Voici un dossier comportant quelques articles sur Internet qui concernent les lois HADOPI et ont attiré notre attention

http://www.zataz.com/news/19011/HADOPI--anonyme--anonymat--tracer--telechargement.html

Loi HADOPI ? Mise à mal en 3 secondes chrono

Publié le 14-05-2009 à 13:06:45 dans le thème Lois - Justice

Pays : France - Auteur : Damien Bancal

Exclusif : La loi HADOPI a été adoptée par la France. Elle va permettre de punir les copieurs à partir de leur IP. Démonstration.

Dans la forme, la loi Création et Internet parait plus que nécessaire. Trop de copieurs, trop d'argent engrangé par les pirates, ... Il fallait, indiquent les députés, mettre fin aux différents trafics et débordement sur Internet. Bilan, 54 % des députés ont voté en faveur de la réponse graduée. Dés octobre, à partir de l'adresse IP des copieurs, des courriers d'avertissements seront envoyés par la Haute Instance en charge de faire respecter la loi. Les récidivistes pourront voir leurs connexions coupées de 2 à 12 mois.

Sauf qu'il va être intéressant de voir comment *HADOPI* va combattre l'exemple très concret que la rédaction de ZATAZ.COM va vous présenter.

Comme vous devez le savoir maintenant, les connexions Internet, P2P, Email, FTP, IRC, ... se font d'IP à IP. *001* contacte *002* et conversent ensemble. Les députés, en votant HADOPI, sont persuadés qu'à partir de cet élément il sera tout à fait possible de remonter aux copieurs. Piratage de l'IP ? A l'internaute de se protéger. Pour ce faire, il va devoir "*s'équiper*" d'un cerbère qui est censé le protéger et prouver sa bonne fois. Un firewall qui va logguer entrées et sorties dans la machine de l'internaute ? Même la ministre de la culture ne sait pas encore comment agir.

Les internautes souhaitant un peu d'anonymat sur la toile savent qu'il est possible d'utiliser l'IP d'un tiers. Pas besoin d'être un "*génie*" [Ca n'existe pas, NDR] de l'informatique pour le faire. Pas besoin de sortir l'artillerie lourde du "piratin" ou autres "hackers" pour se faire passer pour une autre machine. Il existe sur la toile plusieurs sites Internet proposant des IP venus d'ailleurs. Des serveurs, des machines pouvant servir de proxies, comme connexion de rebond. *001* passera par le proxy *007* pour joindre *002*. Bilan, *002* pensera voir passer *007* en lieu et place de *001*. Un site Français annonce mettre en place ce genre de "sécurité". Son nom ? *IPODAH* (HADOPI à l'envers, NDR]

Là ou cela peut malheureusement devenir très cocasse est que dans les IP diffusées, nuits et jours, par les sites en question peuvent être ... troublants pour les chasseurs de pirates. Il est possible de trouver de petites perles bien françaises. Prenons un seul exemple, nous en avons des dizaines dont plusieurs basés à Cannes, du côté du festival.

Il y a quelques heures, un des portail dédiés aux proxies nous a proposé d'utiliser l'adresse 84.14.247.119. Nous aurions pu le faire dans la mesure ou nous avions besoin d'un peu de distance entre des pirates d'un forum russe et notre connexion de rédaction. Sauf que l'IP en question n'est rien d'autre que celui de la Banque Postale.

Updated in RealTime Free Socks 5 Proxy Lists.

IP:Port Host name	Hosting country	Last good check (hh:mm:ss ago)	Uptime %
76.88.241.19:4987	--	00:01:16	100.0%
76.11.129.53:44639	--	00:02:16	50.00%
84.14.247.119:1080	--	00:07:16	93.10%
81.27.108.62:443	--	00:10:16	79.75%
68.47.34.162:48891	--	00:10:16	56.39%
68.48.30.70:46447	--	00:10:16	63.33%
24.184.196.124:30427	--	00:20:16	56.52%
68.41.100.199:49141	--	02:12:16	51.61%
68.48.134.218:35601	--	03:29:16	29.59%

Nous imaginons déjà la tête des fonctionnaires en charge de l'HADOPI face à ce genre d'IP.

HADOPI va-t-elle être capable de gérer les « demandes » ? L'internaute aura-t-il connaissance du premier avertissement ? Plus d'un système anti spams risque de « tilter » vue l'affluence des courriels annoncés. A noter qu'un internaute suspendu chez Orange pourra se réabonner chez un autre FAI, ou sous un autre nom. On parle de double peine (coupure + paiement de l'abonnement) alors qu'en fait HADOPI en signe une triple de peine. Le volet pénal de la *loi DADVSi* existe toujours. Il n'a pas été aboli. HADOPI pourra se cumuler avec les 300,000 euros d'amende et jusqu'à 5 ans de prison ferme proposé par la loi DADVSi. Dernier petit point de taille. Les Fournisseurs d'Accès indiquent ne pas pouvoir couper Internet tout en laissant ouvert le téléphone et la télévision dans les abonnements triple play.

Pour finir, bon courage aux utilisateurs lambda qui pensent être sur des sites légaux. Des sites pirates qui ressemblent comme deux goûtes d'eau [*Lire*] à des sites licites pullulent sur la toile. A lire, d'ailleurs, un comparatif dans le magazine CAPITAL, en kiosque en ce moment chez vos marchands de journaux.

Bref, le casse tête ne fait que commencer... Bonjour chez vous !

http://archives.lesechos.fr/archives/2009/lesechos.fr/09/16/300376175.htm

hightec • actu
Lesechos.fr • Le 16 septembre 2009

La loi Hadopi validée, mais déjà dépassée

Au terme d'une saga de près de deux ans, avec de nombreux rebondissements, le projet de loi contre le téléchargement illégal a été adopté mardi par les députés. Mais le texte est déjà largement dépassé du point de vue technologique.

Validée , la loi Hadopi ne fait guère trembler les pirates. D'abord parce que contre le téléchargement illégal, entamée il y a près de deux ans, n'a pas encore reçu son point final. Une commission mixte paritaire, composée de sept sénateurs et de sept députés, a validé ce mercredi la version du texte votée par les députés. La version finale du projet de loi doit maintenant faire l'objet d'un vote définitif le 21 septembre au Sénat et le 22 à l'Assemblée. Autre étape à prévoir : devant le Conseil constitutionnel, qui avait déjà invalidé en juin dernier une partie du premier texte sur l'Hadopi. Une fois les fourches caudines des sages passées, il faudra encore publier la loi, mettre en place la Haute autorité pour la diffusion des oeuvres et la protection des droits sur Internet (Hadopi) et commencer à envoyer les mails d'avertissement aux internautes concernés.

