Réponse de l'AFA à la consultation de la Commission Européenne sur les contenus créatifs en ligne dans le marché unique

Introduction

Créée en 1997, l'Association des fournisseurs d'accès et de services Internet (AFA) regroupe les prestataires techniques de communication électronique constitués en France sous forme de sociétés commerciales, autour de quatre activités spécifiques :

- les réseaux,
- l'hébergement,
- l'accès,
- les services en ligne

L'AFA comprend ainsi les principaux fournisseurs d'accès français (France-Télécom, Neuf-Cegetel, SFR, Télécom-Italia, Numericable, Dartybox, Bouygues Telecom …) ainsi que plusieurs hébergeurs (MSN France, Google France, AOL, Kewego …).

Commentaires généraux

L'Association des fournisseurs d'accès et de services Internet (AFA) se réjouit de la mise en place prioritaire, au niveau communautaire, d'une politique de promotion des usages et services innovants.

Du fait de la généralisation de l'accès haut débit à Internet, la *"mise en place rapide et efficace de nouveaux services ainsi que des modèles commerciaux correspondants pour la création et la diffusion de contenus et de connaissances européens en ligne"* est nécessaire pour la création d'un véritable marché intérieur des contenus en ligne, comme le souligne à juste titre la Commission européenne dans sa communication du 3 janvier 2008 relative aux *"contenus créatifs en ligne"*[1] (en ce compris les créations audiovisuelles en ligne, jeux en ligne, publication en ligne, contenus éducatifs en ligne, contenus générés par les utilisateurs).

Du fait du développement particulièrement avancé du haut débit en France, les nouveaux usages et services connaissent un fort engouement de la part des consommateurs français.

[1] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur les contenus créatifs en ligne dans le marché unique, SEC (2007) 1710, 3 janvier 2008.

Aussi, l'accroissement de la disponibilité des contenus créatifs en ligne, dans le respect du droit d'auteur, constitue une priorité absolue pour l'ouverture du marché intérieur.

Pour compléter ces remarques d'ordre général, l'AFA se propose de répondre précisément aux questions 9, 10 et 11.

Annexe
Contenus créatifs en ligne : questions politiques et réglementaires soumises à consultation

Offre licite et piratage

9) Comment une collaboration approfondie et efficace entre parties intéressées peut-elle améliorer le respect des droits d'auteur dans l'environnement en ligne ?

Face à la banalisation de la pratique de contrefaçon numérique, l'amélioration du respect des droits d'auteur dans l'environnement en ligne requiert l'implication de l'ensemble des acteurs (ayants droit, fournisseurs d'accès et hébergeurs) dans la lutte contre la piraterie.

Dans cette perspective, les membres de l'AFA ont développé une coopération efficace depuis plusieurs années avec les autorités judiciaires et répondent à plus de 90 % des réquisitions qui leur sont adressées. Les demandes restantes ne peuvent être satisfaites notamment lorsqu'elles sont incomplètes ou quand elles portent sur des données qui ne font pas l'objet d'une obligation de conservation. En outre, ces réponses sont adressées pour la grande majorité d'entre elles dans un délai de 24 heures, ce qui atteste de la mobilisation de l'ensemble des prestataires techniques.

Sur la collaboration effective entre fournisseurs d'accès / ayants droit

Depuis plusieurs années, l'AFA a toujours recherché et promu la concertation avec les industries culturelles, pour le développement de l'offre légale :

- Conclusion de la « Charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre la piraterie numérique (28 juillet 2004) ;
- Communication : mise à disposition gracieuse d'espaces publicitaires pour la promotion offre musicale en ligne, au bénéfice du SNEP (diffusion du film « Le Batteur » (2004) promotion du site promusicfrance.com) ;
- ***Proposition d'amendement dit d' « approche graduée » avec l'industrie cinématographique*** (non examinée par le Parlement en raison de l'urgence) ;
- Charte VOD (20 décembre 2005) ;
- Déclaration conjointe du 21 décembre 2006 de lutte contre la piraterie AFA / ayants droit de l'industrie cinématographique.

Les fournisseurs d'accès membres de l'AFA ont ainsi soutenu des actions de communication spécifiques et ciblées, permettant de sensibiliser le public aux effets négatifs du piratage et à la nécessité de respecter les droits d'auteur. À titre d'illustration, les fournisseurs d'accès

Internet membres de l'AFA ont procédé à diverses opérations de sensibilisation via e-mailing vers leurs abonnés.

Malheureusement, ces diverses initiatives n'ont pas débouché sur une meilleure circulation des œuvres cinématographiques et audiovisuelles en France ni sur un développement satisfaisant de l'offre légale musicale.

S'agissant en particulier de la VOD, nonobstant une forte demande potentielle de près de 46 % des internautes (étude du CNC / Novatris - novembre 2006**)**, ce marché est toujours un marché émergent, notamment en raison des difficultés d'accès aux droits que rencontrent les opérateurs**.**

Comme le rapport relatif au « développement et la protection des œuvres culturelles sur les nouveaux réseaux » (novembre 2007) le souligne : "*l'offre numérique légale, tant cinématographique que musicale, n'est pas encore suffisamment connue, valorisée, et à certains égards jugée légitime*." (p.11).

Afin de "*désinciter*" le recours au piratage des utilisateurs souhaitant avoir accès à des contenus en ligne, le rapport sus-visé recommande le développement d'une offre légale riche et attractive.

Face à l'ampleur de la demande potentielle, la Commission a la possibilité de promouvoir des solutions ambitieuses et innovantes, sources de création de valeur pour l'ensemble des acteurs concernés :

1. **Raccourcissement de la chronologie des médias au niveau européen (4 mois après sortie films en salles)**

L'ouverture de la fenêtre VOD, particulièrement tardive en France (7 mois et demi après la sortie en salles), ne permet pas de promouvoir l'attractivité de l'offre VOD.
Afin de lever cette barrière, la première recommandation du rapport sus-visé[2] consiste à *"ramener la fenêtre VOD de 7 mois et demi après la sortie en salles à **4 mois**"*, via par exemple un accord interprofessionnel.

L'AFA, bien que très favorable à la réduction de la fenêtre, s'interroge sur la réelle portée d'un tel accord entre des professionnels qui disposent, à coté des droits VOD, de droits sur d'autres modes d'exploitation susceptibles de limiter leurs intérêts dans la VOD. En outre, l'AFA s'inquiète de la qualification et de la validité d'un tel accord au regard du droit de la concurrence, en particulier en matière d'entente illicite.

