension, par tout moyen, du contenu d'un service de communication au public en ligne portant atteinte à l'un des droits de l'auteur, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut, de cesser d'en permettre l'accès.

Ces dispositifs, s'ils sont encadrés par un certain formalisme qui ne paraît pas excessif au regard des droits en jeu et qui peut permettre d'éviter un passage devant le juge en cas d'accord préalable, sont rapides et peuvent être efficaces. Toutefois, leur mise en oeuvre suppose une interprétation ouverte des dispositions introduites en 2004 dans la loi relative à l'informatique et aux libertés quant à la possibilité pour les sociétés de perception et de répartition des droits d'auteur de mettre en place des dispositif de recherche d'infractions, dans la lignée de la position que le Conseil d'Etat a prise en annulant, par un arrêt du 23 mai 2007 (*SACEM et autres*, 288149) une décision du 18 octobre 2005 de la CNIL estimant le contrôle que des sociétés d'auteur entendaient mettre en place comme non proportionné aux objectifs poursuivis.

[9] Ces sanctions ont été complétées par diverses contraventions (décret n° 2006-1763 du 23 décembre 2006, codifiant ces dispositions aux articles R. 335-3 et R. 335-4 du code de la propriété intellectuelle).

La voie de la réparation est enfin ouverte. Les juges[10] donnent la plus grande portée aux articles 6-I-2 et 6-I-3 de la loi du 21 juin 2004 relative à la responsabilité (civile et pénale) des prestataires techniques, au terme desquels une action prompte est exigée pour retirer les données incriminées ou bloquer un accès dès qu'il y a connaissance effective de faits illégaux. La connaissance de faits illicites est en effet entendue de manière très large au regard de la nature de l'activité d'hébergement des plate-formes de partage des vidéos. Cet article est ainsi un fondement solide d'engagement de la responsabilité, au moins civile, des sites de mise à disposition – à condition bien sûr que les ayants droit apportent au juge des éléments prouvant la présence de contenus illégaux (art. 6-I-5).

1.2.2 Plusieurs outils techniques sont désormais disponibles.

Trois approches, conjugables, déterminent autant de grandes méthodes qui peuvent être mises en œuvre pour lutter contre le téléchargement illicite en s'appuyant sur des technologies récentes et par suite perfectibles.

- **déceler la circulation de contenus illicites à partir d'outils de filtrage placés au sein du réseau**. Cette approche implique nécessairement les fournisseurs d'accès Internet. Les outils techniques correspondants existent et peuvent être mis en place en un point plus ou moins centralisé du réseau (pouvant aller du poste de l'utilisateur ou des points de raccordement au réseau jusqu'aux nœuds centraux de chaque fournisseur d'accès à internet). Cette approche, qui répond plutôt à un objectif de lutte contre le téléchargement illicite par la voie du pair-à-pair, peut nécessiter la mise en place de systèmes d'extraction et d'observation des flux par des intégrateurs de solutions comme *Qosmos* ou *I-tracing*. Néanmoins, les solutions techniques actuelles, diverses, récentes, relativement performantes mais encore perfectibles, n'ont jamais été déployées de façon opérationnelle à grande échelle, ce qui soulève des problèmes non encore résolus.

- **empêcher l'arrivée sur le réseau de contenus illicites à partir d'outils de filtrage mis en place chez les hébergeurs ou les éditeurs de services**. Il s'agit de pouvoir veiller à ce que la mise en ligne de contenus protégés se fasse en cohérence avec les droits associés et selon les conditions négociées avec les ayants droit. Cette approche, qui passe par des techniques d'identification de fichier telles que celles proposées par l'INA, *Advestigo*, ou *Audible Magic*, est devenue essentielle avec l'explosion récente des sites de partage de vidéo, vecteur important du téléchargement illicite actuellement.

- **repérer les flux illicites par observation externe réalisée par les ayants droit ou les autorités publiques à des fins dissuasives ou répressives**. Il s'agit de détecter la circulation sur les réseaux, à partir d'un accès client adapté, de contenus protégés préalablement ciblés, en vue de la constatation d'infractions ou de l'engagement de mesures appropriées. Cette approche est déjà mise en œuvre avec une certaine efficacité par certains ayants droit qui recourent à des sociétés telles que *CoPeerRight Agency*.

Ces trois approches peuvent s'appuyer sur des technologies communes, notamment lorsqu'il s'agit d'identifier les contenus, soit à partir de leur empreinte numérique (*fingerprinting*), soit en décelant un tatouage numérique inséré dès l'origine (*watermarking*). Les outils de marquage des œuvres et de reconnaissance de contenu multimédia (à partir d'un filigranage préalable ou par

[10] v. par exemple : TGI de Paris, 13 juillet 2007, *Christian C, Nord-Ouest Production c/ SA DailyMotion, SA UGC Images* ; TGI de Paris, 19 octobre 2007, *S.A.R.L. Zadig Productions, Messieurs J. V. et M. V. c/ Société Google Inc, L'Association des Fournisseurs d'Accès et de services internet.*

calcul empreinte) développés par de nombreuses sociétés (par exemple, outre celles déjà citées, Communications SA, *LTU Technologies*, Thomson ou Vivacode) peuvent servir à alimenter des bases de données pouvant être utilisées aussi bien pour le filtrage par les fournisseurs d'accès que pour le filtrage par les hébergeurs ou le repérage par les ayants droits.

A ces approches portant sur les réseaux d'échange ou sur les plate-formes d'hébergement de contenus s'ajoutent les techniques à base de DRM *(Digital Rigths Management)* qui visent à contrôler l'accès par l'utilisateur final d'une œuvre numérisée particulière (voir § 3.2).

2 INCITER AU DEVELOPPEMENT DE L'OFFRE LEGALE D'OEUVRES SUR INTERNET.

La première démarche pour désinciter l'offre illégale sur internet est de rendre l'offre numérique légale plus attractive, d'abord en terme de contenu, mais aussi et surtout en terme de facilité d'utilisation, de disponibilité et de prix. Il existe encore plusieurs verrous qui contraignent l'offre légale. Or il faut freiner voire arrêter le réflexe des nombreux internautes insatisfaits des conditions actuelles de l'offre légale de recourir systématiquement au téléchargement illicite.

2.1 Accélérer la mise à disposition en vidéo à la demande.

2.1.1 Aligner la fenêtre VOD sur la fenêtre DVD.

En France, les fenêtres d'exploitation sont réglementées, alors que dans d'autres pays la définition du rythme d'exploitation s'opère contractuellement pour chaque film. Le principe de la chronologie des médias est nécessaire, car chacun des modes de diffusion consécutifs tire des revenus propres qui permettent au final de financer la production cinématographique française. Néanmoins, l'apparition de nouveaux médias impose une insertion plus efficace de ceux-ci dans l'exploitation des films et un raccourcissement des délais de retour des investissements engagés. A l'ère de la numérisation, le raccourcissement du cycle de l'investissement constitue un facteur essentiel de la compétitivité des industries audiovisuelles.

Dans ce cadre, le renouvellement de l'accord du 20 décembre 2005 réglementant la durée des fenêtres, qui est arrivé à échéance le 20 décembre 2006, est en cours de négociation. La fenêtre pour la vidéo à la demande était de 33 semaines, contre 6 mois (24 semaines) pour le DVD. Ce décalage ne s'explique pas, s'agissant d'une offre qui, si le support diffère, est similaire. Un alignement de la VOD[11] sur le régime applicable à la vidéo physique est une première étape indispensable.

2.1.2 Ouvrir des discussions devant conduire à raccourcir les fenêtres de la chronologie des médias.

Les délais prévus actuellement – 6 mois entre la sortie en salle et l'exploitation DVD ; 9 mois pour le *pay per view* ; 12 mois pour Canal + ; 24 mois pour les chaînes ayant coproduit le film et 36 mois pour les chaînes en clair – paraissent inadaptés au rythme actuel de consommation des biens, et en décalage avec la plupart des délais observés dans les pays européens. Il est difficile de nier que la persistance de délais longs constitue une invitation au piratage, pour le moins paradoxale à l'époque où les industries culturelles entendent promouvoir une offre légale.

La mission est persuadée des avantages que chacun tirera d'un raccourcissement des fenêtres dans le sens des pratiques européennes. Ces dernières prouvent que des fenêtres

[11] Cela concerne aussi bien la location (VoD, SVoD) que la vente électronique.

d'exploitations plus courtes n'empêchent pas la bonne exploitation des films lors de leur sortie en salle, le lien entre la disponibilité d'une oeuvre en DVD et une éventuelle baisse de fréquentation en salle n'étant pas établi. Par ailleurs, les films tournent en salle plus vite, leur durée moyenne d'exploitation étant de quelques semaines. Une fenêtre de six mois paraît excessive. Plus encore, les différentes études qui ont pu être réalisées tendent à prouver que la diffusion en salle puis en DVD ou en VOD s'alimentent : la fréquence de visionnage d'une vidéo augmente à mesure que la consommation de films en salle est importante. La possibilité que le spectateur content, ou curieux, puisse trouver rapidement le film qu'il recherche de manière légale est essentielle. Il est rappelé, à cet égard, que rien n'interdit aux ayants droit, à la manière des américains, de différer, au-delà de ce délai, la sortie DVD et VOD pour ceux des films qui connaissent un succès prolongé en salle.

La mission a d'ailleurs constaté que ce souci était partagé par la grande majorité de ses interlocuteurs. Elle considère qu'un délai de quatre mois pour la mise à disposition d'oeuvres sur internet est un objectif souhaitable. Toutefois, dans le souci de trouver un accord, elle propose de laisser le soin aux partenaires d'aboutir à une solution commune, dans un délai d'un an à compter la mise en oeuvre de la politique ciblée ou du MAS, pour raccourcir la première fenêtre dans le sens de la moyenne européenne – en conservant le fait que la fenêtre de la VoD soit systématiquement calée sur celle du DVD – mais aussi ensuite toutes les fenêtres d'exploitation. Cette discussion devra évidemment tenir compte de l'existence des fenêtres d'exclusivité postérieures à l'ouverture de la fenêtre DVD et VOD, qu'il s'agisse de celle de Canal + ou des chaînes en clair.

Par ailleurs, la mission recommande que, pour faciliter cet aménagement, son impact économique sur les différents acteurs de la chaîne de valeur soit évalué et que, si nécessaire, les mécanismes de prélèvements pour le Centre national de la cinématographie ou d'aides reçues de celui-ci soient révisés en conséquence.

2.2 Elargir substantiellement le nombre des œuvres musicales en ligne sans mesure technique de protection.

Il a paru évident à la mission que le manque d'attractivité de l'achat en ligne d'oeuvres musicales est très lié aux contraintes d'utilisation que les mesures de techniques de protection imposent. L'achat d'une oeuvre numérique n'est intéressant que s'il permet la même liberté d'usage que le support physique. S'il n'existe pas de possibilité de conserver, en cas de changement d'ordinateur, les titres achetés pour former une bibliothèque personnelle ou s'il est impossible d'écouter cette musique sur le lecteur de son choix, le consommateur se refusera à acheter. L'interopérabilité est une condition de l'affirmation d'une offre numérique accessible, tant par les utilisateurs de logiciels propriétaires que par les utilisateurs de logiciels libres, dont les pratiques sont contradictoires avec l'usage actuel des mesures techniques. La liaison d'un contenu à un logiciel donné est clairement un obstacle.

Aussi, si les mesures techniques de protection peuvent être des outils pertinents de gestion des droits si, comme c'est le cas dans le domaine du cinéma, un standard existe, elles deviennent des obstacles lorsque divers modèles propriétaires se développent. La mission considère que tant que ne sera pas mis en place un standard de mesure technique assurant l'interopérabilité des fichiers musicaux, il faut permettre l'offre au détail de tous les fichiers musicaux en ligne sans mesure technique.

Toutefois, dans la perspective de trouver un accord d'ensemble, la mission considère qu'il est nécessaire :

- de mettre, dans un délai maximal d'un an à compter la mise en oeuvre de la politique ciblée ou du MAS, tous les catalogues d'œuvres françaises en ligne sans mesure technique de protection.