Mais, surtout, les pirates savent d'ores et déjà largement contourner les limites posées par la loi. Il est vrai que plus un texte portant sur des nouvelles technologies tarde à être adopté, plus il a de chances d'être périmé lors de sa publication. Avec son parcours sinueux, l'Hadopi n'échappe pas à la règle. Et nul besoin d'être un spécialiste en informatique pour pirater aujourd'hui en toute tranquillité, ou presque. Une simple recherche sur Internet permet de trouver, en quelques secondes, toutes sortes de moyens -qui restent le plus souvent illégaux, il faut le rappeler- pour lire des contenus multimédias sans payer le prix fort, tant du point de vue pécuniaire que judiciaire. Au lendemain du vote de la loi Hadopi, la requête "contourner Hadopi" recueille ainsi 58.700 réponses dans Google. Parmi les mieux classées, les titres sont explicites : "10 antidotes anti-Hadopi ", "top 10 des astuces pour contourner Hadopi" ou encore "contourner HADOPI en 27 secondes".

Sanctionner les députés

Certains sites enjoignent à la *"résistance"*, faisant vibrer la fibre "citoyenne" des internautes. Ils conseillent donc de *"contester systématiquement"* les avertissements envoyés par l'Hadopi ou encore de *"voter"* pour sanctionner les élus qui ont validé l'Hadopi. Et surtout, affirment-ils, il ne faut *"pas avoir peur"*, car il est statistiquement peu probable de recevoir un avertissement de l'Hadopi. Le blog linuxmania a fait le calcul : *"Sachant qu'au moins 5 millions de français utilisent le P2P régulièrement, vous recevrez donc, en moyenne, un email d'avertissement tous les 500 jours soit tous les ....16 mois."* Soulignant que *"les compteurs HADOPI sont remis à 0 tous les 6 mois"*, le blog conclut qu'il n'y a pas de quoi s'inquiéter.

D'autres sites suggèrent des techniques plus radicales. Ils rappellent qu'il est toujours possible de transférer un contenu multimédia entre amis grâce à un CD/DVD gravé ou une clé USB. Cela reste illégal, mais rien ne transite par Internet. D'autres suggèrent de télécharger à partir du réseau wi-fi non protégé d'un voisin imprudent. C'est son adresse IP qui sera identifiée, et il sera légalement considéré comme responsable des piratages.

Outre ces pratiques peu sophistiquées, la toile regorge de solutions plus technologiques pour pirater l'esprit léger, à défaut d'avoir la conscience complètement tranquille. Les sites de "streaming" sont notamment plébiscités. La lecture en continu permet de lire un flux audio ou video à mesure qu'il

est diffusé. Il y a bien un téléchargement, mais seulement temporaire et partiel. Les données disparaissent au fur et à mesure qu'elles sont lues, et ne sont donc pas stockées durablement sur l'ordinateur de l'internaute. L'offre en streaming est très vaste, les sites se rémunérant généralement grâce à la publicité qui encadre la séquence visionnée. Et même les chaînes de télévision historiques proposent une partie de leurs programmes en lecture en continu sur leurs sites internet.

Masquer les adresses IP

Autre option : le "direct download", ou téléchargement direct. Il permet, comme son nom l'indique, de télécharger un fichier multimédia, mais cette opération s'effectue à partir d'un serveur central, rattaché à un site web proposant des contenus, et non en utilisant les ressources de plusieurs utilisateurs, comme c'est le cas dans le "Peer to peer" classique (téléchargement en pair à pair). L'avantage pour l'internaute est que son adresse IP n'est connue que des administrateurs du site de téléchargement direct. Et, pour espérer y accéder, il faut déposer plainte et perquisitionner. Or, les sites de téléchargement direct sont le plus souvent basés à l'étranger, donc hors de la juridiction française.

Les pirates peuvent aussi masquer eux-mêmes leur identité. Il suffit pour cela de passer par un proxy anonyme (ou encore via un serveur VPN) qui dissimule l'adresse IP de l'internaute sous une autre adresse IP, généralement basée à l'étranger. Le site web consulté verra la fausse identité, et non la vraie. Certains systèmes, facilement accessibles sur internet, proposent même de brouiller encore plus les pistes en changeant en permanence et automatiquement les fausses adresses IP, tout en cryptant les communications, ce qui fait qu'il devient impossible de savoir de quelle nature (texte, image, vidéo, audio...) est le fichier transféré. Pour résister à l'Hadopi, le classique peer to peer devient, lui aussi, de plus en plus anonyme et sécurisé.

Enfin, certains sites proposent de suivre la loi à la lettre en installant un logiciel espion sur son ordinateur, mais en l'isolant dans un second système d'exploitation ou sur un second disque dur. Le logiciel espionnera donc en vain, puisque d'éventuelles pratiques frauduleuses de l'internaute s'effectueront dans un autre espace. Mais son installation devrait permettre de contester un avertissement, en renvoyant à l'Hadopi le disque dur équipé du mouchard et vierge de tout téléchargement.

La liste est loin d'être exhaustive, mais elle illustre bien le fait que la loi n'est même pas promulguée qu'elle est déjà largement dépassée du point de vue technologique. Ironie de l'histoire : les techniques de piratage "sécurisé", réservées il y a encore peu aux seuls pros de l'informatique, se sonr démocratisées à la faveur du débat sur l'Hadopi, provoquant donc l'effet inverse de celui recherché.

Reste que, au-delà des considérations technologiques, la question de fond demeure : quel modèle économique pour le multimédia en ligne ? Un sujet sur lequel doit plancher la nouvelle commission mandatée par le ministre de la Culture Frédéric Mitterrand et confiée à Patrick Zelnik, le président du label Naïve, Jacques Toubon et Guillaume Cerutti, président de Sotheby's France. Leurs conclusions sont attendues d'ici au début du mois de novembre.