La Commission pourrait ici (i) soit écarter la faculté de déterminer collectivement la chronologie des médias dans le cadre d'un accord interprofessionnel, laissant ainsi les acteurs décider individuellement de la portée des droits consentis ; (ii) soit valider la possibilité de conclure de tels accords interprofessionnels au regard du faible développement du marché de la VOD, tout en les encadrant afin de limiter les contraintes pouvant peser sur les nouvelles formes d'exploitation.

[2] Rapport précité, page 25, recommandation n°1.

Dans ce dernier cas, qui a la préférence de l'AFA, la Commission pourrait publier des orientations précises, en préconisant de ramener à 4 mois après la sortie en salle la possibilité d'exploiter des œuvres en VOD et en restreignant fortement les périodes de suspension de la fenêtre d'exploitation en VOD.

2. **L'octroi de subventions conditionnées à une exploitation en VOD**

Le rapport précité recommande de *"subordonner les aides à la production (...) à l'engagement que le film soit rendu disponible en VOD"*.[3]

L'AFA soutient pleinement cette recommandation qui va dans le sens d'une offre diversifiée d'accès aux œuvres cinématographiques.

3. **Meilleure exposition des œuvres**

L'AFA souhaiterait une suspension de la fenêtre VOD limitée à 3 mois pendant les seules périodes de diffusion effective sur les chaines de Pay - TV et les chaînes en clair.

10) Estimez-vous que l'accord récemment signé en France est un exemple à suivre ?

Face au phénomène de la contrefaçon numérique, l'efficacité **du système à mettre en place requiert l'implication** de l'ensemble des acteurs**, pour la définition de solutions** consensuelles**.** Dans ce contexte, et s'agissant des mesures spécifiques concernant les fournisseurs d'accès à Internet, l'AFA soutient la volonté de collaboration qui a présidé à la conclusion de l'accord Olivennes.

Quoi qu'ayant promu depuis plusieurs années la coopération avec les ayants droit, l'AFA n'a pas souhaité s'associer à la signature de cet accord, qui a été co-signé par trois des fournisseurs d'accès membres de l'AFA (France-Télécom, Neuf-Cegetel, Numericable).

En effet, l'AFA représente également les hébergeurs et ne pouvait souscrire à certaines des dispositions de l'accord concernant ces prestataires techniques, dont certaines contrevenaient directement au cadre législatif existant et notamment aux termes de la directive Commerce électronique. Les hébergeurs membres de l'AFA souscrivent pleinement au principe de "*collaboration en toute bonne foi*" entre les prestataires d'hébergement et les ayant droits pour généraliser l'utilisation de technologies de reconnaissance des contenus, et sont déjà activement engagés dans ce processus de collaboration. Toutefois, le projet d'accord faisait référence à "*une obligation faite aux plates-formes d'engager toute mesure visant à combattre la mise en ligne illicite de contenus protégés*". Cette disposition entre en contradiction directe avec l'absence d'obligation de surveillance générale édictée dans la directive européenne Commerce Electronique et par là même avec l'esprit d'un accord de coopération entre les différents concernés.

L'équilibre de l'accord repose sur l'adoption concomitante de mesures relatives au développement de l'offre légale, ainsi qu'un ensemble de mesures techniques et juridiques anti-piraterie.

[3] Rapport précité, page 25, recommandation n°3.

Au regard de l'ampleur de la piraterie, la priorité majeure et urgente devrait être le développement d'une offre légale riche et attractive, qui corresponde aux besoins et aux attentes des utilisateurs.

En contrepartie des engagements souscrits par les ayants droit sur le développement de l'offre légale, les fournisseurs d'accès signataires se sont engagés à collaborer avec les ayants droit sous 24 mois « *sur les modalités d'expérimentation des technologies de filtrage des réseaux disponibles mais qui méritent des approfondissements préalables, et à les déployer si les résultats s'avèrent probants et la généralisation techniquement et financièrement réaliste* ».

L'AFA, ainsi que plusieurs études indépendantes, soulignent l'inopportunité et l'inefficacité du filtrage des contenus sur le réseau des fournisseurs d'accès à Internet (notamment le rapport d'étude des experts Antoine Brugidou et Gilles Kahn en date du 9 mars 2005) et mettent en évidence le coût y associé.

Par cet engagement, les FAI français signataires de l'accord réaffirment ainsi leur bonne volonté pour étudier à nouveau des solutions technologiquement lourdes qui n'ont pas encore apporté la preuve de leur efficacité.

S'agissant des mesures techniques et juridiques anti-piraterie, l'AFA tient à rappeler que leur mise en œuvre doit nécessairement s'inscrire dans le respect de plusieurs principes fondamentaux : respect de la légalité des délits et des peines, des droits de la défense et de la liberté individuelle, respect de l'anonymat (articles 8 de la CEDH, 9 du code civil français et loi française de 1978), respect de la finalité des traitements de données à caractère personnel.

L'AFA considère donc que le contrôle du juge est nécessaire pour assurer le respect de ces principes fondamentaux, et le caractère proportionné des mesures, nécessaire pour assurer l'efficacité du dispositif vis-à-vis des utilisateurs.
A ce stade, et sans pouvoir présager du dispositif final qui devrait découler du processus de décision législatif, l'AFA souhaite rappeler l'importance d'assurer l'équilibre entre la protection de la propriété intellectuelle et les divers droits fondamentaux protégés par l'ordre juridique français et communautaire.

En ce qui concerne les FAI, ces derniers agissent comme des « transporteurs », de la même manière que les services postaux ou les opérateurs de téléphonie. **Ils ne sont donc pas responsables des contenus qu'ils transportent, puisqu'ils n'en sont pas les auteurs et qu'ils ne sont pas à l'origine de leur transmission**.

Inversement, les FAI ont une obligation de neutralité vis-à-vis du contenu des communications privées, conformément au régime applicable aux autres catégories de transporteurs.

Cette obligation de neutralité, justifiée par un **impératif de protection du secret de la vie privée et des correspondances** des internautes, fait l'objet de plusieurs dispositions législatives, conformément à la Directive communautaire 2000/31/CE qu'à la Convention européenne des droits de l'homme du 4 novembre 1950.

Hors de ce cadre juridique, les FAI seraient pénalement responsables de la violation de plusieurs libertés fondamentales en cas de surveillance ou d'interception des communications échangées entre les internautes :

- Atteinte au secret de la vie privée ;
- Atteinte au secret et livraison des correspondances ;
- Violation de la liberté d'accès à l'information ;
- Atteinte au secret des échanges entre certains professionnels (comme les avocats et leurs clients …).