- de négocier des augmentations substantielles du nombre d'oeuvres étrangères disponibles sans verrous numériques.

2.3 Développer des actions de valorisation de l'offre numérique légale.

L'offre numérique légale, tant cinématographique que musicale, n'est pas encore suffisamment connue, valorisée, et à certains égards jugée légitime. La mission fait écho aux propositions qui ont été faites, en particulier par certaines associations de consommateurs et par les représentants des artistes-interprètes, qui seraient de nature à améliorer sa visibilité et son acceptabilité.

- L'instauration d'une signalétique, idéalement européenne, de la gestion des droits visant à informer le consommateur sur les libéralités d'usage associées aux produits dématérialisés : achat définitif ; location sur une courte durée ; écoute limitée ; écoute sur supports spécifiques ;

- La mise en oeuvre d'un portail sur lequel seraient répertoriés les offres légales, et surtout les conditions de cette offre (*streaming*, nombre de copies limité, etc...) ; il pourrait aussi servir d'interface entre consommateurs et prestataires de service, afin d'enrichir l'offre : l'idée serait de mettre fin au réflexe qu'ont les internautes d'aller vérifier sur les sites de téléchargement si une oeuvre non disponible légalement est offerte au téléchargement, en leur permettant non seulement de vérifier l'offre légale existante, mais d'indiquer leurs demandes ;

- L'ouverture de discussions entre les producteurs et les représentants des ayants droit sur les modalités de rémunération, notamment l'exercice des droits exclusifs et la répartition des revenus entres les différents ayants droit ;

- Le conditionnement des aides à la production délivrées par le Centre national de la cinématographie à l'obligation de rendre disponible le film en vidéo à la demande.

2.4 Solliciter de l'Union européenne une baisse de la TVA sur les produits culturels répercutée dans le prix public.

Afin de favoriser l'attractivité et le développement de la vidéo à la demande, il est nécessaire que l'ensemble des biens et services culturels se voit appliqué le taux réduit de TVA. Cette fiscalité allégée serait de nature à assurer un meilleur équilibre économique des offres légales, qui sont encore nouvelles et économiquement fragiles, à la condition nécessaire que cette baisse soit intégralement répercutée dans les prix publics. Si ces derniers parvenaient à obtenir cette généralisation, ils pourraient alors examiner la possibilité d'élargir encore l'assiette des abonnements internet soumise à taux réduit (50% aujourd'hui de l'abonnement « triple play ») en contrepartie de l'institution d'une taxe de financement de la création et de la diversité musicales à la manière de celle instituée au profit du CNC.

3 DESINCITER L'OFFRE ILLEGALE SUR INTERNET.

La facilité d'usage et la disponibilité de l'offre légale, si elles sont essentielles, ne permettront une réduction importante de l'offre illégale que s'il existe aussi parallèlement une politique qui vise à rendre cette dernière plus difficile. Dans ce domaine, la mission a fondé sa réflexion sur une approche réaliste privilégiant des dispositifs proportionnés et évolutifs. Certains mécanismes lui ont ainsi paru ne pas devoir être retenus, pour des raisons techniques, juridiques ou sociales. Elle propose, sur la base d'une clarification des usages divers de l'internet rassemblés sous le terme générique de téléchargement, deux mécanismes qui lui paraissent propres, dans le respect des libertés individuelles, à assurer l'objectif de désincitation de l'offre illégale sur internet.

3.1 Le choix de réponses pragmatiques et proportionnées.

3.1.1 Favoriser des réponses pragmatiques.

La mission est persuadée que la désincitation au piratage numérique doit s'organiser de manière réaliste et pragmatique. Elle a réfléchi aux dispositifs qui pouvaient être mis en oeuvre en se fondant sur trois impératifs.

- *La proportionnalité des dispositifs aux enjeux* – Le monde numérique est un espace de liberté dont les modalités de contrôle doivent être pesées et encadrées. Les enjeux de liberté publique sont centraux. Mais leur prise en compte ne doit toutefois pas justifier l'inaction. Nombre de pays occidentaux (Etats-Unis, Royaume-Uni,...), tout aussi respectueux des droits de l'individu, ont su mettre en place des dispositifs, fondés sur un mélange de pédagogie et de sanctions mesurées, dont les premiers résultats sont prometteurs.

- *Le recours simultané à plusieurs outils* – Il n'existe pas de solution unique à l'efficacité assurée. Il est illusoire de considérer que toute forme de piratage sur internet puisse être arrêtée : la technologie s'adaptera toujours plus rapidement aux contrôles et aux limitations que le droit ou la pratique pourraient imposer. Il faut donc, avant tout, trouver des mécanismes permettant de mettre fin à l'impunité et d'enclencher une prise de conscience, notamment des plus jeunes publics, que la gratuité généralisée et illégale a un coût. Cela nécessite d'utiliser plusieurs outils de manière parallèle, chacun ayant son efficacité relative, mais aussi de cibler les comportements de diffusion plus que de consommation.

- *L'adaptation dans le temps des réponses* – Certaines méthodes envisageables, comme le filtrage, recourent à des outils technologiques de conception encore récente et connaissant une évolution très rapide. Ces solutions seront dignes d'intérêt si elles atteignent leur pleine maturité, grâce à un meilleur étalonnage de leurs performances et à une appréciation plus fine des conditions de leur déploiement à large échelle, notamment en termes de coût, d'architecture, de choix de technologies adaptées et de compréhension des conséquences induites sur les comportements des internautes. On ne peut pas exclure non plus que d'autres technologies soient disponibles à l'avenir et soient alors préférées. La politique à mener doit donc être incitative et favoriser les expérimentations, de sorte à accélérer l'adaptation des outils du contrôle aux évolutions de la technologie et des pratiques du piratage.

3.1.2 Adapter les réponses aux types de piratage.

Les sanctions actuelles, qui peuvent être adaptées à des comportements de contrefaçon massive à but lucratif, paraissent disproportionnées pour des actes limités de contrefaçon à but non commercial. Une réponse uniquement pénale n'est pas satisfaisante : les poursuites, rapportées à la masse des infractions, sont rares, compte tenu de l'impact social de la qualification de délit et du passage devant un tribunal correctionnel. En outre, elles conduisent à ce que des peines légères soient prononcées, même si elles ont semblé récemment s'alourdir. Le dispositif n'a pas non plus de portée pédagogique. Cette voie, qui ne peut fonctionner en fait que par l'exemple, paraît inefficace si elle est la seule possible pour dissuader ou réprimer tous les comportements de téléchargement illégal, en fait très disparates.

Par ailleurs, le défaut de la politique actuelle est de traiter le piratage de manière générale, sans différencier les acteurs, ni les logiques à l'oeuvre derrière le terme de téléchargement illégal. Il a déjà été dit que l'utilisation d'un réseau de pair-à-pair n'appelait pas le même traitement que les sites de mise à disposition. La mission estime ainsi qu'il est primordial de mieux définir la politique visant à désinciter l'offre illégale, et donc de mieux cibler le public. L'accent devrait notamment être mis sur les primo-diffuseurs – les internautes qui mettent les premiers un contenu à disposition de manière illégale – et ceux qui mettent à disposition (*upload*) plutôt qu'aux utilisateurs (*download*), parfois de bonne foi.

La mission propose une grille des usages, auxquels pourraient s'adapter les sanctions à prendre (cf. infra). Il convient ainsi de différencier :

- Le *streaming* ;
- Le téléchargement (*download*) ;
- La mise à disposition (*upload*) modérée accessoire au téléchargement (*download*) ;
- La mise à disposition (*upload*) massive : primo-partageurs ou actions de commerce.

Une telle clarification – si elle correspond à une gamme de sanctions adaptées – paraît nécessaire, compte tenu des incertitudes qui demeurent, chez les internautes, sur le périmètre de l'utilisation légale ou illégale d'une oeuvre sur internet. A cet égard, le périmètre de l'exception de copie privée est encore très incertain. Reste notamment toujours en suspend la question posée par la Cour de cassation quant au fait de savoir si l'origine illicite d'une oeuvre exclut alors nécessairement, quel que soit l'usage, la reconnaissance de l'exception de copie privée visée à l'article L.122-5 du code de la propriété intellectuelle[12].

La mission considère d'ailleurs que devrait être adressée aux Parquets une nouvelle circulaire pénale modifiant celle en date du 3 janvier 2007, qui soit à la fois clarifiée et simplifiée, afin de favoriser une application effective de la loi.

[12] La cour de cassation, par un arrêt du 30 mai 2006, avait cassé un arrêt de la cour d'appel de Montpellier relaxant un jeune homme en possession de films copiés sur CD des poursuites intentées contre lui pour reproduction illégale de ces oeuvres, au motif que de telles reproductions visaient un usage privé. Elle a considéré qu'elle n'avait pas légalement fondé sa décision, faute de s'être interrogé sur le fait de savoir si *« l'exception de copie privée [ne suppose pas], pour pouvoir être retenue, que sa source soit licite »*. La cour d'appel d'Aix-en-provence saisie après renvoi n'a pas tranché ce point dans sa décision du 5 septembre 2007. Si elle a en effet retenu le caractère illicite des fichiers téléchargés et reconnu l'intéressé coupable de contrefaçon, c'est au seul motif que les reproductions avaient été mises à disposition et qu'ainsi les copies de films ne visaient pas un usage privé. La question de savoir si l'origine illicite de la source fait ou non obstacle par elle-même à l'exception pour copie privée reste donc ouverte, même si certaines juridictions se sont prononcées en faveur de l'exigence d'une source licite (*TGI Rennes, 30 novembre 2006 : Juris-Data, n° 2006-324185 ; CA Versailles, 9e ch. corr., 16 mars 2007 : Juris-Data n° 2007-331563*)

3.1.3 Viser une meilleure connaissance de l'ampleur du piratage.

Le piratage est une externalité économique négative[13], une nuisance préjudiciable à la collectivité. Il convient donc de mesurer, au moyen d'un indicateur pertinent et dynamique, l'ampleur réelle du phénomène et son évolution dans le temps. Cet indicateur mesurant, par échantillonnage, les volumes de téléchargements illicites de fichiers musicaux, audiovisuels et cinématographiques peut être aisément établi et actualisé quotidiennement. Il devrait être commandé par le ministère de la Culture et publié par lui au maximum trimestriellement, de préférence mensuellement. Il aurait une vertu informative et, éventuellement, dissuasive, si le constat de sa dérive conduisait les ayants droit et les pouvoirs publics à renforcer leur action. On introduirait ainsi une nécessaire culture du résultat dans la politique de désincitation à l'offre illégale.

Les mesures correspondantes permettraient en outre d'identifier les « parts de marché » des quatre grands fournisseurs d'accès à internet dans le piratage en pair-à-pair. Ces mesures peuvent être aisément complétées par des données issues des fournisseurs d'accès à eux mêmes sur l'utilisation de leur bande passante. Les informations issues des fournisseurs d'accès à internet pourraient être collectées et traitées par l'autorité qui pourrait être chargée de mettre en œuvre le dispositif d'avertissement et de sanction (cf supra).

3.2 Les professionnels de la musique, du cinéma et de l'audiovisuel doivent mieux s'organiser.

La mission considère qu'il incombe d'abord aux professionnels de la musique, du cinéma et de l'audiovisuel de se saisir des outils juridiques existants, qui peuvent être efficaces, et de développer les techniques pertinentes, de plus en plus nombreuses et utilisées à profit.

La mission a en effet constaté que le juge pénal ou de la responsabilité n'était que peu saisi, malgré l'ampleur de la méconnaissance constatée des droits de propriété. Par ailleurs, les dispositifs permettant de prévenir, dans des conditions d'urgence, l'utilisation d'un contenu sans autorisation des ayants droit sur des sites de mise à disposition étaient peu, voire pas, utilisés alors qu'ils peuvent déjà utilement servir à demander la suppression des contenus illégaux, ou même la fermeture temporaire des sites hébergeurs. Au demeurant, sur ce point, la mission a noté la volonté de coopération des principaux responsables des sites communautaires et de partage. Les plus importants de ces derniers mettent à disposition des formulaires en ligne permettant d'identifier facilement des oeuvres précisément recherchées, de signaler leur présence, et d'obtenir leur suppression dans un très bref délai. La mission estime qu'un tel système d'information, très réactif, gagnerait à être généralisé et qu'il incombe aux ayants droit concernés de négocier la généralisation de son insertion. Il serait d'autant plus utile que les oeuvres disposeraient d'un empreinte, et qu'un fichier commun – ou du moins un tiers de confiance « certificateur » – à tous les ayants droit existerait.