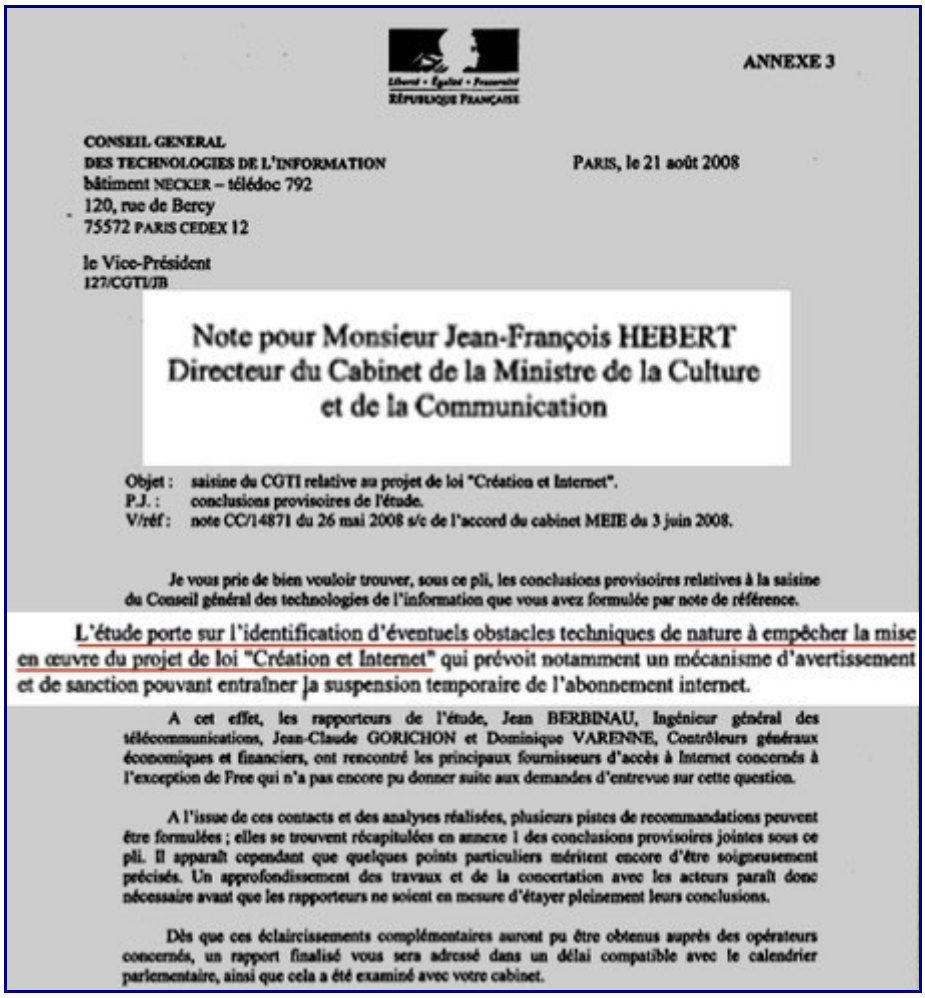
http://www.marianne2.fr/Exclusif-la-loi-Hadopi-chere-et-inefficace_a176970.html

Exclusif : la loi Hadopi chère et inefficace…

Emmanuel Lévy avec Sylvain Lapoix | Samedi 14 Mars 2009 à 07:00 | Lu 27333 fois

Annexé au projet de loi Création et Internet défendu par Christine Albanel, le document que s'est procuré Marianne prouve que les options retenues par le ministère de la Culture pour lutter contre le téléchargement illégal seraient coûteuses à mettre en place et techniquement inefficaces. Marianne2.fr publie en exclusivité cette note confidentielle.

C'est un rapport, désormais public, que les députés s'apprêtant à voter la loi Création et Internet, et son volet répression du téléchargement, n'ont malheureusement pas reçu dans leur casier. Pas plus que les annexes, qui elles demeurent confidentielles et dont *Marianne* a pu prendre connaissance.



ANNEXE 3

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GENERAL
DES TECHNOLOGIES DE L'INFORMATION
bâtiment NECKER – télédoc 792
120, rue de Bercy
75572 PARIS CEDEX 12

PARIS, le 21 août 2008

le Vice-Président
127/CGTI/JB

Note pour Monsieur Jean-François HEBERT
Directeur du Cabinet de la Ministre de la Culture et de la Communication

Objet : saisine du CGTI relative au projet de loi "Création et Internet".
P.J. : conclusions provisoires de l'étude.
V/réf : note CC/14871 du 26 mai 2008 s/c de l'accord du cabinet MEIE du 3 juin 2008.

Je vous prie de bien vouloir trouver, sous ce pli, les conclusions provisoires relatives à la saisine du Conseil général des technologies de l'information que vous avez formulée par note de référence.

L'étude porte sur l'identification d'éventuels obstacles techniques de nature à empêcher la mise en œuvre du projet de loi "Création et Internet" qui prévoit notamment un mécanisme d'avertissement et de sanction pouvant entraîner la suspension temporaire de l'abonnement internet.

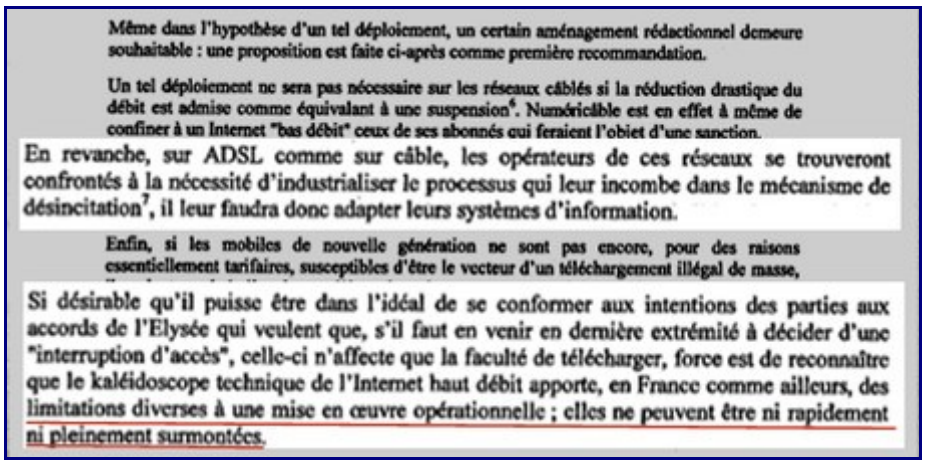
A cet effet, les rapporteurs de l'étude, Jean BERBINAU, Ingénieur général des télécommunications, Jean-Claude GORICHON et Dominique VARENNE, Contrôleurs généraux économiques et financiers, ont rencontré les principaux fournisseurs d'accès à Internet concernés à l'exception de Free qui n'a pas encore pu donner suite aux demandes d'entrevue sur cette question.

A l'issue de ces contacts et des analyses réalisées, plusieurs pistes de recommandations peuvent être formulées ; elles se trouvent récapitulées en annexe 1 des conclusions provisoires jointes sous ce pli. Il apparaît cependant que quelques points particuliers méritent encore d'être soigneusement précisés. Un approfondissement des travaux et de la concertation avec les acteurs paraît donc nécessaire avant que les rapporteurs ne soient en mesure d'étayer pleinement leurs conclusions.

Dès que ces éclaircissements complémentaires auront pu être obtenus auprès des opérateurs concernés, un rapport finalisé vous sera adressé dans un délai compatible avec le calendrier parlementaire, ainsi que cela a été examiné avec votre cabinet.