Une telle surveillance des correspondances ne serait pas plus acceptée par le corps social que si elle était diligentée par des services postaux.

Les pouvoirs et attributions de l'Autorité publique placée sous le contrôle du juge, qui nécessiteront l'adaptation de textes législatifs en vigueur et la création de nouveaux, devraient permettre la mise en place d'un dispositif fondé sur l'envoi, par les fournisseurs d'accès à Internet et ″sous le timbre de l'Autorité″, de **messages électroniques spécifiques de sensibilisation** aux internautes. L'objectif premier d'un tel dispositif est d'avoir un **caractère pédagogique**.

L'envoi de messages de sensibilisation aux internautes s'est en effet avéré extrêmement concluant aux Etats-Unis. Une étude de la Motion Picture Association a révélé que 70 % des contrevenants cessaient leurs pratiques après l'envoi du premier message. 20 % des internautes restants cessaient leurs pratiques après l'envoi du second message. Le seul envoi de deux messages de sensibilisation permettrait ainsi de toucher 80 à 90 % de la population cible.

Toutefois, la mise en place d'un tel système suppose le respect de plusieurs règles : règles relatives au traitement des données personnelles, finalité purement pédagogique du fait de l'impossible imputabilité de l'acte de contrefaçon à l'abonné.

S'agissant des sanctions envisagées, il convient de ne pas en minimiser ou banaliser la portée: suspendre, même temporairement, l'abonnement Internet d'un utilisateur, ce n'est pas seulement l'empêcher d'accéder à des contenus contrevenants aux droits d'auteur, c'est aussi et surtout lui interdire l'utilisation à un vecteur communication et d'expression devenu indispensable, qui offrent l'accès à une pluralité d'information, à une diversité de contenus, ou à une multitude de services publiques. À ce titre il convient également de souligner les risques techniques induits par la suspension, réduction de débit ou coupure définitive même prises par une autorité habilitée et non le FAI, qui auraient **un impact certain sur l'utilisation d'autres services**.

11) Estimez-vous que la mise en œuvre de mesures de filtrage serait un moyen efficace pour éviter les atteintes aux droits d'auteur en ligne ?

L'ensemble des travaux conduits depuis dix ans sur le filtrage des contenus sur Internet a démontré que cette mesure était inefficace et disproportionnée, pour lutter tant contre les contenus illégaux tels que la pornographie enfantine (I) que contre les atteintes aux droits d'auteur.

Cette appréciation s'applique tant au filtrage des contenus sur le web (II) qu'au filtrage des contenus sur les réseaux « peer-to-peer » (III).

L'AFA entend enfin souligner les risques juridiques du filtrage pour les fournisseurs d'accès à Internet ou FAI (IV).

1. La lutte de l'AFA contre la cybercriminalité

Depuis sa création en 1997, l'Association des fournisseurs d'accès et de services Internet (AFA) s'est attachée à favoriser et développer la coopération avec les autorités judiciaires.

Cette coopération s'est notamment traduite par :

- La mise en œuvre d'une déontologie professionnelle sur la conservation des données par les fournisseurs d'accès et les hébergeurs ;
- La création d'un Point de Contact dès 1998 pour recevoir et rediriger les signalements de contenus illégaux, notamment de pornographie enfantine et de provocation à la haine raciale, vers les autorités compétentes ;
- Une participation active aux groupes de travail pilotés par la Direction générale de la Police nationale sur les réquisitions judiciaires (modélisation, définition de points d'entrée uniques chez les prestataires, etc.) ;
- Une participation aux sessions de formation « Technologies de l'information et de la communication » de la Gendarmerie, de la Police et de l'Ecole Nationale de la Magistrature ;
- La signature d'une charte contre les contenus odieux en 2004 ;
- La création d'un Label « net + sûr » en 2005 sous le parrainage du ministre délégué à l'Industrie.

L'industrie française de l'accès à Internet estime qu'il ne lui appartient pas de contrôler ou de limiter les allées et venues sur Internet de tous les citoyens, ou les informations qu'ils échangent, ce rôle de contrôle n'appartenant, le cas échéant, qu'aux seuls pouvoirs publics. Toutefois, elle contribue pleinement au travail des autorités judiciaires en répondant à leurs réquisitions. La recherche de la responsabilité de l'auteur du contenu nous semble être un modèle de régulation à la fois efficace et républicain sur le plan national et international.

2. Le filtrage du web par les fournisseurs d'accès à Internet

L'AFA s'oppose depuis plusieurs années aux mesures de filtrage de sites web par les fournisseurs d'accès. De telles mesures auraient de très graves impacts sur l'industrie, les consommateurs et les citoyens.

Afin d'éviter toute confusion, il est primordial de bien distinguer les métiers d'hébergeurs et de fournisseurs d'accès à Internet. Autant il n'y a aucune difficulté à mettre en œuvre une mesure de coupure lorsque l'auteur du dommage est client du prestataire technique (prestation d'**hébergement**) : la décision de coupure a un effet définitif de cessation du dommage, qui est mis en œuvre de manière simple par le prestataire technique. En revanche, la situation est infiniment plus délicate dans l'hypothèse où la mesure devrait être mise en œuvre par le **fournisseur d'accès**. Car il n'y aurait pas de cessation du dommage, le contenu étant toujours accessible.

2.1 Difficultés techniques

La mesure du filtrage de l'accès à Internet pose de nombreuses difficultés techniques (voir une étude complète, réalisée en 2005 par l'expert judiciaire Jean-Raymond Lemaire)

L'accès à un site Internet se déroule de la manière suivante : le nom de domaine du site visé (par exemple, www.minefi.gouv.fr) est converti, par l'intermédiaire d'un Domain Name Server (DNS) exploité par le FAI de l'internaute à l'origine de la requête (en pratique, il s'agit d'un système informatique permettant ce type de conversion), en une adresse IP (par exemple, pour www.minefi.gouv.fr : 194.51.23.246) correspondant spécifiquement au site en cause.

Tous les documents figurant sur le site concerné sont identifiés par une Uniform Ressources Locator (URL).

Il apparaît que seules trois techniques de filtrage sont envisageables au niveau des FAI : le blocage de l'adresse IP, celui du nom de domaine ou celui de l'URL. Pour autant, aucune d'entre elles n'apparaît adaptée au résultat recherché.