De manière générale, il paraît nécessaire que la réponse des professionnels de la musique, du cinéma et de l'audiovisuel soit mieux coordonnée. La situation actuelle est marquée par un éclatement des ayants droit qui est préjudiciable à la cohérence de la politique de lutte des professionnels contre l'offre illégale, et même à son efficacité. C'est pourquoi un organisme inter-professionnel réunissant les professionnels de la musique, du cinéma et de l'audiovisuel pourrait

[13] La notion d'externalité négative désigne une situation économique dans laquelle l'acte de consommation ou de production d'un agent a des conséquences négatives sur l'utilité des autres agents, sans que cette influence ne se traduise par une variation des prix.

être mis en place. Cette agence, émanation des sociétés de perception et de répartition des droits, pourrait ester en justice. Elle doit pouvoir en effet bénéficier de la nouvelle rédaction de l'article L. 331-2 du code de la propriété intellectuelle issue de l'article 33 de la loi du 29 octobre 2007 de lutte contre la contrefaçon[14].

Elle pourrait servir de levier :

- à une action concertée et lisible de la profession dans la lutte contre la contrefaçon numérique, la mission n'ayant pu que constater le très faible recours aux dispositifs légaux permettant de sanctionner les comportements de piratage, ou d'obtenir réparation ;

- à l'évaluation, au choix et à la promotion de technologies de marquage et de reconnaissance des contenus (*watermarking* et *fingerprinting)* communes, ou aussi convergentes que possibles, aux professions concernées, essentielles à la lutte contre le piratage numérique ;

De tels efforts des industries culturelles sont essentiels à la réussite sur le long terme d'une politique visant à désinciter l'offre et la consommation illégales.

3.3 Plusieurs dispositifs pourraient être mis en place.

3.3.1 Les dispositifs doivent pleinement prendre en compte l'état du droit et de la technique, ainsi que les attentes de la société.

Le piratage, qui fait intervenir un nombre important d'acteurs – internaute, hébergeur, éditeur de logiciel, ayant droit, etc... – sur un support dématérialisé où les inquiétudes relatives à la protection des libertés publiques sont fortes, est à la confluence de plusieurs régimes juridiques concurrents qui, s'ils sont justifiés, peuvent poursuivre des objectifs contradictoires. Ils rendent l'élaboration d'un dispositif de lutte délicate, de sorte que des solutions évoquées, lors des auditions ou dans une littérature désormais fournie, toutes ne sont pas envisageables.

Deux logiques fondamentales ont guidé le travail de la mission. Il n'est, d'une part, guère compatible avec les principes généraux du droit français de permettre la mise en place d'une justice privée, dans les mains des ayants droit ou des prestataires de services (hébergeurs et fournisseurs d'accès,...). D'autre part, la protection des personnes et des données doit être pleinement garantie. Les possibilités d'octroyer à des agents privés la possibilité de détenir et de traiter des fichiers personnels doivent ainsi être appréciées avec vigilance.

Plusieurs dispositifs, souvent évoqués, n'ont ainsi pas été retenus, soit parce qu'ils ne sont pas mûrs, soit parce qu'ils ne sont pas réalisables, pour des raisons juridiques ou d'acceptation sociale.

[14] Le nouvel article L. 331-2 du code de la propriété intellectuelle dispose que *« outre les procès-verbaux des officiers ou agents de police judiciaire, la preuve de la matérialité de toute infraction aux dispositions des livres Ier, II et III du présent code et de l'article 52 de la loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle peut résulter des constatations d'agents assermentés désignés selon les cas par le Centre national de la cinématographie, par les organismes de défense professionnelle visés à l'article L. 331-1 et par les sociétés mentionnées au titre II du présent livre. Ces agents sont agréés par le ministre chargé de la culture dans les conditions prévues par un décret en Conseil d'Etat. »*

3.3.1.1 Le filtrage.

La mise en place d'un dispositif de filtrage ou de contrôle des échanges par des radars est une proposition souvent avancée. Il convient toutefois de différencier plusieurs logiques, le filtrage pouvant porter soit sur des ports, des protocoles ou des sites tels les plate-formes d'hébergement et de partage de contenu, soit sur les fichiers circulant les réseaux.

A – Le filtrage de ports, de sites ou de protocoles.

Un filtrage peut déjà être juridiquement possible, dans certaines circonstances spécifiques. En effet, aux termes de l'article L. 336-1 du code de la propriété intellectuelle (article 27 de la loi dadvsi), le président du tribunal de grande instance, statuant en référé, peut ordonner sous astreinte toute mesure nécessaire à la protection du droit d'auteur et des droits voisins lorsqu'un logiciel est « principalement utilisé pour la mise à disposition illicite d'œuvres ou d'objets protégés »[15]. Par ailleurs, comme il a déjà été signalé, l'article 6-I-8 de la loi pour la confiance dans l'économie numérique ouvre aux ayants droit la possibilité de saisir l'autorité judiciaire pour prescrire en référé à un prestataire technique toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné, ce qui peut inclure, le cas échéant, un blocage d'accès à un site. La mise en oeuvre de ces dispositifs impliquent un recours systématique au juge.

De manière générale, la mission considère qu'un tel filtrage, s'il peut permettre une action ciblée efficace, doit servir de technologie d'appoint en raison des effets collatéraux qu'il peut induire, notamment de blocage éventuel d'échanges de contenus légaux. Elle s'est attelée à une analyse des avantages et des inconvénients des techniques disponibles (v. annexe).

B – Le filtrage des fichiers.

Les techniques de filtrage sur les plate-formes d'hébergement et de partage des œuvres numérisées (audio ou vidéo) sont d'ores et déjà utilisées. Elles permettent un filtrage en amont de la mise en ligne, et se développent au travers d'accords entre ayants droit et fournisseurs d'accès à internet. Leur utilisation devrait pouvoir être généralisée rapidement sans obstacle majeur puisque les déploiements s'opéreraient sur un nombre de sites par définition réduits. L'intérêt serait de freiner considérablement les mises à disposition illicites, et notamment celles des primo-diffuseurs. Pour cela, il conviendrait que les acteurs s'entendent sur le choix d'une technologie d'empreinte (ou d'un nombre réduit d'entre elles) et que les éditeurs et les ayants droit fassent effort pour fournir des sources permettant l'établissement des catalogues d'empreintes de référence aussi larges que possible, ce qui permettra aux ayants droit de fixer les conditions d'autorisation de circulation des œuvres sur les réseaux. Une telle orientation permettrait aussi de soutenir des entreprises innovantes françaises, très présentes sur les technologies en question, et de leur donner une bonne visibilité internationale sur un secteur porteur. Le contrôle des empreintes auprès de la base de référence pourrait être mutualisé, et par exemple confié à un « tiers de confiance », ce qui en réduirait les coûts et améliorerait l'efficacité.

Par ailleurs, s'agissant de filtrage des réseaux, le mécanisme reviendrait à installer des dispositifs permettant de filtrer des contenus de sorte à ne laisser circuler que les oeuvres dont les ayants droit ont autorisé la circulation, ou qui ne nécessitent pas d'autorisation, et de bloquer les produits circulant illégalement. Il s'agirait d'un filtrage en temps réel, directement chez le fournisseur d'accès à internet, et non sur le poste client. Sur le principe, il y aurait vérification du

[15] La formulation de cet article est toutefois d'une ambiguïté qui fait échec à sa pleine efficacité, dès lors qu'il est difficile d'établir le critère du caractère principal de l'usage aux fins de mise à disposition illicite d'œuvres protégées.

passage sur le réseau d'une oeuvre appartenant à un ayant droit (le plus souvent, au catalogue d'une société d'auteur), essentiellement au travers de son empreinte numérique. Cette même technique peut servir des finalités différentes : soit un filtrage de tête de réseau, à l'initiative des ayants droit et/ou des fournisseurs d'accès, qui bloquerait la circulation d'une oeuvre, soit un filtrage visant une répression a posteriori, avec intervention de la puissance publique.

a) Le filtrage préventif pour empêcher l'infraction.

La mission considère que le déploiement à large échelle des technologies actuelles de filtrage en amont, sur lesquelles elle s'est précisément penchée (v. annexe), mérite des approfondissements préalables. En effet, de nombreuses questions sont soulevées dès lors qu'il s'agirait de procéder à un déploiement relativement généralisé et donc lourd : quelle architecture (au cœur du réseau ou au plus près des nœuds de raccordement des internautes) ; quels coûts réels d'investissement et d'exploitation ; quel effet sur les comportements des internautes (chiffrement, techniques d'anonymisation…). Leur utilisation requiert donc une réflexion plus approfondie et une mobilisation des ayants droit.

b) Le filtrage répressif pour sanctionner l' infraction (radar).

L'utilisation des mécanismes de filtrage pour mettre en place ce que l'on appelle des « radars » surveillant la circulation d'oeuvres sans autorisation des ayants droit pour y appliquer une réponse pénale – sur le modèle de la lutte contre l'insécurité routière – soulève des questions importantes de protection des correspondances et de la vie privée. La mission considère qu'elle n'est pas encore de nature à être acceptée par l'opinion, inquiète d'une volonté de contrôle trop systématique des échanges sur les réseaux, qui sont avant tout des espaces de liberté.

3.3.1.2 Un système uniquement contractuel d'avertissement et de sanction.

Plusieurs pays étrangers, comme les Etats-Unis ou le Royaume-Uni, mettent en place un mécanisme d'avertissement et de sanction de nature uniquement contractuelle. Il consiste à ce que les fournisseurs d'accès à internet, saisis par les ayants droit d'actes susceptibles d'être de la contrefaçon, envoient dans un premier temps plusieurs messages d'information et, en cas de récidive, prennent une sanction, telle que la diminution provisoire de la bande passante, l'interruption de l'abonnement, voire sa résiliation. Le dispositif d'avertissement paraît, à l'usage, largement dissuasif pour les internautes qui reçoivent le message, des sanctions étant rarement prises. Il suppose, pour que cette efficacité désincite au piratage, qu'il soit mis en oeuvre sur une échelle suffisante.

Un tel dispositif, qui repose entièrement sur des acteurs privés et des obligations résultant des seuls contrats d'abonnement, est difficilement envisageable en droit français.

D'une part, il est difficile de trouver une base juridique à une sanction prise par le fournisseur d'accès sans intervention d'un juge ou d'une autorité publique, ni imposition d'une obligation légale. En effet, cette sanction ne pourrait être considérée comme une simple sanction contractuelle ; elle revêtirait un caractère pénal, dès lors qu'elle porterait sur une violation d'un droit de propriété. Or seul un juge est compétent pour constater et sanctionner une telle infraction. Surtout, l'acte de contrefaçon est en tant que tel étranger au contrat conclu entre l'internaute et le fournisseur d'accès, qui porte sur une fourniture technique et non sur le contenu auquel l'abonnement donne accès, ce que rappelle la loi pour la confiance dans l'économique numérique.

D'autre part, un dispositif de cette nature repose sur des fichiers d'infractions détenus par des personnes privées (à la fois les fournisseurs d'accès à internet et les ayants droit), ainsi que sur la possibilité pour ces dernières d'effectuer le rapprochement entre l'adresse IP et le nom du titulaire de l'abonnement sans que le juge n'intervienne. Or, outre le fait que pour l'instant la CNIL n'autorise que de manière restrictive la tenue par les ayants droit de fichiers de faits susceptibles de constituer des infractions, le Conseil constitutionnel (DC n° 2004-499 du 29 juillet 2004) a estimé, au regard des règles posées par l'actuel article 34-1 du code des postes et des communications électroniques, qu'il incombait au juge d'effectuer le rapprochement entre l'adresse IP et le nom du titulaire de l'abonnement.