Extrait de la note : page de garde

Produit par les crânes d'œufs du Conseil général des technologies de l'information (CGTI), en gros le corps des ingénieurs telecom, ce rapport (en téléchargement ci-dessous) réalisé à la demande des ministères de l'économie et de la culture, est on ne peut plus sévére sur la faisabilité technique de la coupure du flux internet pour acte de piratage.



Même dans l'hypothèse d'un tel déploiement, un certain aménagement rédactionnel demeure souhaitable : une proposition est faite ci-après comme première recommandation.

Un tel déploiement ne sera pas nécessaire sur les réseaux câblés si la réduction drastique du débit est admise comme équivalant à une suspension[6]. Numéricâble est en effet à même de confiner à un Internet "bas débit" ceux de ses abonnés qui feraient l'objet d'une sanction.

En revanche, sur ADSL comme sur câble, les opérateurs de ces réseaux se trouveront confrontés à la nécessité d'industrialiser le processus qui leur incombe dans le mécanisme de désincitation[7], il leur faudra donc adapter leurs systèmes d'information.

Enfin, si les mobiles de nouvelle génération ne sont pas encore, pour des raisons essentiellement tarifaires, susceptibles d'être le vecteur d'un téléchargement illégal de masse,

Si désirable qu'il puisse être dans l'idéal de se conformer aux intentions des parties aux accords de l'Elysée qui veulent que, s'il faut en venir en dernière extrémité à décider d'une "interruption d'accès", celle-ci n'affecte que la faculté de télécharger, force est de reconnaître que le kaléidoscope technique de l'Internet haut débit apporte, en France comme ailleurs, des limitations diverses à une mise en œuvre opérationnelle ; elles ne peuvent être ni rapidement ni pleinement surmontées.

Extrait de la note : page 2

Le projet de loi Création et Internet, défendu bec et ongle par Christine Albanel dans l'hémicycle, prévoyait la coupure de la connexion Internet de toute personne ayant procédé à des téléchargements illégaux. Or, sur chacun des points de cette *« répression du piratage »*, la note confidentielle met à mal les rêves de filtre infaillible de la ministre de la Culture.

Premier souci : difficile de savoir qui utilise un réseau filaire ou sans fil pour récupérer des films sur un réseau. Entre les réseaux Wifi publics, les téléphones portables bientôt assez puissants pour télécharger ou les accès en entreprise, la note recense toutes les failles du système qui empêchent d'identifier le *« coupable »*. Difficile d'attraper le voleur quand on n'a identifié que l'échelle !

La coupure même de la connexion Internet pose ensuite la question des offres « triple play », combinant accès au web, téléphone et télévision. Interrompre la connexion, c'est empêcher de télécharger... mais aussi de passer des coups de fil et de regarder TF1 ! Les solutions techniques impliquent pour les fournisseurs d'accès *« d'industrialiser la procédure »* permettant de ne couper qu'une partie du service, autrement dit de modifier tous leurs modems afin de permettre à l'Etat de couper l'accès au web !

Un frein parmi d'autres qui amène les conseillers techniques à conclure que les limitations prévues par la loi *« ne peuvent être ni rapidement ni pleinement surmontées. »*
Faute de trouver le raccourci technique magique auquel rêvait le ministère de la Culture, ils prônent la modification d'un terme crucial du projet de loi : à *« suspension »* du service Internet, *« il sera alors préférable de substituer le mot restriction. »*

Et c'est un argument que beaucoup avaient oubliés pour contrer la loi Hadopi : avant d'être liberticide ou rétrograde, elle est avant tout sarkozyste. C'est-à-dire, à l'instar des heures supplémentaires ou du paquet fiscal, foncièrement chère et inefficace !

Mis à jour samedi 14 mars 2009 à 10h10.

http://linuxmanua.blogspot.com/2009/04/10-antidotes-anti-hadopi.html

10 antidotes anti-Hadopi

Alerte rouge :

Alors que le pays sombre dans une grave crise économique, la priorité de nos gouvernants .... c'est HADOPI :

Répression massive des internautes.

Sans intervention de l'institution judiciaire.

Sans contrôle possible de la CNIL.

Sur la base de dénonciations massives d'officines privées, sans preuves.

300.000 emails d'accusation par mois sans contestation possible.

90.000 lettres recommandées par mois sans contestation possible.

30.000 coupures par mois de l'accès à internet, pour une durée de 1 an, avec des possibilités de contestation totalement délirantes.

La présomption d'innocence ne s'applique pas. La charge de la preuve est renversée : c'est à vous de prouver que vous êtes innocent.

Quasi obligation de mettre sur son PC un logiciel (payant) espionnant en temps réel vos communications y compris vos emails.

Adoption du principe du sur-référencement : l'ordre d'apparition des sites Web, sur les moteurs de recherche, sera décidé par l'Etat.

Adoption du principe de filtrage du Web : on va décider pour vous ce que vous pourrez consulter ou non.

Toutes les lignes rouges sont franchies.

Rejeté de justesse, par l'Assemblée Nationale le 9 avril 2009, ce texte de loi fera l'objet d'un nouveau vote le 12 mai. Les parlementaires godillots la voteront certainement, cette fois-ci, après avoir reçu les instructions de vote.

Afin de **contourner HADOPI et vous préparer à la résistance totale et à la riposte** face à ce venin totalitaire, vous trouverez ci-dessous **les 10 premiers antidotes.** D'autres solutions suivront.

N'hésitez pas à rajouter, en commentaires, vos propres solutions. Je compléterai ainsi régulièrement cet article.

Antidote n°1 : Ne pas avoir peur

HADOPI prévoit, en vitesse de croisière, 10.000 emails d'avertissement par jour.

Sachant qu'au moins 5 millions de français utilisent le P2P régulièrement, vous recevrez donc, en moyenne, un email d'avertissement tous les 500 jours soit tous les ....16 mois.

Sachant que les compteurs HADOPI seront remis à 0 tous les 6 mois, vous pouvez dormir tranquille ... PC allumé bien sur.

Sachant qu'HADOPI n'arrivera jamais à identifier quotidiennement 10.000 internautes, afin de leur envoyer un mail ou une lettre, vous pouvez même faire la grasse matinée.

Sachant que la date annoncée d'application de Hadopi est 2011, autant dire 1 siècle en temps Internet, il est donc totalement prématuré de se précipiter, en apnée, vers des solutions sécurisées de protection de la vie privée.

De plus, en 24 mois, de nouvelles solutions techniques de contournement vont bientôt être proposées, avec de beaux boutons en couleurs et des paramétrages toujours plus simples.

Antidote n°2 : Contester systématiquement

Votre contestation est nulle car non prévue dans cette "loi".