- **Le blocage de l'adresse IP (cf. figure annexe 1 de l'étude jointe)**

Cette technique permet d'interdire l'accès à un site lorsque le DNS convertit le nom de domaine du site en cause en une adresse IP prédéterminée. Ainsi, dans l'exemple précité, lorsque l'adresse IP 194.51.23.246 est détectée, celle-ci est bloquée, de sorte que l'accès au site www.minefi.gouv.fr est impossible.
Pour autant, il convient de souligner que plusieurs noms de domaines distincts (par exemple, www.minefi.gouv.fr et www.finances.gouv.fr) peuvent correspondre à une seule et même adresse IP (ici 194.51.23.246).
Dans un tel cas, le blocage de l'adresse IP empêche l'accès à tous les noms de domaines concernés, c'est-à-dire à l'ensemble des sites hébergés sur le serveur auquel est attribuée l'adresse IP en cause. Dans l'exemple précité, bloquer l'adresse IP 194.51.23.246 reviendrait donc à empêcher l'accès aux sites www.minefi.gouv.fr et www.finances.gouv.fr , alors même que ces sites sont distincts et que leurs contenus respectifs peuvent être différents.

- **Le blocage du nom de domaine (DNS) (cf. figure annexe 2 de l'étude jointe),**

Cette technique consiste à bloquer l'accès à un nom de domaine particulier en empêchant, au niveau du DNS, sa conversion en l'adresse IP correspondante. Dans l'exemple précité, seule l'adresse www.minefi.gouv.fr serait alors inaccessible, les internautes pouvant continuer à se connecter à l'adresse www.finances.gouv.fr.
La principale difficulté soulevée par cette technique réside dans le fait que, dans le cas où plusieurs sites distincts ont le même nom de domaine (ce qui est notamment le cas s'agissant des pages personnelles des abonnés à un FAI hébergées par celui-ci), l'accès à l'ensemble de ces sites est rendu impossible.
Par exemple, pour bloquer un site personnel de jeux en ligne hébergé par Virgin en Angleterre : http://freespace.virgin.net/betandloose (fictif), il faudrait bloquer http://freespace.virgin.net et donc tous les sites (plusieurs millions) utilisant ce nom de domaine.

S'il devait être mis en place, ce moyen de filtrage obligerait le fournisseur d'accès concerné à faire évoluer son architecture technique. Mais cette méthode est aisément contournable : il suffit à un utilisateur de modifier un paramètre pour se connecter à l'Internet en utilisant le DNS d'un fournisseur d'accès ne pratiquant pas le filtrage ou en accédant au site en tapant son adresse IP.

- **Le blocage de l'URL (cf. figure annexe 3 de l'étude jointe),**

Cette technique consiste à bloquer l'URL identifiant le site Web concerné. A cette fin, le fournisseur d'accès est obligé d'installer un serveur proxy (voir étude) pour surveiller l'intégralité de la navigation de ses abonnés et les empêcher d'accéder au site correspondant à l'URL donnée. Les fournisseurs d'accès seraient dans l'obligation d'investir dans des filtres et, de ce fait, de revoir l'intégralité de leur architecture technique.

Les investissements (plusieurs millions d'euros par opérateur) seraient nécessairement lourds en termes de machines, d'espaces d'hébergement, de maintenance et de migration de la connexion de l'ensemble des parcs d'abonnés. Outre son coût, cette méthode est aisément contournable lorsque l'internaute utilise une connexion sécurisée (puisqu'il est alors impossible de « lire » ce qu'il visite), ou lorsqu'il utilise un site dit d'anonymisation c'est-à-dire masquant toute navigation ultérieure.

2.2 – L'inefficacité de la mesure

Aucune mesure de filtrage de l'accès à Internet n'est en mesure d'empêcher efficacement l'accès au contenu filtré.

Les conclusions de l'expert judiciaire Jean-Raymond Lemaire, dont l'objectivité a été reconnue par l'ensemble des parties au procès Aaargh sont les suivantes :

« A notre avis, en l'état de la technique, bloquer l'accès à un site Internet est une opération qui peut être pénalisante (dégradation des performances et coût élevé) pour une efficacité très aléatoire.

Aucune des techniques possibles à ce jour, filtrage de l'adresse IP ou du nom de domaine, n'empêchera des Internautes qui souhaitent accéder à un site de la faire.

Par ailleurs, tout blocage fera obligatoirement l'objet d'une information et les moyens de contournement feront également l'objet d'information. Suite à une décision « juste », n'encouragerons nous pas les Internautes, et les plus jeunes d'entre eux, à étudier puis utiliser les solutions de contournement ? »

L'analyse des différentes méthodes de filtrage a effectivement permis de mettre en exergue les limites inhérentes à ces techniques. Les moyens de contournement restent nombreux tant pour le fournisseur de contenu (diffuseur de l'information) que pour les internautes eux-mêmes.

- **De nombreux moyens de contournement**

Le volume de contenu transmis sur Internet et sa nature sans cesse changeante rendent impossible l'établissement et la mise à jour d'une liste complète, opportune et cohérente de sites interdits, d'autant plus que ces sites peuvent facilement changer d'URL ou d'adresse IP pour contourner le filtre mis en place.

Les utilisateurs peuvent demander l'accès à des sites de façon totalement anonyme par l'intermédiaire d'un service de procuration, ou même faire des demandes de contenus chiffrées et recevoir les réponses chiffrées, annulant toute possibilité de filtrage.

Outre les faiblesses susmentionnées des méthodes de filtrage, les restrictions imposées aux fournisseurs d'accès français pourraient être contournées par les utilisateurs qui se connectent au réseau Internet par l'intermédiaire de fournisseur d'accès étrangers ou de serveur proxy.

Un des arguments souvent avancés par les partisans d'un filtrage à l'accès est que cette mesure, bien qu'imparfaite, parasite l'accès aux sites illégaux et finit par décourager les internautes comme les auteurs.
L'exemple du site négationniste Aaargh montre, au contraire, que la décision de bloquer ce site a contribué à la diffusion de son contenu. La publicité faite autour de cette affaire a largement contribué à la notoriété d'un site au départ confidentiel. Son contenu s'est retrouvé dupliqué sur de nombreux sites miroirs.
Pour les sites de jeux illégaux, on peut penser que l'effet dissuasif sera d'autant moins important que certains de ces sites sont protégés par la législation de leur pays d'hébergement. Sauf à bloquer l'adresse IP et donc de nombreux autres sites, le filtrage ne gênera aucunement l'auteur du site qui dispose de nombreux moyens pour rediriger les internautes vers son site, surtout si son hébergeur ne le contraint pas à déménager.