Sur ce dernier point, le débat pourrait être ouvert par la question de savoir si une adresse IP est ou non une donnée (directement ou indirectement) personnelle. Les positions juridictionnelles sont encore divergentes. Si la réponse est positive, la mission considère que les obstacles juridiques sont difficilement surmontables (v. annexe). Si la réponse est négative, reste entière l'impossibilité de justifier d'une base juridique à l'imposition d'une sanction par le seul contrat, sans recourir à la loi.

Cela explique, dans les deux cas, qu'une voie uniquement contractuelle – c'est-à-dire sans modification législative – ne puisse être retenue.

3.3.2 Deux dispositifs pourraient être mis en place par les pouvoirs publics.

La mission estime que deux dispositifs sont envisageables par les pouvoirs publics. Ils ont chacun des atouts.

3.3.2.1 Une politique ciblée.

Il serait question de donner à la consommation de contenus culturels sur internet un cadre d'usage clair et légitime, fondé sur une information et un engagement de sanctions en cas de méconnaissance. Un tel dispositif reposerait sur des réponses ciblées en fonction tant des types de piratage (cf. 3.1.2) que des comportements des internautes. Il ne viserait donc pas les actes de récidive. Sa vertu première serait de rompre avec un traitement uniquement pénal, et d'adapter les sanctions à la nature des actes commis.

Le dispositif fonctionnerait en trois strates :

→ Une action large de communication à l'égard du public.

Les fournisseurs d'accès devront d'abord envoyer des messages généraux aux abonnés, tels que ceux exigés par l'article L. 336-2 du code de la propriété intellectuelle introduit par l'article 28 de la loi dadvsi du 1er août 2006[16], dont le décret d'application devrait désormais être rapidement pris.

Ils devront également envoyer des messages ciblés, à la demande des sociétés d'auteurs. Un tel dispositif d'information ciblée est possible sous réserve d'une éventuelle modification de l'article 34-1 du code des postes et des communications électroniques (même si l'envoi étant

[16] Cet article a introduit un article l'article L.336-2 du code de la propriété intellectuelle, qui prévoit que *«les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne adressent, à leurs frais, aux utilisateurs de cet accès des messages de sensibilisation aux dangers du téléchargement et de la mise à disposition illicites pour la création artistique. Un décret en Conseil d'État détermine les modalités de diffusion de ces messages».*

totalement automatique, on peut s'interroger sur la réalité de la conservation de données de connexion). Le système serait le suivant : les représentants des ayant droits relèveraient, comme ils sont déjà habilités à le faire, les coordonnées numériques des internautes contrevenants ; les fournisseurs d'accès à internet enverraient les messages. Ces derniers ne seraient pas toutefois pas à l'origine des messages d'information et d'avertissement sur les risques de sanctions, tant civiles que pénales, que les internautes encourent, mais uniquement les prestataires de l'information délivrée – même s'il y aurait mise en oeuvre d'un traitement, qui devrait donc être autorisé par la CNIL.

→ Une articulation des sanctions, fondée sur une pleine mobilisation tant des pouvoirs publics que des ayants droit.

Le ciblage doit ressortir d'une politique coordonnée de la profession, notamment pour la fixation des seuils, qui pourrait être prise en charge par une agence inter-professionnelle (cf. 3.2) ou par une autorité de régulation neutre et indépendante, telle que, par exemple, l'autorité de régulation des mesures techniques de protection déjà existante.

→ Les axes de cette politique reviendraient à ce que certains usages, tels que par exemple la consultation d'oeuvre en *streaming*, ne soient pas l'objet de sanctions. Les autres actes de représentation et de reproduction dont le rapport a fait état plus haut (cf. 3.1.2) seraient réprimés soit par une contravention, soit comme un délit, les sanctions les plus lourdes devant être réservées aux contrefaçons les plus graves (primo-partageurs, action de commerce, téléchargements massifs). La définition des sanctions appropriées nécessiterait la fixation par tous les acteurs d'une grille d'action.

Un tel dispositif nécessitera uniquement de prévoir que tous les actes de contrefaçon numérique ne soient pas également susceptibles d'être considérés comme un délit. A cet égard, compte tenu de la décision du Conseil constitutionnel relative à la loi dadvsi[17], il convient d'assurer l'égalité devant la sanction en ne fixant pas une règle qui discriminerait une technique spécifique. Il conviendra donc de fixer les contours de la contravention à partir de critères objectifs de criminologie et des concepts de référence de la propriété littéraire et artistique que sont la reproduction et la représentation.

3.3.2.2 Un mécanisme d'avertissement et de sanction.

La seconde solution envisageable consiste à mettre en place un mécanisme permettant d'avertir les internautes contrevenants et, le cas échéant, de les sanctionner, notamment par une suspension ou une rupture de leur contrat d'abonnement. Elle aurait une forte portée pédagogique, par l'envoi dissuasif de mises en demeure, et reposerait sur des sanctions proportionnées visant la répétition des mêmes actes.

La mise en oeuvre de ce mécanisme peut répondre à deux schémas généraux.

Le premier schéma est fondé sur l'intervention d'une autorité publique qui aurait pour mission d'avertir, après « plainte » des ayants droit, les internautes contrevenants et, le cas échéant, de les sanctionner elle-même – ou de transmettre le dossier au juge compétent pour qu'il décide de la sanction appropriée.

[17] Le Conseil constitutionnel a estimé que le fait de soustraire les seuls échanges de pair-à-pair de la qualification de délit méconnaissait le principe d'égalité, dès lors que cela ne reposait pas sur un critère objectif, l'outil technique étant insuffisant pour justifier une différence de traitement.

Le second schéma reposerait sur l'intervention directe – mais sous le contrôle du juge – des fournisseurs d'accès à internet pour sanctionner, après avertissements, les personnes ayant méconnu l'obligation légale de sécuriser leur poste informatique, une disposition législative fixant les conséquences de la violation de cette obligation.

Dans tous les cas, il paraît impératif à la mission que les juridictions spécialisées dans le droit de la propriété intellectuelle soient rapidement et effectivement mises en place. Leur développement est essentiel à l'efficacité de toute politique de désincitation de l'offre illégale.

3.3.2.2.1 Un mécanisme piloté par une autorité publique.

Cette autorité publique – qui, en fonction de son périmètre, pourrait être constituée à partir de l'extension des prérogatives de l'Autorité de régulation des mesures techniques de protection, la mission jugeant inopportun de créer une nouvelle autorité – aurait pour mission d'assurer la phase d'avertissement, soit avant de prononcer elle-même une sanction, soit en amont de l'intervention du juge.

A – L'autorité avertit le titulaire de l'abonnement et décide de la sanction à émettre en cas de répétition des mêmes actes.

L'autorité, saisie d'une plainte d'un ayant droit qui aurait constaté des actes de représentation et de mise à disposition de tiers d'œuvres sans autorisation des titulaires :

- ferait, sur la base – et après vérification – des informations recueillies par l'ayant droit, les réquisitions auprès des opérateurs pour identifier les auteurs de ces actes ;

- enverrait avant sanction, par l'intermédiaire des fournisseurs d'accès, une mise en demeure qui prendrait la forme d'un message électronique d'avertissement et de mise en garde au titulaire de l'abonnement ; en cas de répétition du même acte, elle enverrait une nouvelle mise en demeure par lettre recommandée ;

- en cas de constatation d'une seconde répétition, sur une période considérée et pour un volume à déterminer, prendrait une sanction[18] qui irait de la suspension temporaire à la résiliation du contrat ;

L'action de l'autorité visera à sanctionner le titulaire de l'abonnement pour avoir laissé poursuivre la commission, au moyen de son abonnement, d'actes illégaux de représentation et de mise à disposition de tiers d'œuvres protégées, et ainsi de ne pas avoir mis en oeuvre les moyens adéquats de sécurisation de son poste. Les poursuites intentées contre le titulaire de l'abonnement seraient alors fondées sur les principes posés à l'article L. 332-15 du code de la propriété intellectuelle introduit par la loi du 1er août 2006[19], qui devrait toutefois être modifié pour introduire des conditions plus précises, la portée impérative de cet article n'étant pas précisément

[18] Le pouvoir de sanction des autorités administrative est encadré par plusieurs exigences constitutionnelles. Cf. notamment DC, 96-378, 23 juillet 1996.

[19] L'actuel article L. 335-12 du code de la propriété intellectuelle dispose que *« le titulaire d'un accès à des services de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de reproduction ou de représentation d'oeuvres de l'esprit sans l'autorisation des titulaires des droits prévus aux livres I et II, lorsqu'elle est requise, en mettant en oeuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application du premier alinéa du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. »*

établie en l'état de sa rédaction, ainsi que certaines garanties permettant au titulaire de lever la présomption de responsabilité qui repose sur lui[20].

L'autorité prendra une sanction administrative distincte de la sanction pénale que l'auteur d'un acte de contrefaçon peut encourir[21]. La sanction pourrait être une sanction pécuniaire. Mais il paraît plus pertinent qu'il s'agisse de la suspension ou de la résiliation du contrat de l'abonné. A cet égard, il conviendra de régler l'articulation de l'activité de l'autorité avec les éventuelles poursuites pénales qui, à raison des mêmes faits, pourraient être intentées contre l'internaute contrevenant[22].

Le suivi de la procédure et la prise de la sanction requièrent qu'à un moment, les coordonnées numériques dont dispose l'autorité soient rapprochées du nom du titulaire de l'abonnement. En l'état actuel du droit, cela nécessite, ainsi que l'a précisé le Conseil constitutionnel dans sa réserve d'interprétation dans sa décision n° 2004-499 du 29 juillet 2004, une intervention du juge. On peut toutefois envisager une modification de l'actuel article 34-1 du code des postes et des communications électroniques – sur lequel le Conseil constitutionnel a fondé sa réserve d'interprétation – pour permettre à cette autorité publique d'opérer le rapprochement elle-même. Une telle modification paraît acceptable compte tenu des garanties d'indépendance et d'impartialité présentées par une autorité réunissant des agents dotés de prérogatives de puissance publique.

Par ailleurs, l'autorité devra être autorisée par la Commission nationale de l'informatique et des libertés à mettre en oeuvre des fichiers et une modification de l'article 34-1 du code des postes et des communications électroniques est également nécessaire pour l'autoriser à conserver, pour une durée définie, des données de connexion.

B – L'autorité assure l'avertissement et une médiation obligatoire en amont de l'intervention du juge, qui décidera de la sanction.

Dans ce cas, l'autorité assurerait[23] une phase obligatoire de médiation, qui prendrait la forme des mises en demeure opérées par message électronique et par lettre recommandée (la

---

[20] Il s'agira alors d'une responsabilité pour fait d'autrui, que l'on peut rencontrer dans de nombreux droits civils, mais aussi en matière pénale (v. par exemple DC *n°76- 70, 2 décembre 1976, rec. 39 in Les Grandes décisions du CC, 1999, p. 364, n° 25-16* ; *DC n° 99-411 du 16 juin 1999)* malgré l'affirmation du principe de personnalité de la peine – qui est applicable aux sanctions administratives (Conseil d'Etat, 29 octobre 2007, *LOSC Lille Metropole*, 307736). Eu égard à la nature matériellement civile des sanctions que l'autorité pourrait prononcer, la question de l'imputabilité se pose donc avec moins d'acuité, d'autant plus que l'obligation de sécurisation incombe bien directement au titulaire de l'abonnement. On notera d'ailleurs avec intérêt la décision de la Section du contentieux du Conseil d'Etat du 22 novembre 2000 *Société Crédit agricole Indosuez Chevreux, (Recueil Lebon, p.537, concl. A. Seban, chronique AJDA 2000.997)* qui s'inspire de l'idée, affirmée par le Conseil constitutionnel dans sa décision du 17 janvier 1989 relative au CSA (*DC n° 88-248, Rec p. 18, RFDA 1989, p. 215, note B. Genevois*), que les principes applicables en matière de répression n'ont pas la même portée qu'en droit pénal lorsqu'ils sont appliqués aux sanctions administratives, et que des aménagements sont par suite envisageables.

[21] Il n'y a donc pas de difficulté au regard la règle *non bis in idem* qui interdit de sanctionner deux fois une même personne, dans la mesure où les décisions de l'autorité et celles du juge pénal visent à sanctionner la violation de deux règles différentes du code de la propriété intellectuelle (défaut de sécurisation du poste ; acte de contrefaçon).