Contestez quand même.
Réponses possibles au mail ou à la lettre :

- Vous n'avez pas Internet,
- Vous ne comprenez pas leur email,
- Satan a piraté votre Wifi,
- Belzébuth et Lucifer habitent vos enfants,
- Signalez poliment l'erreur : L'IP incriminée dans le mail ne correspond pas à votre n° de Sécurité Sociale,
- Ce n'est pas votre IP mais celle du voisin (donnez un nom),
- A cette date là, vous étiez en vacances à l'étranger (insérez des photos, minimum 10 Mo par photo),
- Adoptez un profil bas : Excusez-vous platement de devoir leur demander de bien vouloir aller se faire foutre,
- Chuck Norris ne souhaite pas être dérangé,
- etc ....

Aucun système administratif ne peut faire face à 20.000 contestations par jour : 10.000 x 2 car vous n'oublierez pas de contester par 2 mails séparés:

1 mail pour contester, 1 mail pour confirmer la contestation voire un 3eme

pour leur demander s'ils ont bien pris en compte vos mails ou pour relancer, ou pour exiger des excuses ... etc.

La prévention c'est important : Contestez même si vous n'avez pas reçu de mails. Essayez d'être aussi cons qu'eux, il y a encore de la marge.

Cerise sur le gâteau : Mettre en copie, par un simple et unique copier coller, les 296 députés pro-Hadopi.

En attendant, la mise en place de la Loi, vous pouvez vous entrainer avec les emails des créateurs de cette loi magnifique :

- friester@assemblee-nationale.fr
- flefebvre@assemblee-nationale.fr
- pgosselin@assemblee-nationale.fr
- philippegosselin50@orange.fr

(Inutile de les inscrire sur des sites de cul. C'est déjà fait)

Antidote n°3 : Voter

Hadopi, maintenant ou en 2011, est une inacceptable attaque contre nos libertés individuelles et nos vies privées.

Aux prochaines élections et ce jusqu'au retrait de cette «loi» : Votons et catapultons les, loin, très loin, là-bas, sur la Lune.

Inscrivez vos élus fautifs à ce beau voyage : Par courtoisie, envoyez également un email à votre député pour l'informer que vous ne renouvellerez pas son CDD, ainsi que celui de ses collègues, à l'occasion des prochaines élections.

Voici comment contacter votre Député

Vous voulez connaître l'attitude de votre député concernant cette loi ?

Restez assis, voici la liste des collabos [Mise à jour du 12/05]. Un rappel de cette liste sera fait avant chaque élection.

Vous aussi, vous pouvez votez : Plan de Résistance

Antidote n°4 : Le Streaming Vidéo

- Facilité : 5/5
- Avantage : catalogue important, indétectable
- Inconvénient : parfois publicité ou restriction de durée
- Le "must" : installer un câble HDMI entre le PC et la TV. Avec cela, n'oubliez pas de ~~télécharger~~ d'acheter des cacahouètes.

Les meilleurs sites de streaming : Liste 1, Liste 2, Liste 3, Liste 4, Liste 5

Quelques noms : MégaVidéo, AlloStreaming, Lookiz

Bien souvent, ces sites limitent le temps de streaming à 72 minutes pour inciter les accros des séries à passer à l'abonnement payant mais des solutions existent pour outrepasser ces restrictions. Parmi elles, une extension pour Firefox (Illimitux).

Vous pouvez aussi utiliser des débrideurs en ligne (Mega-Unlimited, MegaStreaming, Rapid8...). Voici une liste complémentaire de débrideurs gratuits.

Télécharger 1 vidéo en streaming :

- ***Méthode 1 :*** avec Firefox + VideoDownloadHelper ou Youtube to MP3 ou Easy Youtube Downloader (MP4 possible).
- ***Méthode 2 :*** Des applications en ligne (Gazzump, Dirpy,...) permettent, sans rien installer, de transformer une vidéo en streaming en tout ce qu'on veut (MP3, AVI, WMV, WAV, MOV, FLV). Il suffit de taper le nom de sa chanson.
- ***Méthode 3 :*** RealPlayer. En visionnant une vidéo en streaming, cliquez sur "Télécharger cette vidéo". Les fichiers ainsi obtenu avec l'extension ".FLV" peuvent se lire notamment avec VLC.
- ***+ 24 autres Méthodes :*** sur Mashable

Antidote n°5 : La Musique en ligne

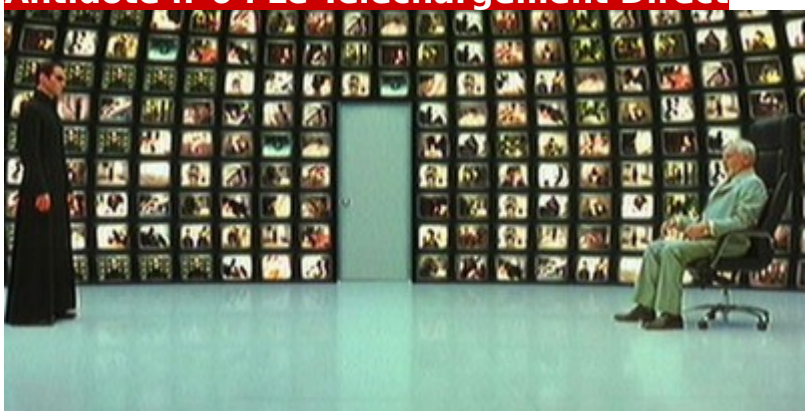
- Facilité : 5/5
- Avantage : Catalogue énorme, indétectable

20 sites gratuits de Musique en ligne

Si vous avez vraiment besoin du fichier mp3, des méthodes permettent d'enregistrer une musique en streaming en quelques secondes :

- ***Méthode n°1 :*** Streamy (Windows, Linux) qui a le gros avantage de récupérer tout seul le nom du morceau et de l'album. Et oui, pourquoi se fatiguer ? Ne marche pas avec D****r mais marche très bien avec J**a. Pour l'installation sous Linux, installez au préalable le paquet ffmpeg.
- ***Méthode n°2 :*** TubeMaster++ (Windows, Linux, Mac). Tutoriels : Tuto1, Tuto2.
- ***Méthode n°3 :*** En configurant sa carte son + Audacity.

Antidote n°6 : Le Téléchargement Direct



- Facilité : 4/5
- Avantage : Catalogue important, méthode imparable

Les sites de téléchargement direct échappent complètement à la surveillance car les adresses IP des internautes qui s'y connectent ne peuvent pas être collectées sans la collaboration des fournisseurs d'accès à Internet. Avec ce type de site, les fichiers sont hébergés sur des serveurs centraux et ne sont pas partagés.

L'adresse IP de l'internaute en train de télécharger n'est pas « visible » par un

tiers sur Internet. Seuls les administrateurs du site de téléchargement direct en ont connaissance. Pour y accéder, il faut déposer plainte et perquisitionner. Or tous ces sites sont basés à l'étranger et ne sont pas concernés par la loi française.