La plupart des moyens de contournement sont à la portée de chacun et accessible à tous. (http://www.rsf.org/rubrique.php3?id_rubrique=527). Il ne fait aucun doute qu'une mesure de filtrage contre les jeux en ligne contribuera fortement au développement des solutions de contournement et à leur assimilation par le plus grand nombre.

- **Un coût important pour les prestataires français tant publics que privés**

Enfin, ces méthodes de filtrage représentent un coût important pour un fournisseur d'accès dont l'architecture technique devra être profondément remaniée pour supporter la mise en œuvre d'un procédé de filtrage, surtout si celui-ci se veut raisonnablement couvrir les principaux contenus ou activités illicites."

Au total, les moyens de filtrage qui pourraient être mis en œuvre par les fournisseurs d'accès seraient donc :

- très coûteux, **ce coût se retrouvant au total sur la facture des internautes**
- **aisément contournables**.

Ils ne représentent donc pas une solution aux problèmes qu'ils seraient censés résoudre. En outre, la mise en place de serveurs proxies, qui serait inéluctable si le filtrage de l'Internet venait à être institué, poserait de **graves problèmes aux enquêtes judiciaires**. En effet, les serveurs proxies empêchent généralement une conservation de données d'identification

supérieure à quelques jours alors qu'en l'absence de telles installations la durée de conservation peut être beaucoup plus longue.

3. Le filtrage des contenus peer-to-peer par les fournisseurs d'accès à Internet

3. 1 Difficultés techniques

- **La mise en œuvre problématique du filtrage à grande échelle**

Le filtrage de protocoles P2P tel qu'il est proposé par certains éditeurs de solutions techniques est une mesure qui nécessite l'implémentation de plusieurs milliers de boîtiers sur les réseaux de chaque FAI.

Tandis que la possibilité d'implémenter une telle mesure sur un réseau de fournisseur d'accès de taille raisonnable n'a jamais été démontrée, son coût exorbitant n'est pas compensé par son efficacité à lutter effectivement contre les atteintes aux droits, ainsi que nous le verrons ultérieurement.

Le filtrage systématique a par ailleurs été considéré comme « non pertinent » par un rapport d'étude des experts Antoine Brugidou et Gilles Kahn en date du 9 mars 2005 (disponible à l'adresse http://www.afa-france.com/piraterienumerique.pdf) :

*« **Le filtrage à grande échelle sur le réseau pourrait se heurter à une problématique de mise en œuvre :***
Le filtrage à grande échelle du trafic peer to peer sur un très grand nombre d'internautes pourrait poser un problème de coûts de mise en œuvre et de maintenance. Compte tenu de l'évolution des architectures des FAI, un tel filtrage supposerait la mise en œuvre d'un nombre significatif de boîtiers dans le réseau, une administration de ces boîtiers et probablement des évolutions de l'architecture réseau proprement dite – ainsi que des évolutions au niveau des systèmes d'information ».

Il convient enfin de noter que les fournisseurs d'accès ont des obligations de qualité de service et de sécurité de leur réseau, incompatibles avec un tel déploiement.

- **L'évolution des protocoles**

A supposé qu'un système de filtrage des échanges P2P puisse être implémenté sur les réseaux, l'évolution des protocoles imposerait sa mise à jour régulière. Les tests préalables à la mise en œuvre de nouvelles versions logicielles par les fournisseurs d'accès Internet sur leurs réseaux prennent toutefois de deux à trois mois alors que les évolutions des logiciels de peer-to-peer ne prennent que quelques jours, rendant ainsi vaine toute tentative de faire une mise à jour efficace.

- **L'asymétrie du trafic**

L'analyse d'un flux par un système de filtrage doit être faite simultanément en trafic montant et descendant. A défaut, le contenu de l'échange ne peut pas être analysé.

Or, la plupart des FAI n'utilisent pas les mêmes équipements pour gérer ces deux types de trafic, ce qui permet tant d'offrir des temps performants de latence aux abonnés que d'optimiser la répartition des charges. Le routage des paquets de données vers l'internet peut ainsi emprunter une voie tout à fait différente de celle qu'utiliseront les paquets en provenance d'Internet vers l'utilisateur.

Le filtrage des échanges P2P par empreinte numérique, donc l'identification des œuvres transitant sur les réseaux, supposerait donc de dédoubler le nombre de boîtiers nécessaires à l'analyse du trafic afin de surveiller tant le trafic montant que le trafic descendant, à supposer que la technologie démontre être capable d'analyser l'information recueillie pour reconstituer un flux donné.

- **La difficulté d'envisager un système à la demande**

La mise en œuvre d'un système de filtrage des échanges P2P à la demande de l'internaute imposerait aux FAI de faire évoluer leurs infrastructures pour leur implémenter un système particulièrement complexe de reconnaissance des internautes. En effet, ces derniers se voient le plus souvent attribuer des IP dynamiques, autrement dit se connectent à chaque fois avec une adresse IP différente : il n'est donc pas possible d'opérer ou non le filtrage sur la base des seules IP.

La construction de ce système serait extrêmement coûteuse et serait susceptible de provoquer des problèmes techniques et des latences préjudiciables aux autres services Internet, tout en étant promis à une obsolescence après quelque semaine, ainsi que nous l'analyserons plus loin dans l'analyse (III 2).

Un système de filtrage à la demande ne trouve en conséquence sa pertinence que dans une solution logicielle que l'utilisateur peut installer lui-même, s'il le souhaite, sur son poste de connexion. Un tel système permet en effet d'atteindre l'objectif souhaité, sans soulever les obstacles techniques que nous venons d'évoquer, ni les griefs d'inefficacité ou les obstacles juridiques que nous examinerons ci-dessous (III. 2 et IV).

3.2 L'inefficacité de la mesure face au chiffrement des échanges

Le filtrage des échanges P2P serait une mesure particulièrement inefficace, car obsolète quelques semaines ou quelques mois après son implémentation.

Les solutions de filtrage de contenu, notamment basées sur une technologie de reconnaissance d'empreintes numériques, sont en effet incapables de lire les flux chiffrés.

Par flux chiffré, il faut entendre le chiffrement des paquets par SSL, qui empêche d'en déterminer le contenu et le protocole, mais également le simple fait d'adjoindre une DRM à un fichier, même si cette DRM est « ouverte » autrement dit qu'elle ne comporte aucune restriction quant à l'utilisation de l'œuvre à laquelle elle s'attache.