[22] V. notamment la question de l'articulation des ces pouvoirs avec les obligations résultant de l'article 40 du code de procédure pénale.

[23] Pour tous les actes de contrefaçon ou pour une partie seulement de ces actes, les plus graves pouvant être réservés à une sanction après une saisine directe du juge – ainsi, par exemple, de la mise à disposition (*upload*) massive : primo-partageurs ou actions de commerce.

même séquence que celle précédemment présentée). L'autorité serait alors un filtre obligatoire permettant de prévenir la répétition des mêmes actes.

A la différence du schéma précédent, elle ne prendra pas elle-même la sanction finale, qui restera du ressort du juge pénal – il devra s'agir d'une ou des juridictions spécialisées en propriété intellectuelle. Le juge ainsi saisi décidera de la sanction appropriée pour ces personnes qui auraient, malgré les avertissements, réitéré des actes illégaux. Sur ce point, une réflexion devrait être menée sur la nature de la peine. On devrait notamment prévoir qu'une des peines (accessoires) dont le juge peut disposer serait la suspension ou la résiliation du contrat d'abonnement[24]. Il pourrait aussi s'agir d'une amende contraventionnelle qui devrait être acquittée pour chaque acte de contrefaçon, ce qui pourrait conduire à des sanctions pécuniaires très fortes (v. annexe). Notons que le recours à des sanctions contraventionnelles ne priverait nullement les titulaires de droits de leur dédommagement, puisqu'ils pourront obtenir des dommages et intérêts du juge de proximité statuant par ordonnance pénale en application de l'article 528-2 du code de procédure pénale, mais aussi se constituer partie civile devant le tribunal correctionnel ou devant le tribunal de police.

Il sera également nécessaire d'autoriser l'autorité à faire le rapprochement entre les données de connexion et le titulaire de l'abonnement sans intervention du juge, ainsi que de conserver des données de connexion (cf. supra).

Quel que soit le schéma adopté, la procédure suivie devant l'autorité sera écrite et contradictoire, de sorte que l'internaute puisse assurer sa défense. Ses décisions seront susceptibles de recours devant une juridiction.

L'autorité devra également disposer du pouvoir d'enjoindre, avec astreinte si nécessaire, aux fournisseurs d'accès de respecter leurs obligations de transmission des messages d'avertissement et de mise en garde.

Il devrait également être envisagé que cette autorité, saisie par des ayants droit, dispose de la capacité d'exiger des prestataires techniques (hébergeurs, fournisseurs d'accès,...) toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication en ligne, à la place de la voie judiciaire actuellement ouverte par certaines des dispositions de l'article 6 de la loi pour la confiance dans l'économie numérique[25]. La décision que l'autorité prendrait dans ce domaine serait elle-même contrôlée par un juge.

Dans le même ordre d'idée, l'autorité devrait avoir une activité de régulation, par l'émission de guides de bonnes pratiques ou d'information des internautes sur les usages et les mécanismes de sécurisation. Elle pourrait aussi, sous réserver de l'avis de la Commission

---

[24] On soulignera que, bien qu'une telle peine ne soit pour l'instant pas expressément prévue par les textes, de nombreux juges pénaux, qui disposent du choix de l'opportunité de la peine, en ont d'ores et déjà disposé.

[25] Il s'agit ici de la prévention d'un dommage, et non de la sanction d'un acte de contrefaçon. Un tel pouvoir de régulation peut ressortir du juge, comme c'est le cas actuellement, mais également d'une autorité administrative, dès lors qu'il ne s'agit aucunement d'un pouvoir de sanction pénale qui, lui, ne pourrait revenir qu'à un juge. Sur le plan juridique, c'est une logique similaire, au regard de la directive 2000/31/CE du 8 janvier 2000 et de la loi n° 2004-575, à celle qui conduirait à l'instauration d'un filtre, dont la mission considère (v. annexe), que sa mise en oeuvre peut être légalement imposée par un juge ou une autorité publique.

nationale de l'informatique et des libertés, disposer d'un fichier des personnes dont le contrat a été résilié.

On précisera enfin que, quels que soient le schéma et les réformes législatives à opérer, ces procédures peuvent être mises en place facilement, car elles sont automatisables et que l'autorité sera à même de décider de la volumétrie de son action en fonction des moyens que les pouvoirs publics pourront rendre disponibles.

3.3.2.2.2 Un mécanisme résultant d'une obligation légale.

Ce dispositif reposerait sur une séquence d'avertissement et de sanction similaire à celle présentée dans le cadre de l'autorité, mais serait mis en oeuvre directement par les fournisseurs d'accès à internet. Il reposerait non sur une modification des contrats entre ces derniers et leurs abonnés (cf. 3.3.1.2) mais sur l'obligation légale de sécurisation du poste posée par l'article L. 335-12 du code de la propriété intellectuelle – dont la rédaction actuelle devrait, comme il a été dit plus haut, être revue. La loi imposerait aux fournisseurs d'accès de suspendre[26] et, en cas de récidive, de résilier le contrat d'abonnement du titulaire contrevenant à l'article L. 335-12 du code de la propriété intellectuelle. La contestation de la décision de suspension ou de résiliation se ferait devant une des juridictions spécialisées dans la propriété intellectuelle appelée à se mettre en place.

Ce mécanisme n'est, à vrai dire, envisageable que si une disposition législative circonstanciée vient préciser que les adresses IP recueillies et stockées par les ayants droit et les fournisseurs d'accès ne constituent pas des données directement ou indirectement nominatives. Dès lors les fichiers détenus par les ayants droit et les fournisseurs d'accès pourraient être mis en oeuvre sans autorisation de la CNIL. La mission a en effet eu l'occasion de préciser (cf. supra 3.3.1.2) que dans le cas contraire, les modifications législatives à envisager paraissent délicates (v. annexe, également). Mais il ne paraît pas impossible pour le législateur de déterminer lui-même la nature juridique d'une adresse IP. Toutefois, une telle évolution doit être appréciée avec prudence, en raison de son impact qui dépasse la question de la lutte contre la contrefaçon numérique. C'est en effet, de manière plus globale, les question essentielles du choix par les autorités publiques des outils de régulation de l'internet et de la protection des données personnelles sur les réseaux. A cet égard, on rappellera que la France entend organiser, dans le cadre de la présidence à venir de l'Union européenne, une réunion des commissions nationales traitant de la protection des données personnelles.

[26] Un fournisseur d'accès ne remplissant pas cette obligation d'envoi de message et de sanction pourrait être l'objet de sanctions pénales et financières ; un juge pourrait être saisi par les ayants droit.

CONCLUSION

Dans le domaine de la lutte contre la contrefaçon numérique, la mission considère qu'il existe des mesures à la fois efficaces et respectueuses des libertés individuelles. Pour être conformes aux principes du droit français, elles doivent cependant être différentes dans leur expression des mécanismes que des pays étrangers ont pu instituer, ou sont en train d'instituer.

La mise en place d'une politique ciblée, et plus encore, du mécanisme d'avertissement et de sanction constituerait un choix politique fort, car elle est coûteuse pour l'Etat, qui s'engagerait ici dans une action volontariste et spécialisée. Elle ne paraît à la mission envisageable que si les professionnels des industries concernées s'engagent, en parallèle, d'abord à saisir les leviers déjà existants et à s'organiser dans ce but et ensuite à permettre une amélioration rapide des conditions de l'offre légale.

RECOMMANDATIONS DE LA MISSION

1. Ramener la fenêtre VOD de 7 mois et demi après la sortie en salle à 4 mois. A cette occasion, les professionnels du cinéma analyseront l'impact d'une telle mesure sur chacun des acteurs économiques de la production et de la distribution et réexamineront si nécessaire les mécanismes de financement du cinéma.

2. Aussi longtemps que les mesures techniques de protection (DRM) font obstacle à l'interopérabilité, abandonner ces mesures sur tous les catalogues de musique.

3. Subordonner les aides à la production du Centre national de la cinématographie à l'engagement que le film soit rendu disponible en VOD.

4. Généraliser le taux de TVA réduit à tous les produits et services culturels, cette baisse étant intégralement répercutée dans le prix public.

5. Dans le cas où cette baisse serait obtenue, élargir l'assiette des abonnements internet « triple play » soumis au taux réduit en contrepartie de l'institution d'une taxe alimentant des fonds de financement de la création et de la diversité musicales comme cela a été fait pour le cinéma.

6. Publier un indicateur de piratage tenu par les pouvoirs publics, au maximum trimestriellement, de préférence mensuellement.

7. Regrouper les ayants-droit en un agence unique chargée de lutter globalement contre le piratage et de favoriser l'évaluation, le choix et la promotion de technologies, communes ou convergentes, de marquage et de reconnaissance des contenus.

8. Généraliser les techniques de filtrage des contenus pirates par accord avec les ayants droit sur les plate-formes d'hébergement et de partage des œuvres numérisées grâce au choix d'une technologie d'empreinte (ou d'un nombre réduit d'entre elles), qui trouverait sa pleine utilité si éditeurs et ayants droit fournissent les sources permettant l'établissement de larges catalogues d'empreintes de référence.

9. Expérimenter les techniques de filtrage des fichiers pirates en tête des réseaux par les fournisseurs d'accès à internet et les généraliser si elles se révèlent efficaces.

10. Simplifier et clarifier la circulaire adressée au Parquet pour l'application de la loi dadvsi pour favoriser une application plus effective de la loi.

11. Prendre le décret déterminant des juridictions spécialisées dans la lutte contre la contrefaçon numérique, ainsi que celui prévu par l'article L. 336-2 du code de la propriété intellectuelle relatif aux modalités de diffusion de messages envoyés par les fournisseurs d'accès pour sensibiliser les internautes.

12. La Commission nationale de l'informatique et des libertés doit tirer les conséquences de l'arrêt du 23 mai 2007 du Conseil d'Etat annulant sa décision du 18 octobre 2005 refusant à diverses sociétés d'auteur l'autorisation nécessaire à la mise en place d'un fichier permettant la recherche et de la constatation des actes de contrefaçon sur Internet.

13. Mettre en place soit une politique ciblée de poursuites, soit un mécanisme d'avertissement et de sanction allant jusqu'à la suspension et la résiliation du contrat d'abonnement, ce mécanisme s'appliquant à tous les fournisseurs d'accès à internet. Il peut nécessiter la mise en place d'une autorité indépendante.

ANNEXE 1 : FICHES TECHNIQUES ET JURIDIQUES

CONSIDERATIONS TECHNIQUES

1. – La lutte contre les téléchargements illicites peut faire appel à plusieurs approches s'appuyant sur des outils techniques existants mais dont les performances réelles restent encore à évaluer en cas de déploiement à grande échelle.

De nombreux outils existent ou sont en cours de développement (cf. rapport). Différents dans leur approche et donc dans leurs performances et limitations, ils sont proposés par plusieurs sociétés dont un certain nombre de groupes industriels ou de PME innovantes françaises.

Les présents développements visent à présenter les caractéristiques des outils techniques existants et les limites de chacun.

1.1 – Les outils de filtrage par les FAI.

Ils ont pour finalité principale la détection dans des cas prédéterminés, et, le cas échéant, le blocage, de l'accès de l'internaute soit à des URL ou des adresses IP, soit à certains ports, soit à certains protocoles, soit, enfin, à certains contenus. Le filtrage peut aussi permettre de recueillir les adresses IP des émetteurs et/ou des destinataires des flux litigieux :

- ***le filtrage d'URL ou d'adresse IP*** impose de repérer préalablement les adresses à bloquer ce qui nécessite une analyse des flux en temps réel et une grande réactivité de traitement. De tels systèmes sont déjà mis en œuvre pour bloquer sur demande judiciaire l'accès à des sites interdits *(apologie de crimes contre l'humanité, pédophilie…)*.