Oui, c'est cela aussi la mondialisation. On nous avait pourtant dit qu'il fallait nous y adapter.

Voici les 2 principaux sites de stockage en ligne permettant de faire du téléchargement direct :

- RapidShare
- MegaUpload

Allons droit au but : Mega-films, LibertyLand, ... sont des annuaires de films. Il n'y a plus qu'a cliquer pour télécharger.

Voici les moteurs de recherche qui vont avec et qui vous aideront à trouver des films et des mp3 :

- Download any stuff
- Fileonfire
- GammaFiles
- Schufs
- Buskka
- Rapidzearch
- FileTube
- 4megaupload
- Megadownload
- Ddlsearch.free

.... sans oublier les inévitables astuces :

Astuces pour MegaUpload :

Télécharger sans limite :>Ici<
Transformer un compte membre en compte Premium : >Ici<

Il existe une multitude d'extensions Firefox spécialisées. A noter, entre autres :

- MegaUpload Time Attack
- MU Bundle Final
- Skipscreen
- MegaUpload DownloaderHelper

Astuces pour RapidShare :

3 outils complémentaires : >Ici<
Gérer les files d'attente : >Ici<

Autres astuces :
Uploadez sur 12 sites de stockage en même temps : Upload Mirrors
Gestionnaire de Téléchargement : Cryptload
L'extension Firefox Universal Uploader permet de charger/télécharger avec une interface, simple, sur vos sites de téléchargements préférés.

Voici les super moteurs de recherche de MP3 dont le terrain de jeu est l'intégralité du Web :
10 sites de téléchargement de MP3

Il y a aussi les Newsgroups qui sont des serveurs ou vous pouvez échanger anonymement et trouver tout ce que vous voulez :

- *Avantage :* Rapidité, Choix, Anonymat complet.
- *Inconvénient : Payant par forfait mensuel.*
- Explications synthétiques sur les Newsgroups : >Ici<
- Explications complètes de A à Z sur Info du Net
- Choisissez la meilleure offre : >Ici<
- Télécharger sur les Newsgroups Usenet avec Giganews : >Ici<

Et pour finir, n'oublions pas les discrets mais néanmoins rapides et efficaces **Boards Warez** (Wawa Mania et Compagnies)

Antidote n°7 : Le P2P Sécurisé

Vous trouverez sur le lien ci-dessous **3 techniques imparables de Peer to Peer, avec pour chacun d'elle, une sélection d'au moins 2 solutions efficaces** :
Top 8 des solutions P2P certifiées Hadopi Proof

Antidote n°8 : Masquer votre réelle adresse IP

Pour masquer votre identité, pourquoi ne prendriez-vous une adresse IP du Canada, des Seychelles, de Chine, ou d'ailleurs ? Double effet garanti : Non seulement vous êtes hors de portée des erreurs de l'HADOPI mais en plus cela va les faire chier.

C'est simple et légal :

Cyber Résistance : Anonyme en 2 minutes

D'autres utiliseront le Wifi comme technique de dissimulation :

Hadopi et les 100 joies du WIFI

Le Must est de passer ses communications via un serveur VPN à l'étranger :

Vpn . Egalité . Fraternité

5 minutes de paramétrage de son PC suffisent. Une fois réalisée cette opération, il vous suffit de 2 clics de souris pour activer ce type de connexion et rendre ainsi totalement inopérant tout système de surveillance ou de filtrage d'internet.

Antidote n°9 : Neutralisation du logiciel espion

Vous ne souhaitez pas que l'Etat espionne vos communications ?

Néanmoins, mettre sur son PC le logiciel espion d'HADOPI sera quasi obligatoire si vous souhaitez vous disculper en cas d'accusation erronée de HADOPI.

Voici la solution :

VirtualBox (Wikipedia) permet de faire tourner un 2ème système d'exploitation sur son PC. Autrement dit, il créé un second PC virtuel sur votre PC.

Installez **VirtualBox** (Windows, Mac, Linux) et enfermez y le mouchard d'HADOPI. Celui-ci sera donc bien installé sur votre PC mais il n'enregistrera rien.

Concernant ce fameux logiciel espion obligatoire, la confusion est encore totale

: En effet, notre Ministre, Mme Albanel (**1ère vidéo**) ne connait pas encore vraiment la différence entre logiciels parefeu, espion, antivirus, suite bureautique ... etc.

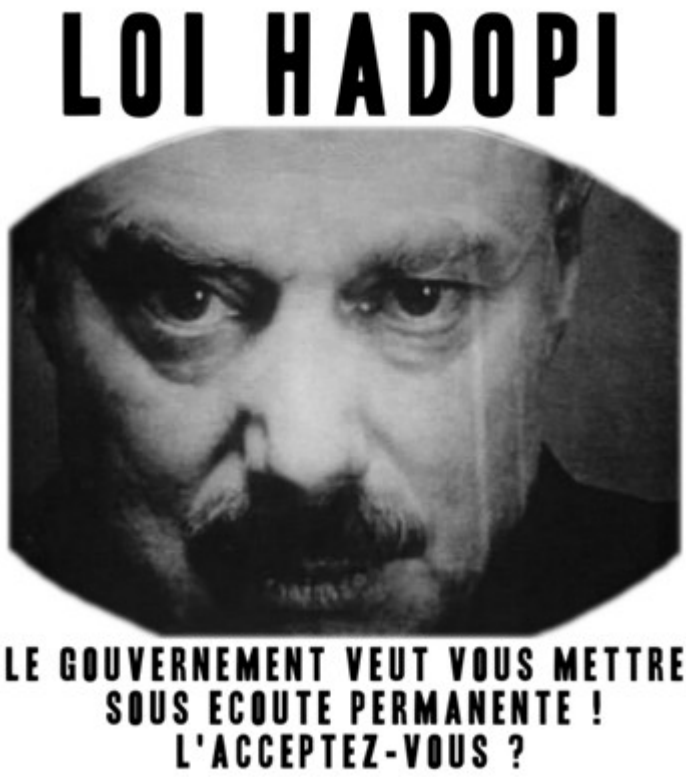
N'hésitez pas à les contacter pour savoir où ils en sont :
Ministère de la culture et de la communication
3 rue de Valois - 75033 Paris Cedex 01
Téléphone : + 33 1 40 15 80 00 (7/7 24/24)

Encore plus affligeant :
2ème vidéo : Son remplaçant, Frédéric Mitterrand, lui, ne sait même pas ce que signifie HADOPI.

3ème vidéo : Les députés qui votent cette loi, eux, ne savent même pas ce qu'est le Peer to Peer et le Streaming.

4ème vidéo : Le petit soldat pourfendeur d'Internet, Frédéric Lefebvre, lui, ne sait pas ce que veut dire Web 2.0 qu'il dénigre en permanence.