S'agissant du chiffrement à proprement parler, un grand nombre de logiciels qui permettent des échanges P2P le proposent aujourd'hui en option. L'implémentation d'une mesure de filtrage sur les réseaux des FAI aurait pour conséquence inexorable de conduire les développeurs de logiciels de P2P à généraliser cette fonctionnalité ou son aisance d'utilisation. Cette généralisation du chiffrement des échanges peut être extrêmement rapide

et, contrairement à ce qui peut parfois être dit à ce sujet, particulièrement aisée pour n'importe quel internaute, même néophyte. Communiquer en P2P chiffré, lorsque la fonctionnalité est développée, n'est pas plus difficile que de consulter ses comptes bancaires en ligne, procédure utilisant également le chiffrement.

L'adjonction d'une DRM « ouverte » à un fichier rendant la reconnaissance de ce dernier impossible par un système de filtrage et pouvant être faite par n'importe quel internaute, il est par ailleurs certain que l'implémentation d'un système de filtrage sur les réseaux des FAI entraînerait l'adjonction systématique de telles DRM sur les fichiers partagés en peer-to-peer.

En conséquence, une solution de filtrage des échanges P2P, basée notamment sur la technologie dite de « *finger printing* », deviendrait obsolète et inutile peu de temps après son implémentation sur les réseaux des FAI, tant par l'utilisation de DRMs ouvertes en écoute à tous que par l'utilisation généralisée du chiffrement.

Il n'est pas, par ailleurs, imaginable d'interdire les flux chiffrés. Ce serait interdire l'utilisation du protocole https, donc interdire les échanges sécurisés sur le web. Cela porterait préjudice tant au développement du commerce en ligne qu'à la sécurité des internautes, lorsqu'ils transmettent des informations sensibles ou effectuent des opérations sur leurs comptes bancaires. Ces protocoles sont, également, largement utilisés par les entreprises pour protéger l'accès à leurs systèmes d'information.

L'interdiction des DRMs n'est pas plus envisageable.

4. Les risques juridiques du filtrage pour les fournisseurs d'accès à Internet

Les demandes de filtrage adressées aux fournisseurs d'accès par les autorités ou des tiers privés restent encore obscures quant à ses modalités. Toutefois, deux systèmes sont généralement évoqués, qui laissent entrevoir de nombreuses difficultés juridiques, que le filtrage en question concerne le web ou le peer-to-peer. Le premier système, relatif au web, consisterait pour les fournisseurs d'accès à Internet à bloquer l'accès à une liste de sites dressée par les autorités. Le second système, relatif au trafic peer-to-peer, consisterait pour les fournisseurs d'accès à bloquer les contenus dont l'empreinte correspondrait à une œuvre protégée dont l'empreintes figurerait dans une base de donnée constituée à cet effet avec l'aide des titulaires de droits.

Au-delà des difficultés posées par l'exclusion du juge, pourtant garant des libertés individuelles et du respect du principe de proportionnalité, de chacun de ces processus, l'AFA s'inquiète de conséquences juridiques de cette mesure pour ses membres.

- **L'entrave aux usages légitimes du réseau Internet**

Le blocage d'un serveur pour rendre inaccessible un contenu peut entraver l'accès à d'autres sites licites (jusqu'à plusieurs centaines de milliers si le site à bloquer est une page personnelle d'un hébergeur grand public). Dans l'exemple du blocage d'un site de jeux, protégé par la législation du lieu d'hébergement, les nombreux sites indûment bloqués pourraient engager la responsabilité du FAI. Les clients de ce dernier pourraient également reprocher à leur FAI de ne pas fournir le service auquel ils ont souscrit.

Cette même logique est applicable au blocage des contenus sur les réseaux peer-to-peer, dans le court laps de temps où les échanges ne seront pas chiffrés et qu'ils pourront donc être reconnus par le système. En effet, le fait qu'une œuvre soit protégée par des droits de propriété intellectuelle ne signifie pas que cette œuvre ne puisse pas être échangée ou vendue avec l'accord des titulaires de droits, ce que le système ne saura pas reconnaître. Par ailleurs, le système est susceptible de reconnaître, donc de bloquer, des œuvres composites ou des oeuvres plus brèves que l'œuvre originale (exemple des bandes-annonces) dont la distribution est parfaitement légitime. Enfin, ce système est faillible, donc susceptible de bloquer des œuvres sans rapport avec les empreintes d'œuvres protégées présentes dans la base de donnée.

- **La responsabilité des fournisseurs d'accès pour leur méconnaissance de la compétence exclusive du juge**

Le caractère illicite des sites web bloqués ou de l'échange des œuvres dont l'empreinte figure dans la base pourrait être contesté. En l'état actuel de la législation française mais également européenne, seul un juge (ou une autorité publique selon le système juridique envisagé) peut constater l'illégalité d'un site ou de l'utilisation d'une oeuvre. Ce principe a pour but d'assurer le respect de plusieurs droits fondamentaux, dont le droit à un procès équitable et le droit à la liberté d'expression, son corollaire étant la liberté d'accès à l'information.

Afin de garantir ces libertés individuelles, les fournisseurs d'accès ont d'ailleurs une obligation de neutralité face aux communications des utilisateurs de leurs services. Cette obligation, inscrite en droit français aux articles L. 32-1, II, 5° et D. 98-5 du Code des postes et des communications électroniques, est également une condition de la limitation de leur responsabilité. L'article L. 32-3-3 de ce Code, transposant l'article 12 de la Directive 2000/31/CE, prévoit en effet que la responsabilité des fournisseurs d'accès à Internet peut être engagée lorsque ces derniers ne respectent pas leur obligation de neutralité, notamment lorsqu'ils sélectionnent ou modifient les contenus qui font l'objet d'une transmission sur leur réseau.

Sans une décision de l'autorité judiciaire, la responsabilité du FAI bloquant l'accès à un site ou empêchant le transfert d'un fichier peer-to-peer pourrait donc être engagée. Une censure illégitime peut en effet entraîner toute une série de dommages pour l'éditeur du site, le diffuseur légitime d'un fichier ou l'internaute souhaitant accéder à l'information, à titre gratuit ou onéreux (entrave à l'exercice d'une activité économique, à la liberté de la vie privée, à la liberté d'accès à l'information…)

A cet égard, il convient de noter que la jurisprudence nationale, après avoir un temps retenu la compétence systématique des juridictions françaises pour juger les faits ou actes ayant eu pour support technique le réseau Internet dès lors que ces derniers étaient accessibles depuis la France et alors même qu'ils étaient hébergés à l'étranger, utilise désormais un critère d'attribution de compétence plus strict. Le nouveau critère, plus rationnel, n'admet la compétence territoriale des juridictions françaises que si les faits ou actes incriminés constatés sur Internet possèdent « un lien suffisant, substantiel ou significatif avec le dommage allégué ». Un tel lien doit être caractérisé au cas par cas : à défaut, le juge français lui-même ne pourrait se prononcer sur les actes ou faits incriminés.