  Limites :

  - ce type de filtrage, déjà pratiqué par les FAI à une échelle réduite pour les sites interdits, bloque en général et dans la pratique l'accès à l'ensemble d'un serveur pouvant contenir bien d'autres éléments que le contenu illicite identifié ; la généralisation d'un tel mode de filtrage dans le cadre de la lutte contre le téléchargement illicite poserait de ce point de vue un problème de responsabilité aux FAI ;
  - le blocage d'URL ou d'adresses IP nécessite une surveillance constante du net car il est toujours possible de modifier une adresse IP ou une URL bloquée.

- ***le filtrage de ports*** : les services P2P utilisent des ports clairement identifiés qu'il est possible de bloquer ; le filtrage de ports est possible sur tous les routeurs utilisés par les opérateurs *(Cisco, Juniper, Extreme, Etwork, Foundry…)*

  Limites :

  - le blocage de port entraîne le blocage de tous les usages du port, y compris les usages égaux ;
  - ce type de filtrage n'est efficace qu'à court terme, les utilisateurs ayant la possibilité de contourner les mesures de filtrage en modifiant les ports initialement choisis par les éditeurs de P2P.

- ***le filtrage de protocoles*** : ces outils permettent de bloquer certains types d'échanges à partir du repérage des règles qui les régissent voire de leur comportement ; des outils existent sur le

marché comme Netenforcer d'Allot, PacketShaper de Packeteer, P-Cube ou NBAR de Cisco, IP-engines d'Ipanema…

Limites :

- le filtrage de protocole va bloquer également les usages légaux du protocole (dans le domaine de la R&D, le P2P permet la mise en commun de ressources technologiques comme la puissance de calcul et la bande passante, le P2P est également utilisé par des sociétés commerciales pour la distribution légale et contrôlée des contenus protégés par le droit d'auteur comme des démonstrations de jeux, de logiciels, des bandes annonces, des mises à jours de logiciels, etc…) ;
- le filtrage de protocole permet de bloquer les téléchargements illicites utilisant le P2P, mais le P2P n'est plus la seule voie de téléchargement illicite de contenus depuis le développement des « news groups » et des sites de partage vidéo dont le succès va croissant.

- ***le filtrage de contenus*** : il s'agit de déceler, et de pouvoir bloquer si elles sont utilisées de façon illicite, des données préalablement marquées lorsqu'elles transitent sur les réseaux. Le filtrage de contenus peut s'appuyer, d'une part, sur des techniques de tatouage numérique, qui consistent à vérifier une marque inscrite préalablement à l'intérieur d'un document et contenant des informations de copyright ou d'autres messages de vérification, ou, d'autre part, sur des techniques d'empreintes numériques, qui consistent à calculer un condensat numérique d'un document et à le comparer à une base de données d'empreintes numériques de référence *(voir infra 2ème approche, pour l'analyse des outils de reconnaissance de contenus multimédia).*

  Limites :

  - les bases d'empreintes sont par nature très volumineuses et il paraît difficile de les installer à tous les nœuds du réseau d'un FAI ; de plus, elles sont développées dans des formats propriétaires par plusieurs sociétés concurrentes auxquelles les ayants droit ont la possibilité de recourir indifféremment ;
  - les techniques de reconnaissance de contenu multimédia développées jusqu'ici ont au mieux été testées et mises en œuvre au niveau de serveurs fermés sans comparaison d'échelle avec les réseaux ouverts exploités par les FAI ; le déploiement à grande échelle des systèmes de filtrage de contenus soulèvent des questions qui restent à étudier en termes de coût, d'architecture technique et d'impact sur le comportement des internautes ;
  - la mise en œuvre de filtrage par les contenus au niveau des FAI risquerait de susciter, surtout de la part des fraudeurs organisés, des stratégies de contournement, parfois d'ailleurs déjà activables sur certains logiciels de P2P comme le recours au chiffrement ou aux techniques « d'anonymisation » d'adresse IP ;
  - il convient d'examiner dans quelle mesure le filtrage des contenus par les FAI est compatible avec le cadre juridique dans lequel opèrent actuellement les FAI, un débat européen sur la question du filtrage pouvant être ouvert à l'occasion du prochain « paquet télécom » entant que de besoin.

Tous les mécanismes de filtrage décrits ci-dessus peuvent être mis en place en différents points du réseau par les fournisseurs d'accès internet *(FAI).* Ils peuvent procéder soit à une analyse exhaustive des flux, soit à une analyse par sondage, selon leurs performances.

Le point d'implantation du filtrage n'est pas neutre. Si le filtrage est effectué dans le cœur de réseau du FAI, les volumes à traiter sont très importants et aucune sonde ne permet à ce jour le filtrage d'un flux de plusieurs gigabits. Par ailleurs, dans ce cas, la partie du trafic « local » qui ne passe pas toujours par le cœur du réseau risque d'échapper au filtrage. Si le filtrage est mis en place au niveau des nœuds élémentaires des réseaux, le nombre d'équipements à installer s'avère considérable. Dans tous les cas, et même si les estimations sont très variables, les coûts de mise en place d'un système de filtrage par les FAI seront élevés aussi bien en investissement qu'en exploitation.

Il est également possible d'envisager l'installation d'un système de filtrage sur le poste de l'abonné à son initiative à l'image de ce qui se fait en matière de contrôle parental. Dans cette hypothèse, l'efficacité sur la fraude consciente est par essence limitée puisque le déclenchement des instruments de filtrage est provoqué à l'initiative de l'abonné. Néanmoins, l'effet global sur la fraude peut être important, notamment dans le cadre d'une prise de conscience parentale.

Les mécanismes de filtrage par les FAI peuvent donc s'appuyer sur un certain nombre de technologies innovantes prometteuses, récemment développées, qui n'ont cependant pas encore atteint le stade de leur pleine maturité. En conséquence, il est difficile d'évaluer leur efficacité réelle dans le cadre d'un déploiement « grandeur nature », tant à court terme, du fait des incertitudes soulevées par le changement d'échelle, qu'à moyen terme, du fait des possibilités non négligeables de contournement.

Dans ce contexte, il conviendrait de recourir à des expérimentations préalables et à une évaluation objective des coûts de déploiement et d'exploitation des différentes solutions au regard des performances attendues, avant d'envisager un déploiement à large échelle ou le choix d'un fournisseur de solution plutôt qu'un autre.

1.2 – Les outils de filtrage par les hébergeurs ou les éditeurs de services.

Ils ont pour objectifs d'empêcher, ou au moins de limiter, la mise en ligne de contenus protégés par des tiers non détenteurs de droits.

Les ayants droit ont tout intérêt à repérer les contenus protégés circulant sur les sites de partage vidéo ou les « news groups » pour pouvoir engager des procédures à des fins préventives ou répressives.

Ainsi, et de plus en plus, les gestionnaires de sites de partage de vidéo cherchent à recourir, en liaison avec les ayants droit, à des systèmes automatisés de reconnaissance de contenus qui sont mis en œuvre en amont par l'hébergeur au moment de la demande de mise en ligne par l'internaute *(upload),* afin de bloquer l'opération si elle porte sur des contenus protégés.

Les systèmes correspondants utilisent des outils de reconnaissance de contenu multimédia qui peuvent être soit :

- **des outils se fondant sur les empreintes numériques** *(« fingerprint »)* : ils consistent à calculer, à partir de son contenu, l'empreinte *(c'est à dire un condensé numérique caractéristique)* d'un document circulant sur le réseau et à la comparer à une base de données d'empreintes numériques de référence. Ces outils sont mis en œuvre par des sociétés comme l'INA, Advestigo, Audible Magic, LTU technologies,… La fiabilité de tels

systèmes dépend de la richesse de la base de données sur laquelle ils s'appuient et sur leur robustesse aux modifications, aux changements de format, à la compression des oeuvres;

- **des outils se fondant sur le tatouage numérique** *(« watermarking »)* : le système de tatouage numérique nécessite que le document ait été marqué préalablement à sa diffusion par les ayants droit avec des données contenant des informations de copyright ou d'autres messages de vérification. Ce type de solution est développé, par exemple, par Thomson, Communications SA ou Vivacode. Il s'agit ensuite de rechercher et d'analyser la marque inscrite à l'intérieur d'un document circulant sur le réseau et de s'assurer que la version ainsi identifiée est bien autorisée pour la transaction où elle est décelée . Les tatouages doivent être les plus résistants possibles aux attaques sans qu'une résistance absolue ne puisse jamais être garantie.

Les outils d'empreinte numérique comme les outils de tatouage ont des formats propriétaires appartenant à chacune des sociétés qui les développent.

Même si les outils de reconnaissance de contenus multimédia présentent des limites techniques, leur intérêt pour limiter le téléchargement illégal par la voie des sites de partage vidéo est réel et tout accord entre les gestionnaires de ces sites et les ayants droit tendant à la généralisation de leur utilisation est à encourager.

1.3 – Le repérage des flux illicites par l'observation externe.

Des outils existent et sont déjà mis en œuvre par certains ayants droit pour détecter la circulation sur les réseaux de contenus protégés préalablement ciblés.

Il s'agit en fait de simulateurs de clients P2P qui se positionnent comme n'importe quel usager des réseaux pour observer les flux circulant sur le P2P, en vérifier le contenu et repérer ainsi les flux illicites à partir d'une cible de surveillance définie préalablement par l'industrie du contenu.

S'agissant du repérage des téléchargeurs, la détection des téléchargements illicites par les ayants droit nécessite l'identification préalable des fichiers contrefaits. Ensuite, les outils mis à disposition des ayants droit par différentes sociétés *(comme CoPeerRight Agency, Advestigo en France mais aussi BayTSP, Safenet et Mediadefender aux Etats-Unis)* permettent d'enregistrer, par exemple chaque seconde, les utilisateurs qui téléchargent ou mettent en partage ces fichiers. Ceci peut permettre également de mesurer le nombre de téléchargements partiels ou complets de ces fichiers contrefaits et le manque à gagner pour les ayants droit.

En ce qui concerne les données relatives à l'internaute enregistrées par ces systèmes et pouvant être utilisées à des fins probantes, il est possible de repérer que telle adresse IP a terminé son téléchargement à telle date, heure et minute.

L'association de l'adresse IP avec l'identité de l'internaute nécessite ensuite de recourir aux FAI. Les adresses IP ainsi enregistrées peuvent également être utilisées pour adresser des messages ou des contraventions. Il convient de signaler que le rapprochement de l'adresse IP et de l'identité du contrevenant présumé n'est pas toujours assurée *(cas du WiFi ou des réseaux d'entreprise, recours à des techniques de masquage d'adresses IP).*

Certaines sociétés comme CoPeerRight Agency ont développé des outils destinés à

rechercher plus spécifiquement les primo-diffuseurs. Un outil de ce type est mis en œuvre par le Syndicat des éditeurs de logiciels de loisirs *(SELL)* dans le domaine des jeux vidéo, dans le cadre d'une procédure automatisée validée par la CNIL en mars 2005. L'outil simule la recherche de fichiers illicites à télécharger à partir de mots-clés et lance des recherches chaque seconde sur les différents réseaux P2P. Dès qu'un fichier arrive sur les réseaux, sont enregistrées, d'une part, les caractéristiques du fichier *(nom, taille, compression format, signature...)* et, d'autre part, les caractéristiques du premier diffuseur *(date, heure, adresse IP du terminal utilisateur, nom pseudo, logiciel utilisé, protocole utilisé, adresse du serveur dans le cas des réseaux centralisés, userhash...).*

Les systèmes d'observation externe se fondent sur le caractère ouvert des réseaux P2P. Mais, si les conséquences de l'observation en terme de sanction augmentent, il est probable que le recours au chiffrement progressera ce qui pourrait réduire la portée de ces mécanismes, voire les rendre inopérants. Par ailleurs, les réseaux P2P ont tendance à évoluer vers des « réseaux d'amis » où ne sont admis que les participants identifiés par le groupe ce qui rend impossible l'observation « cachée » des réseaux P2P actuellement pratiquée.

Malgré ces limites, l'observation externe des flux illicites reste un bon moyen pour traquer les primo-diffuseurs dans un cadre d'une recherche délictuelle de contrefaçon, en axant les investigations sur les cibles prioritaires souhaitées par les ayants droit. En dehors de ce cas, ces solutions n'ont d'intérêt direct dans la lutte contre le téléchargement illégal que s'il est mis en place en aval un système d'alerte et/ou de sanction.