Antidote n°10 : Propager massivement ces antidotes



affiche.fr

Une pub visionnaire et détournée datant de 1998 de Club Internet :

"*Hadopi restera dans les mémoires, comme cette loi présomptueuse qui aura voulu atteindre l'horizon, rattraper un progrès qui ira toujours plus vite qu'elle*".
Un député lucide.

http://www.commentcamarche.net/news/5851561-la-loi-hadopi-n-aurait-pas-d-effet-sur-le-telechargement-illegal-selon-une-etude

La loi Hadopi n'aurait pas d'effet sur le téléchargement illégal, selon une étude

CommentCaMarche le mardi 9 mars 2010 à 14:02:49
(Paris - Relax news) - La récente loi Hadopi contre le téléchargement illégal n'aurait pas d'effet sur cette pratique, selon une étude réalisée par l'université de Rennes 1. A l'inverse, le piratage aurait augmenté depuis la promulgation du texte. En cause, les nouvelles pratiques de piratage qui échappent à la loi, comme le streaming, qui permet de consulter du contenu audio ou vidéo sans avoir à le télécharger sur son ordinateur.

Conduite auprès de 2.000 personnes dans la région Bretagne entre novembre et décembre 2009 (soit environ trois mois après la promulgation de la loi), cette étude révèle que le nombre de pirates sur Internet en France a augmenté de 3% sur cette période, alors que la plupart des internautes interrogés avaient connaissance de l'existence de cette loi et de ces principales dispositions.

Les réseaux peer-to-peer, cible principale de la loi Hadopi, ont vu leur fréquentation baisser : 15% des utilisateurs de ces réseaux ont définitivement cessé de le faire avec l'adoption de la loi. En revanche, seulement un tiers de ces ex-pirates ont renoncé à toute forme de piratage sur Internet. Les deux tiers restants se sont tournés vers des systèmes de téléchargement alternatifs qui échappent au périmètre de cette loi, comme le streaming illégal ou le téléchargement sur des sites d'hébergements de fichiers (Rapidshare, Megaupload, etc.).

"La réduction du nombre d'internautes qui utilisent les réseaux peer-to-peer s'est donc accompagnée d'une hausse des autres formes de piratage non prises en compte par la loi Hadopi (+27%). Cet accroissement fait plus que compenser la diminution du nombre d'utilisateurs des réseaux Peer-to-Peer" explique le rapport de l'étude.

L'enquête révèle par ailleurs que les "pirates numériques" ne sont pas forcément de mauvais acheteurs de contenus légaux en ligne. La moitié d'entre eux (dont 27% sont des utilisateurs des réseaux peer-to-peer) sont en effet des "acheteurs numériques" de musique ou de vidéo sur les plateformes légales.

En conclusion, les chercheurs de Rennes 1 estiment que la loi Hadopi, en coupant la connexion Internet des pirates peer-to-peer, pourrait réduire la taille du marché légal des contenus culturels numériques.

Adoptée en septembre dernier par les parlementaires, la loi Hadopi a instauré une autorité indépendante (l'Hadopi) chargée d'envoyer des messages d'avertissement aux internautes identifiés comme ayant téléchargé de manière illégale des contenus en ligne. La démarche retenue est celle de la "riposte graduée" ; avertissement par e-mail, puis lettre recommandée en cas de récidive, et, en cas de troisième infraction, suspension de l'abonnement Internet pour une durée maximale d'un an. Le contrevenant risque également une amende (de 1.500 à 300.000 euros), voire une peine pouvant aller jusqu'à trois ans de prison.

Les premiers messages d'alertes ne seront toutefois pas envoyés aux pirates avant le printemps 2010, au plus tôt.

http://www.journaldunet.com/ebusiness/expert/42410/quelles-obligations-pour-les-fournisseurs-de-services-wi-fi.shtml

Quelles obligations pour les fournisseurs de services Wi-Fi ?
Un fournisseur d'accès Wi-Fi (bar, hôtel, cybercafé, hotspot municipal...) doit il connaître l'identité des utilisateurs en plus que de conserver les données de trafic ?
(08/10/2009)

Selon la CNIL, un cybercafé n'est pas tenu d'identifier l'utilisateur d'un de ses ordinateurs, et ne devait conserver que les données de trafic (date et heures de connexion, sites visités, destinataires des communications, etc…). Pourtant, rien n'est moins certain.

Le wifi est un service à valeur ajoutée qui séduit un grand nombre de professionnels, qui sont tentés de le mettre à disposition de leurs clients. On trouve des hots spots de plus en plus souvent, dans des bars, des restaurants, évidemment dans les cybercafés, mais également dans les aéroports, certaines administrations, les parcs d'expositions et autres grandes surfaces, et le maillage ne fait que croître.

1. Rappel 1 : la notion de wifi

Le nom wifi correspond initialement au nom donné à la certification délivrée par la WECA (Wireless Ethernet Compatibility Alliance), organisme chargé de veiller à l'interopérabilité entre les matériels répondant aux standards techniques internationaux de réseau local sans fil (« WLAN », norme IEEE 802.11).

Grâce au wifi, il est possible de créer des réseaux locaux sans fil à haut débit, et ainsi de relier des ordinateurs portables, des postes de bureau, des assistants personnels (PDA) ou des périphériques, à une liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur, et de plusieurs centaines de mètres en milieu ouvert. Dans les lieux publics, le réseau wifi se traduit le plus souvent par l'installation de bornes wifi (« *hot spots* »).

Naturellement, ce sont les fournisseurs d'accès internet (FAI) par réseau filaire qui mirent en place les premiers réseaux wifi dans des zones à forte concentration (gares, aéroports, hôtels, trains, etc.), et qui ont proposé cet accès internet sans fil aux particuliers. Ces FAI permettent en outre à de nombreux professionnels (cybercafés, mais également bars, grands magasins, gestionnaires de salons, administrations...) de proposer une connexion wifi à leurs propres clientèles.

Le professionnel est donc ici dans la situation d'un client privé qui recourt aux services d'un FAI (les plus connus étant bien entendu Orange, Free, Numéricable, SFR, etc.) afin d'équiper ses locaux d'un réseau wifi et d'en proposer l'utilisation à ses salariés ou à sa propre clientèle au sein de ses locaux.

La question se pose alors de savoir si ce professionnel, qui propose une connexion wifi à ses clients, ne devient pas lui-même FAI, et s'il n'est pas ainsi soumis aux obligations qui incombent aux FAI en tant qu'opérateurs de communications électroniques.

Rappelons d'abord quelles sont ces obligations, qui sont nombreuses.

2. Rappel 2 : les obligations du fournisseur d'accès

Les sources légales de la réglementation applicable au wifi, le plus souvent élaborées pour internet

quel que soit le mode de connexion, sont plurales.