- **L'atteinte à la vie privée et à la protection des correspondances**

Le risque juridique pesant sur les fournisseurs d'accès et exposé au développement précédent serait renforcé en matière d'échanges peer-to-peer.

En premier lieu, la mise en œuvre d'un système de filtrage des échanges de P2P qui ne serait pas à la demande des internautes serait certainement attentatoire au secret de la vie privée au sens de l'article 8 de la Convention européenne des droits de l'homme et de l'article 9 du Code civil français. La surveillance des activités des individus est ainsi considérée par la Cour de cassation française, hors-ligne, y compris sur la voie publique[4].

En second lieu, le blocage des échanges peer-to-peer par les fournisseurs d'accès serait sans doute contraire à la liberté de correspondance, également protégée par l'article 8 de la Convention européenne des droits de l'homme et dont l'atteinte est pénalement sanctionnée en droit français.

La protection accordée aux correspondances par le droit pénal bénéficie en effet à tout support de communication, quel que soit son mode d'acheminement[5]. Cette protection du support bénéficie au contenu de la communication, à compter du début de sa transmission jusqu'à ce que la dernière information ait été reçue par son destinataire[6]. Les conditions de cette protection tiennent à la définition même de la correspondance : la correspondance est la communication d'une information personnelle et temporelle, permettant l'interactivité, à une ou plusieurs personnes individualisées et déterminées[7].

A la lumière de cette analyse, il semble bien qu'une communication peer-to-peer soit par principe une correspondance protégée au sens du droit pénal. Une telle communication est en effet interactive, entre deux personnes déterminées et individualisées. Il reste à savoir si cette communication est toujours personnelle et temporelle, c'est-à-dire si elle est adaptée au destinataire à l'instant précis de la communication. Elle le sera sans doute dans la plupart des situations, le téléchargement d'un fichier étant la conséquence d'une requête précise du destinataire, répondant à ses besoins à l'instant de la communication.

Ainsi, la mise en œuvre par les FAI d'un système de filtrage des échanges de peer-to-peer ayant pour effet de bloquer certains fichiers selon les directives adressées au système par une base de donnée, conduirait ces prestataires à risquer de commettre, pour chacun de ces blocages, une interception de correspondance.

L'interception de correspondance par un fournisseur de service de communications électroniques est toutefois réprimée par l'article 432-9 du Code pénal français :
« *Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les*

[4] Voir par ex. Cass. Crim. 15 janv. 2003, inédit titré, n° de pourvoi 02-82278.
[5] T.corr. Seine, 10 juin 1959, D. 1959, p. 592, cité par E. De Marco, l'anonymat sur Internet et le droit », Thèse, Montpellier, 2005, n° 629.
[6] Virginie Peltier, Le secret des correspondances, PU d'Aix-Marseille, 1999, p. 471 ; E. De Marco, précité, n° 632.
[7] Virginie Peltier, Le secret des correspondances, PU d'Aix-Marseille, 1999, pp. 45, 222-227, 239 ; Michel Vivant, Christian Le Stanc, Lucien Rapp et al., Lamy droit de l'informatique, sous la resp. de Michel Vivant, 1997, n° 1676 ; E. De Marco, précité, n°s 627 – 637 ; sur l'individualisation et la détermination du correspondant voir également Pascal Reynaud, « Le fournisseur d'accès et la conservation des données engendrées par les communications électroniques », Com. com. elec., juin 2005, études, 23, not. p. 23.

cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45000 euros d'amende. »
« Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu. »

Ces dispositions ne sont que la transposition, adaptée pour appréhender le comportement des personnes disposant d'un pouvoir technique particulier sur les correspondances, de l'interdiction générale d'atteindre le secret des correspondances, mentionnée à l'article 226-15 du Code pénal :
« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende. »
« Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. »

Le système de filtrage proposé conduirait donc les fournisseurs d'accès à porter atteinte à la liberté des correspondances, de manière intentionnelle, autrement dit à commettre un délit passible de trois ans d'emprisonnement et de 45 000 euros d'amende.

- **L'insécurité juridique née du traitement de données à caractère personnel**

La mise en œuvre d'un système de filtrage des échanges peer-to-peer impliquerait, pour le fournisseur d'accès, d'opérer un traitement des adresses IP d'internautes susceptibles d'avoir échangé illégalement des données.

Un tel traitement répondrait exactement à la définition du traitement de données à caractère personnel relatives à des infractions, que les FAI n'ont pas l'autorisation de mettre en œuvre en vertu de l'article 9 de la loi française n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par loi n°2004-801 du 6 août 2004 :

Une donnée à caractère personnel est en effet, selon l'article 2 de la loi du 6 janvier 1978, « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.* ».
Une adresse IP permettant d'obtenir l'identification précise d'un utilisateur en raison des éléments d'identification détenus par le FAI constitue bien un « *numéro d'identification* » relatif à une personne physique « *qui peut être identifiée* », compte tenu de « *l'ensemble des moyens (permettant) son identification (détenus par) le responsable du traitement ou toute autre personne (notamment le FAI) »*.

Un traitement de données à caractère personnel est par ailleurs *« toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».*

Un traitement de données à caractère personnel relatif à des infractions suppose enfin qu'un lien soit établi entre les données personnelles et des infractions, « présumées ou réelles »[8]. Il s'agit bien, dans notre espèce, de faire un lien entre une adresse IP et une contrefaçon présumée.
Seuls les juridictions, les auxiliaires de justice et les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du Code de la propriété intellectuelle peuvent toutefois procéder à de telles associations au sein d'un traitement de données à caractère personnel, sous réserve pour les deux derniers acteurs d'avoir procédé à une déclaration auprès de la Commission française de protection des données personnelles (CNIL) ou d'y avoir été autorisé par cette Commission.

L'article 9 de la loi de 1978 dispose en effet :
« *Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par :*
1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;
2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;
3° [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]
4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits ».