2. – Si aucune des propositions techniques existantes n'est en mesure d'apporter une solution immédiate et globale au problème du téléchargement illicite, leur mise en œuvre progressive peut permettre des progrès sensibles dans la lutte contre le piratage et participer à la construction d'un nouveau système de gestion des droits numériques associant tous les acteurs concernés.

Les techniques de reconnaissance des oeuvres numérisées peuvent s'appliquer indifféremment à toutes les sortes de contenus numériques : jeux, musique, cinéma, logiciels… Elles peuvent servir aussi bien à repérer les usages illicites, provoquant le déclenchement d'un processus d'alerte et de sanction adéquat, qu'à développer des outils statistiques servant à la répartition des droits ou à mesurer les évolutions dans les volumes à traiter et la nature des offres.

Les outils techniques peuvent permettre de repenser le système de gestion des droits numériques dans le sens de l'efficacité :

- amélioration des capacités d'investigation pour rechercher les primo-diffuseurs et engager les poursuites quel que soit le contenu numérique contrefait ; il semble en effet tout aussi essentiel de s'attaquer à la recherche et à la sanction des primo-diffuseurs qu'à la désincitation des internautes ; sur ce point, il est utile de rappeler que la réglementation française existante permet déjà en l'état de repérer des téléchargements illicites et de porter plainte pour contrefaçon ou atteinte au droit d'auteur et ce sans outil technique nouveau à développer ;

- amélioration de la traçabilité des œuvres permettant d'envisager de nouvelles méthodes de « monétisation » des contenus, notamment par la publicité ; de ce point de vue, un système de marquage de l'ensemble des contenus numériques par des métadonnées robustes *(portant entre autres sujets, sur l'origine de l'oeuvre, son régime juridique…),* dans un cadre si possible standardisé et en dehors de toute intention de filtrage ou de sanction

pour éviter le recours à des solutions de contournement, serait de nature, a minima, à préserver le droit moral des ayants droit par un effet pédagogique auprès des utilisateurs, mais aussi à donner une base solide au calcul de répartition des droits dans le cadre d'un modèle économique rénové.

Sur ce dernier point, il est utile de rappeler que la réglementation française existante permet déjà en l'état de repérer des téléchargements illicites et de porter plainte pour contrefaçon ou atteinte au droit d'auteur et ce sans outil technique nouveau à développer.

QUESTIONS JURIDIQUES AUTOUR D'UN MECANISME D'AVERTISSEMENT ET DE SANCTION

La mise en oeuvre d'un mécanisme d'avertissement et de sanction pose des questions délicates de protection des données personnelles.

Toute réforme est contrainte par une série de jurisprudences. Par une décision n° 2004-499 du 29 juillet 2004, le Conseil constitutionnel a accepté le principe de l'élargissement aux sociétés de perception et de répartition des droits d'auteur des compétences de l'article 9 de la loi n° 78-17 du 6 janvier 1978 sous deux réserves d'interprétation. Deux garanties lui paraissaient en effet être apportées : l'intervention de la Commission nationale de l'informatique et des libertés, en vertu de l'article 25 de la loi n° 78-17 du 6 janvier 1978 et l'assurance qu'en application de l'article 34-1 du code des postes et des communications électroniques, les informations disponibles seront mises à la disposition d'un juge qui effectuera le rapprochement entre l'adresse IP et le nom de l'internaute.

C'est notamment sur le fondement de cette réserve d'interprétation que la Commission nationale de l'informatique et des libertés a refusé à diverses sociétés d'auteur l'autorisation nécessaire à la mise en place d'un dispositif permettant l'envoi, par l'intermédiaire des fournisseurs d'accès à internet, de messages visant des internautes contrefacteurs. Cette décision du 18 octobre 2005 a été annulée le 23 mai 2007 par le Conseil d'Etat. Ce dernier a considéré que la surveillance des réseaux – autorisée par la loi – n'était pas, contrairement à ce qu'estimait l'autorité administrative, disproportionnée au but légitime qui était poursuivi. Il a en revanche confirmé l'appréciation de la commission sur les autres points, au regard du droit existant.

Ces deux décisions du Conseil constitutionnel et du Conseil d'Etat, qui sont centrales aux débats, posent des règles importantes. Les deux hautes juridictions se sont toutefois également prononcées à droit constant. A cet égard, la décision du Conseil d'Etat a seulement pris acte des impossibilités juridiques actuelles, en confirmant la CNIL sur ce point, sans se prononcer sur leur pertinence. Par ailleurs, le Conseil constitutionnel a émis une réserve d'interprétation fondée sur la rédaction actuelle de l'article 34-1 du code des postes et communications électroniques, sans pour autant établir de principe.

Sur ces bases, deux approches sont possibles.

On peut d'abord considérer que les adresses IP ne sont pas des données à caractère, direct ou indirect, nominatives. C'est en ce sens que certaines juridictions se sont prononcées (v. Cour d'appel de Paris, décisions du 27 avril et du 15 mai 2007[27]). Dans ce cas, ayants droit comme fournisseurs d'accès à internet peuvent mettre en oeuvre des fichiers permettant d'avertir les internautes contrevenants sans autorisation de la CNIL, dès lors que ces fichiers sortent du champ d'application de la loi n° 78-17. Une disposition législative précisément écrite en ce sens pourrait permettre de fixer la nature de l'adresse IP, et partant une mise en oeuvre du dispositif d'avertissement et de sanction sans intervention d'une autorité publique. Cette démarche pourrait être de nature à lever le sens des réserves d'interprétation soulevées par le Conseil constitutionnel dans sa décision DC n° 2004-499 du 29 juillet 2004

On peut aussi estimer, comme la CNIL (v. communication du 2 août 2007) et d'autres juridictions (par exemple : tribunal correctionnel de Saint-Brieuc, 6 septembre 2007) – ainsi que

[27] contre lesquels, il est important de le préciser, des recours dans l'intérêt de la loi ont été introduits devant la Cour de cassation.

les travaux du groupe de travail dit groupe 29[28] – que les adresses IP constituent des données indirectement nominatives et qu'ainsi des fichiers les traitant doivent être préalablement autorisés, au terme de l'article 25 de la loi n° 78-17. Dès lors, la mise en oeuvre du mécanisme d'avertissement et de sanction nécessiterait deux réformes législatives importantes :

- Modifier l'article 34-1 du code des postes et des communications électroniques pour autoriser les fournisseurs d'accès à conserver, pendant un délai limité, des données de connexion relative au trafic ;

- Modifier l'article 9 de la loi n° 78-17 pour autoriser les fournisseurs d'accès à internet à constituer un fichier et à conserver des données nominatives ;

Certains arguments peuvent militer dans le sens d'une évolution de ces deux textes.

- En premier lieu, l'envoi de messages purement informatif par les sociétés d'auteur, les fournisseurs d'accès servant alors de prestataires, aurait un rôle de prévention qui est expressément couvert par la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui prévoit comme exception la prévention d'infractions pénales ; la loi française, qui doit être lue au regard de cette directive qu'elle transcrit, ne paraît ainsi pas pouvoir être interprétée comme excluant cette finalité ;

- En second lieu, le Conseil constitutionnel, dans sa décision n° 2004-499 du 29 juillet 2004, a considéré que la lutte contre les pratiques de contrefaçon qui se développent sur le réseau internet, qui passe par la sauvegarde de la propriété intellectuelle et de la création culturelle, constituait un motif d'intérêt général ;

Pour autant, force est de constater que l'ouverture des possibilités offertes par l'article 9 de la loi n° 78-17 a été acceptée avec réserve par le Conseil constitutionnel en 2004 – qui a par ailleurs annulé, pour manque de précision, la rédaction envisagée du 4° de l'article 9 de la loi du 6 janvier 1978 ouvrant la possibilité aux ayants droit de la création culturelle de mutualiser la lutte contre le piratage des oeuvres en constituant des fichiers de « données de connexion » – et que l'article 34-1 du code des postes et communications électroniques pose comme principe fondamental l'effacement des données de connexion, la possibilité de leur conservation devant demeurer exceptionnelle. Des modifications parallèles de ces deux textes au profit de personnes privées paraissent ainsi à la mission délicate. Il ne lui semble pas qu'elles puissent être suffisamment encadrées et proportionnées pour qu'elles soient considérées comme étant de nature à assurer, entre les respect de la vie privée et les autres droits et libertés, notamment le droit de propriété, un juste équilibre.

En revanche, comme il est dit dans le rapport, la seule modification de l'article 34-1[29] au profit d'une autorité publique lui paraît possible, au regard des garanties d'impartialité d'une telle autorité.

---

[28] Le groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2000/58/CE.

[29] Dans le cas d'une autorité publique, une modification supplémentaire de l'article 9 de la loi n°78-17 n'est pas nécessaire. Le fichier devra toutefois être autorisé par la CNIL.

LE FILTRAGE

L'usage de filtres paraît envisageable au regard des engagements européens de la France et du droit national, s'il est ciblé et mis en oeuvre par une autorité publique, ou contrôlé par un juge.

D'une part, l'article 6-I-7 de la loi n° 2004-575 du 21 juin 2004 de confiance dans l'économie numérique précise que les fournisseurs d'accès à internet ne sont pas soumis à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites ; c'est une reprise de l'article 15 de la directive 2000/31/CE du 8 janvier 2000 relative au commerce électronique. D'autre part, l'article L. 32-3-3 du code des postes et communications électroniques, issu de l'article 9 de la loi sur l'économie numérique (article 14 de la directive de 2000), prévoit également une absence de responsabilité tant civile que pénale à raison des contenus transmis par les fournisseurs d'accès à internet ou les hébergeurs, sauf s'ils agissent sur le contenu illicite.

Certains commentateurs tendent à considérer que l'article 15 de la directive de 2000, dans la mesure où elle interdit que soit imposée une « obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites » exclurait que les fournisseurs d'accès à internet puissent placer des filtres. On pourrait certes solliciter de la Commission une communication interprétative sur ce point, compte tenu de la rédaction de l'article de la directive.

Pourtant, la mission pense que ces dispositions doivent être lues au regard de leur objectif : elles concernent les modalités d'engagement de la responsabilité des prestataires de service, et s'adressent donc au juge de la responsabilité qui estimera l'existence ou non de dommages pouvant être réparés. Les principes de la loi de 2004, reprenant ceux de la directive, visent à éviter que le juge national déduise une faute du prestataire du fait de la simple présence sur ses réseaux d'une information illicite au motif qu'il aurait manqué à une obligation générale de surveiller toutes les informations quelconques qu'il transmet. Les articles 14 et 15 soulignent qu'un prestataire de service ne peut être condamné à des dommages et intérêts en raison de violation d'un droit de propriété intellectuelle que pour des faits identifiés. Il s'agit donc de responsabilité civile ou pénale, appréciée de manière étroite. Ces dispositions semblent sans incidence sur une action en cessation ou en filtrage. Un filtre n'aboutit d'ailleurs pas à une surveillance des réseaux : il ne s'agit que d'un instrument technique, qui ne nécessite pas l'intervention du fournisseur d'accès. (v. d'ailleurs la position très argumentée du juge dans la décision, frappée d'appel, du tribunal de première instance de Bruxelles dans la décision *SABAM c/ SA Scarlet* rendue le 29 juin 2007, n° 04/8975/A).

Sur ce point, les considérants 45 et 47 de la directive sont d'ailleurs très clairs. D'une part, il est énoncé que les dispositions de la directive sur la responsabilité ne doivent pas faire obstacle au développement et à la mise en oeuvre effective de systèmes techniques de protection et d'identification ainsi que d'instruments techniques de surveillance rendus possibles par les techniques numériques. D'autre part, il est souligné que les limitations de responsabilité des prestataires de services intermédiaires prévues sont sans préjudice de la possibilité d'actions en cessation de différents types, qui 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.

LA MISE EN OEUVRE DE CONTRAVENTIONS

Cette annexe tente de mettre au clair les possibilité de sanctionner les actes de contrefaçon numérique par la voie de contraventions.