En conséquence, la mise en place d'un système de filtrage des échanges peer-to-peer impliquerait, pour les FAI, de méconnaître les dispositions de l'article 9 de la loi du 6 janvier 1978. Une telle méconnaissance est sanctionnée de cinq ans d'emprisonnement et de 300 000 euros d'amende sur le fondement de l'article 226-19 du Code pénal :

« Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté ».

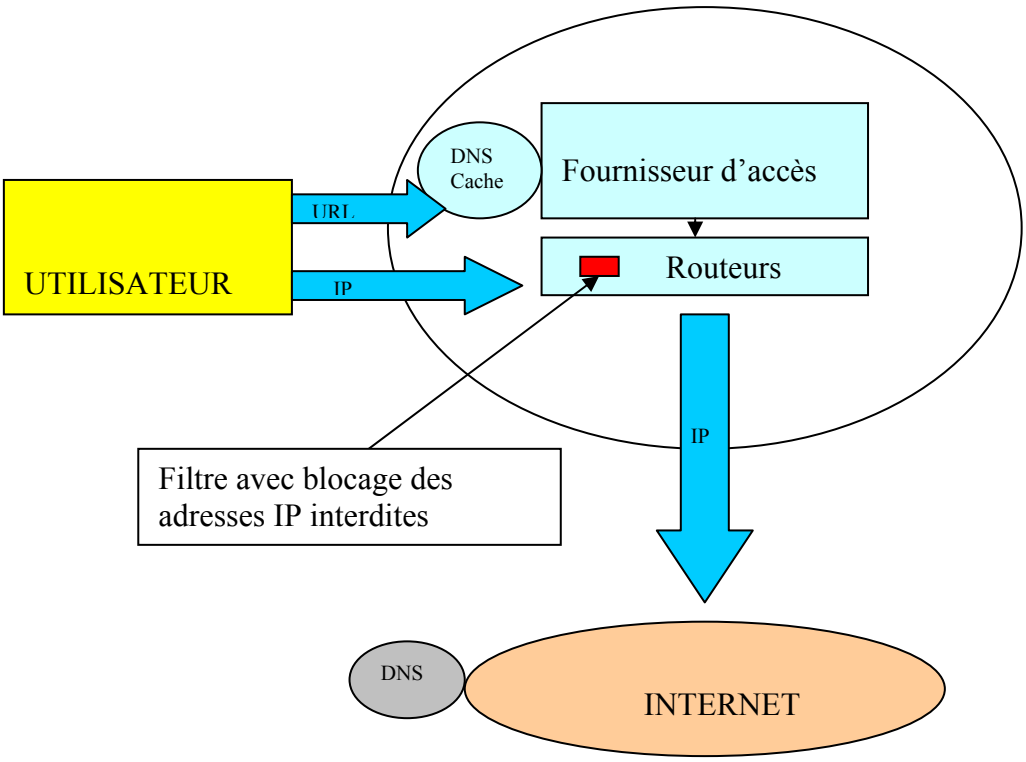
- **L'insécurité juridique née du caractère déceptif de la mesure**

Enfin, la responsabilité du fournisseur d'accès (privé ou public) devrait être clarifiée en cas de contournement massif de la méthode de filtrage, en cas de défaillance technique ou d'incapacité matérielle à réaliser la mesure de filtrage. Le caractère déceptif de cette mesure si elle échouait ne doit pas être négligé.

[8] TGI Paris, 25 juin 2007, société neuf cegetel et autres c. société Techland.

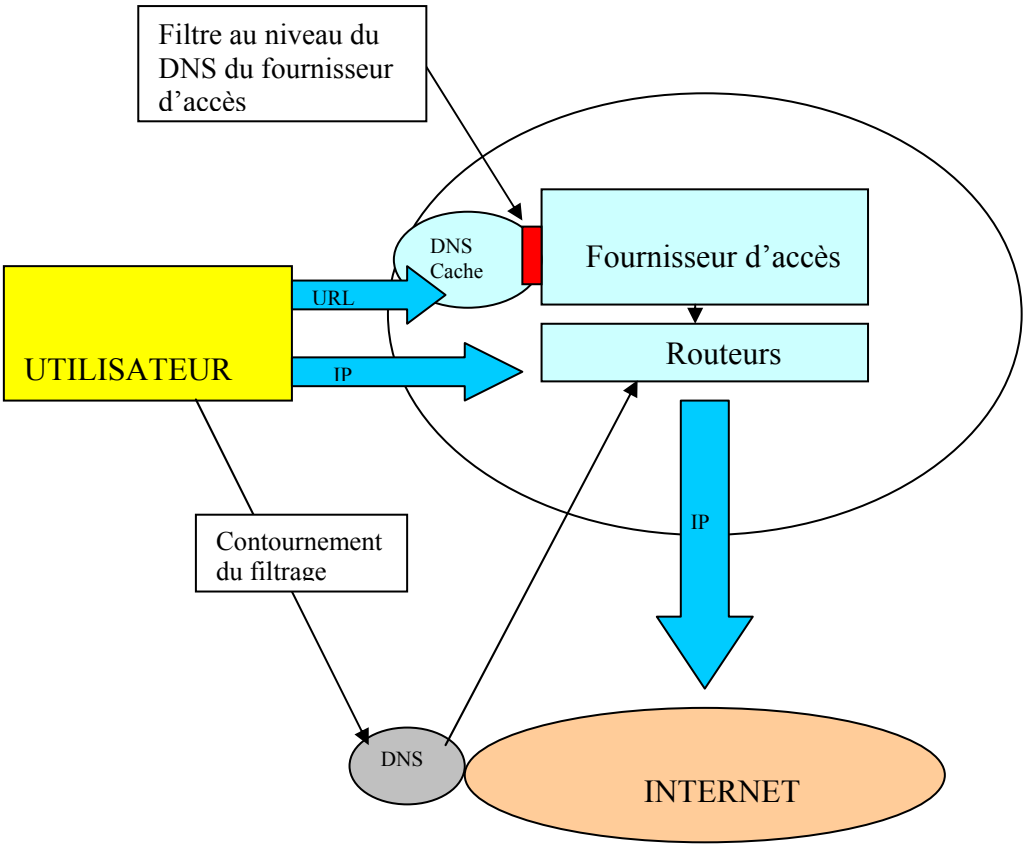
ANNEXE 1

FILTRAGE DE L'ACCES AU NIVEAU DE L'ADRESSE IP



ANNEXE 2

FILTRAGE DE L'ACCES AU NIVEAU DU DNS



ANNEXE 3

FILTRAGE DE L'ACCES AU NIVEAU DE L'URL