Sur le principe, on peut aisément déclasser la contrefaçon de la qualification actuelle de délit à une contravention. L'émission de cette contravention peut alors ressortir de deux logiques :

- La voie normale est l'identification de faits susceptibles d'être des infractions par un agent de police judiciaire qui émet la contravention, puis l'intervention d'un juge, qui constate l'infraction et détermine la peine ;

- La voie automatisée, choisie en matière de sécurité routière, revient à unir les phases d'émission de la contravention, de constatation puis de sanction (qui est standardisée en fonction de la nature de l'infraction) dans les mains des seuls agents de police judiciaire, et à repousser l'intervention d'un juge au stade de la contestation, en cas de refus de paiement ;

Cette dernière hypothèse est la plus intéressante pour la lutte contre la contrefaçon numérique, la première pouvant aboutir à embouteiller les tribunaux. Mais dans ce cas de procédure automatique, les garanties doivent être fortes, car l'accès au juge n'est pas de droit, les agents constatant les infractions et émettant les contraventions par eux-mêmes, ce qui est dérogatoire. Or ces pouvoirs ne peuvent ressortir à des agents privés, même assermentés, comme ceux des sociétés d'auteur. Il est nécessaire que le processus soit assuré par des agents de police judiciaire.

Deux bases juridiques sont le plus souvent suggérées pour établir cette contravention : la sécurisation du poste sur le fondement de l'article L. 335-12 du code de la propriété intellectuelle ; l'acte de contrefaçon, c'est-à-dire l'utilisation d'une oeuvre sans autorisation des ayant droits.

- La sécurisation du poste pose en l'état difficulté, car le caractère pénal[30] de l'actuel article L. 335-12 du code de la propriété intellectuelle n'est pas, comme il a été dit dans le rapport, clairement établi, au regard notamment du principe de personnalisation de la peine – même s'il est vrai qu'il existe une présomption de responsabilité du titulaire de la carte grise pour certaines contraventions au code de la route, mais des conditions très encadrées (cf. art. L. 21-2 du code de la route).

- L'acte de contrefaçon serait une base plus solide. S'il y a déclassement général de tous les actes illégaux de contrefaçon de délit en contravention, aucune difficulté n'existe au regard de la jurisprudence du Conseil constitutionnel relative à la loi du 1er août 2006. Si un déclassement partiel est envisagé, il convient alors d'assurer l'égalité devant la sanction en ne fixant pas une règle qui discriminerait une technique spécifique. Des pistes sont envisageables (téléchargement ; mise à disposition ; téléchargement avant sortie en salle ; téléchargement avant sortie en vidéo ; des critères de volume ne peuvent être exclus ; ...).

[30] La mise en oeuvre sur ce même fondement d'une sanction non pas pénale mais administrative, comme ce sera le cas si l'autorité évoquée dans le rapport est mise en place, ne pose en revanche pas de difficulté dès lors qu'il existe des responsabilités, principalement civiles, du fait d'autrui. V. note 20, p. 21 du rapport.

LA MISE EN OEUVRE D'UNE SANCTION CIVILE

Cette annexe vise à proposer un dispositif qui pourrait, s'il était perfectionné, s'avérer utile et éviter un engagement trop systématique de la responsabilité pénale.

A côté de la sanction pénale est prévue la possibilité d'une réparation civile des actes de contrefaçon constatés par des ayants droit lésés. Le principe normal de la réparation civile est celui de la réparation intégrale de préjudices précisément établis. La fixation par le juge de dommages et intérêts punitifs est traditionnellement refusée, à la différence de la pratique américaine. Mais une évolution pourrait être utilement envisagée dans le sens de la forfaitarisation de la réparation. On peut imaginer que la loi fixe le principe et le montant d'une amende forfaitaire correspondant à diverses catégories d'actes de contrefaçon numérique (mise à disposition ou téléchargement sur un site d'échange ; mise à disposition sur un site dédié ; etc...). Notons ainsi que l'article L. 311-1-3 du code de la propriété intellectuelle, modifié par l'article 31 de la loi n° 2007-1544 du 29 octobre 2007 relative à la lutte contre la contrefaçon, prévoit désormais qu'une somme forfaitaire puisse être, à la demande de la partie lésée, allouée au titre de dommages et intérêts, eux-mêmes étant majorés en cas d'atteinte à un droit d'auteur ou à un droit voisin («Pour évaluer le préjudice résultant de la contrefaçon, d'une atteinte à un droit voisin du droit d'auteur ou aux droits du producteur de base de données, la juridiction prend en considération les conséquences économiques négatives, dont le manque à gagner, subies par la partie lésée, les bénéfices réalisés par l'auteur de l'atteinte aux droits et le préjudice moral causé au titulaire du droit du fait de l'atteinte. /Toutefois, la juridiction peut, à titre d'alternative et sur demande de la partie lésée, allouer à titre de dommages et intérêts une somme forfaitaire qui ne peut être inférieure au montant des redevances ou droits qui auraient été dus si l'auteur de l'atteinte avait demandé l'autorisation d'utiliser le droit auquel il a porté atteinte. »). La voie ainsi ouverte pourrait être davantage explorée.

En plus de ce fondement, il pourrait être prévu de simplifier l'accès à la réparation civile, par l'adaptation de la procédure de l'injonction de payer. Un ayant droit qui constaterait une utilisation non autorisée devrait alors, sur la base des preuves dont il dispose, obtenir d'un juge civil un état exécutoire qui permettra de forcer le débiteur à s'acquitter de la sanction forfaitaire prévue. Il lui suffira d'apporter au juge les éléments caractérisant la contrefaçon ; le juge vérifiera l'exigibilité de la créance au regard des critères fixés par la loi pour définir le périmètre de la sanction. En cas de refus de paiement, ce sera au débiteur d'intenter un recours ; cette inversion de la charge du procès, avec la possibilité que la sanction pécuniaire finale soit majorée en cas de contestation non fondée, pourraient être très dissuasive. Cette procédure peut se dérouler devant le juge d'instance ; elle se fait sur dossier uniquement, sans audience, et est donc très légère. Surtout, ce juge est en capacité de rapprocher l'adresse IP du nom de l'abonné auprès du fournisseurs d'accès à internet.

ANNEXE 2 : LETTRE DE MISSION

Liberté Egalité Fraternité
République Française

Ministère de la Culture et de la Communication

La Ministre

Monsieur Denis OLIVENNES
Président directeur général
FNAC

Paris, le 26 juillet 2007

Monsieur le Président-directeur général,

Le Président de la République a régulièrement affirmé la nécessité de développer toutes « les formes de diffusion légale » des œuvres – audiovisuelles, cinématographiques, littéraires ou musicales, voire vidéo-ludiques – sur les réseaux numériques. En effet, la généralisation d'Internet et des nouvelles technologies qui lui sont liées constitue un enjeu majeur pour le public et pour les acteurs de la création, tant sur le plan de la diffusion la plus large de la culture que sur celui du développement économique. Par ailleurs, le remarquable essor en France du haut débit et des services en ligne est un levier supplémentaire pour favoriser la compétitivité et la croissance de notre économie.

Naturellement, l'essor de l'offre légale implique que le Gouvernement assume les responsabilités qui sont les siennes pour garantir les droits qui protègent la juste rémunération des auteurs et des investisseurs. Cette politique sera conduite de façon résolue. Elle mobilisera les différents services de l'Etat compétents pour mener les actions de prévention indispensables, de même que la lutte contre le téléchargement illicite des œuvres.

Le succès de l'offre légale dépend cependant d'un ensemble complexe de conditions, commerciales, économiques, juridiques et technologiques, sur lesquelles les acteurs de la création, ceux d'Internet et le Gouvernement doivent agir de concert. Pour cette raison, les mesures visant à créer l'environnement le plus favorable à la diffusion des œuvres sur Internet seront d'autant plus efficaces qu'elles auront fait l'objet d'une réflexion approfondie associant les différentes parties prenantes : créateurs, producteurs, professionnels et usagers de l'Internet.

Votre expérience professionnelle, ainsi que la hauteur de vues que vous avez manifestée à l'occasion de vos prises de position dans le débat public, vous désignent à mes yeux pour conduire une mission de réflexion et de concertation destinée à favoriser la conclusion d'un

3, rue de Valois, 75033 Paris Cedex 01 France - Téléphone : 01 40 15 80 00

accord entre professionnels, permettant le développement d'offres légales attractives d'œuvres en ligne et dissuadant le téléchargement illégal de masse.

Vous serez assisté dans cette mission d'Isabelle Falque-Pierrotin, Conseiller d'État, d'un économiste, d'un ingénieur spécialiste des NTIC et d'un magistrat de l'ordre judiciaire. Damien Botteghi, auditeur au Conseil d'État les assistera dans cette tâche.

Afin de valider sur les plans juridique, technique et économique, les préconisations que vous formulerez, vous procéderez notamment à l'audition de personnalités, choisies au titre de leur représentativité des secteurs économiques et des intérêts concernés ou de leurs compétences particulières. Vos analyses seront utilement éclairées par une présentation des solutions mises en œuvre ou envisagées chez nos principaux partenaires, dans l'Union européenne ou au-delà. Je souhaite que vos conclusions puissent se traduire dans un accord interprofessionnel rassemblant toutes les parties prenantes et notamment les acteurs de l'Internet ou, à défaut d'un tel accord, donner lieu à des mesures législatives et réglementaires dont le gouvernement prendrait l'initiative.

Vous disposerez, pour l'accomplissement de votre mission, de l'appui de mon cabinet, des services du ministère de la culture et de la communication et de la direction du développement des médias. Dans des conditions définies par la ministre de la justice et la ministre de l'économie, des finances et de l'emploi, leurs services pourront également vous assister et concourir à votre réflexion. La ministre de l'économie des finances et de l'emploi devra être tout particulièrement associée à cette mission.

Je souhaite disposer des résultats de vos travaux, que je remettrai au Président de la République, le 31 octobre prochain. Afin d'anticiper les modalités de suivi ou de mise en œuvre rapide de vos préconisations, vous voudrez bien me remettre un rapport d'étape le 1er octobre.

Je vous remercie d'avoir accepté d'assurer la conduite de cette mission et vous prie d'agréer, Monsieur le Président-directeur général, l'expression de ma sincère considération.

Christine ALBANEL

ANNEXE 3 : STRUCTURES AUDITIONNEES

<u>Sociétés de perception et de répartition des droits d'auteur</u> :

Adami
Spedidam
Unevi
SACEM
SACD
SCAM
SAIF
SCPP

<u>Représentants des industries de l'audiovisuel, du cinéma et de la musique</u> :

ALPA
Fédération nationale des distributeurs de films
Fédération nationale des cinémas français
BLIC
Association des producteurs indépendants
SNAC
UNAC
CSDEM
SNEP
UPFI
USPA
SPI
UPF
SPECT
SRF
ARP
APC
SORECOP
ADAGP
Warner Bros
SEVN
Motion Picture Association of America

<u>Opérateurs techniques</u> :

Orange France
Free
Neuf cégétel
AFA
GESTE
SELL
SIMAVELEC
DAILYMOTION
Numericable/Noos
YouTube/Google
AFORST

Prestataires de solutions techniques :

Advestigo
Audible Magic
Communications SA
CoPeerRight Agency
Institut national de l'Audiovisuel (INA)
I-Tracing
LTU Technologies
Qosmos
Thomson

Télévisions :

TF1
Canal+
M6

Distributeurs et acteur technique de d'offre légale de musique :

Virgin
Jiwa Music
Yacast

Association de consommateurs et d'internautes :

UFC
Asseco CFDT
UNAF
APRIL
STOP DRM
Ligue ODEBI
SFIB
Alliance TICS, SFIB
Association francophone des utilisateurs de Linux et des logiciels libres (AFUL)

Autorités publiques :

ARCEP
CNIL
ARMT

Autres structures françaises :

Ligue de football professionnelle
Syndicat des vidéoclubs de France
INRIA
BSC Conseil

Structures étrangères :

Warner Bros Entertainment UK
Cabinet du Premier Ministre UK
BPI (British Phonographic Industry)
PPL
EMI Music UK
IFPI
Administration de la Culture et du Commerce UK
Parliamentary Under-Secretary of State, Department for Innovation, Universities and skills
NBC Universal US