2.1 L'obligation déclarative

L'article L.33-1 du Code des postes et des communications électroniques (CPCE) dispose que l'établissement et l'exploitation des « *réseaux ouverts au public* » et la fourniture au public de « *services de communications électroniques* » sont des activités libres, sous réserve d'une déclaration préalable auprès de l'Autorité de régulation des communications électroniques et des postes (ARCEP).

Toutefois, une telle déclaration n'est pas exigée pour l'établissement et l'exploitation de « *réseaux internes ouverts au public* » ni pour la fourniture au public de « *services de communications électroniques* » sur ces réseaux. Par conséquent, l'installation d'un réseau de communications électroniques dans un *espace privé, qui bien qu'ouvert au public n'empiète pas sur le domaine public*, ne nécessite pas de déclaration préalable auprès de l'ARCEP.

Le CPCE explique en effet la différence entre *réseau ouvert au public* et *réseau interne ouvert au public* par le fait que l'espace sur lequel est déployé le wifi est totalement privatif, dans le second cas.

Mais outre cette obligation déclarative, d'autres obligations s'imposent encore aux opérateurs de communications électroniques (OCE), dont relèvent les FAI.

2.2 L'obligation de conservation des données

Premièrement, la loi LCEN du 21 juin 2004 impose aux personnes qui fournissent un accès à internet de garder confidentielles les données personnelles de leurs clients (article 6 III 2 de la loi). Mais en même temps, cette loi leur impose aussi la conservation des données « *de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elle est prestataire* » (article 6 II). Certains y ont vu un paradoxe, mais il n'est qu'apparent. Le FAI doit seulement pouvoir déconfidentialiser les données si l'autorité judiciaire lui en fait la demande. Il reste tenu au secret professionnel.

L'article L.34-1 du CPCE reprend cette exigence. Conformément à la LCEN, le code rappelle donc que l'OCE doit conserver les données permettant l'identification des personnes utilisatrices des services fournis par les opérateurs.

En outre, l'article R.10-13 du CPCE issu du décret du 24 mars 2006 décrit les catégories de données à conserver. Il s'agit des données permettant l'identification de la personne qui s'est connectée, les données de connexion dont la date et l'heure, les données relatives aux équipements utilisés et même les données permettant d'identifier les destinataires de toute communication effectuée. Le décret du 24 mars 2006 fixe la durée de conservation des données à **un an**, durée au-delà de laquelle elles devront être anonymisées.

La loi « *Informatique & Libertés* » du 6 janvier 1978 intervient également, puisque le FAI doit absolument respecter les obligations d'information des personnes quant à leurs droits d'accès, de rectification, d'opposition et de suppression.

En outre, conformément à la décision de ARCEP du 26 avril 2007 (mettant fin à la phase initiale d'expérimentation des réseaux WLAN), les opérateurs wifi sont dorénavant soumis au respect de l'ensemble des dispositions du CPCE.

2.3 L'obligation de sécurisation de la connexion

Censée lutter contre le téléchargement légal, la médiatique loi « *Création & Internet* » du 12 juin 2009, dite « *Hadopi* », a également imposé aux titulaires d'une connexion sans fil de « *sécuriser* » celle-ci afin d'empêcher que des activités illicites soient pratiquées depuis l'ordinateur d'un abonné à son insu.

La loi a modifié la LCEN en imposant aux FAI d'informer les utilisateurs de l'existence des moyens de sécurisation permettant de prévenir les manquements aux articles L.336-1 et suivants du Code de la propriété intellectuelle sanctionnant le téléchargement illicite. Le législateur a ici pris modèle sur l'obligation incombant aux FAI d'avertir leurs clients des outils de filtrage qu'ils leur mettent à disposition.

La loi « *Hadopi* » vise également quiconque utilise une connexion wifi, ce qui vise les internautes, mais également les restaurants, les hôtels, les bibliothèques, les jardins publics, les universités, etc. Un nouvel article L.336-3 du CPI dispose en effet que « *la personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise* ».

Cette obligation pèse donc sur tout professionnel qui dispose d'une connexion wifi, qu'elle serve ses activités professionnelles ou qu'elle soit mise à disposition de ses clients. Rien n'est dit toutefois sur les caractéristiques techniques ni le fonctionnement du dispositif de « *sécurisation* »...

2.4 Sur qui pèsent ces obligations ?

Par conséquent, le FAI qui propose un réseau wifi doit donc de se conformer à l'ensemble des obligations visées ci-dessus. Tout manquement à l'obligation de conservation des données expose la personne à laquelle incombe cette obligation aux sanctions visées aux articles 6-VI de la loi du 21 juin 2004 et à l'article L. 39-3 du CPCE, soit un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques, et 375.000 euros pour les personnes morales.

Or, au regard du volume de données à conserver, comme au regard de la durée minimale de conservation, celle-ci implique une infrastructure matérielle et des espaces-mémoire très conséquents.

Il convient par conséquent d'examiner la notion de « *FAI* », qui est liée à celle « *d'OCE* » au sens de la LCEN. De la qualification d'opérateur de communications électroniques dépend en fait l'application de la réglementation analysée ci-dessus à un nombre plus ou moins grand de professionnels.

En clair : qu'est-ce qu'un FAI au sens légal du terme ? Quiconque propose une connexion internet devient-il pour autant OCE ? Une réponse de bon sens voudrait qu'un hôtel ou un restaurant ne soient pas assimilés à SFR ou Iliad. Mais les textes ne sont pas aussi clairs.

3. La notion de « fourniture d'accès », une notion en continuelle extension

3.1 Du FAI, prestataire technique...

L'article 6-I 1° de la LCEN précisait ce que vise la notion de FAI : il s'agit des « *personnes dont*

l'activité est d'offrir un accès à des services de communication au public en ligne (...) ». Cette notion laissait peu de place à l'interprétation, puisqu'ici sont mises en exergue les notions d'activité économique et d'abonnement, qui permettaient ainsi de caractériser la présence d'un FAI. Le FAI est le « *prestataire technique* », dont l'activité consiste à fournir un accès à internet.

Jusqu'ici, le concept est clair. A s'en tenir à la LCEN, un restaurant ne pourra jamais être soumis aux obligations des FAI, même s'il propose une connexion wifi en terrasse.

3.2 ... au FAI, exploitant de réseau / service proposé au public

Seulement, l'article L.32 du CPCE, issu d'une loi du 9 juillet 2004, dispose qu'on « *entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* ».

Cette définition des OCE est extrêmement large : elle vise les personnes qui « *exploitent* » un réseau de communications électroniques, et celles qui « *fournissent* » au public un service de communications électroniques.

Cette deuxième définition semble pouvoir s'appliquer à toute entité mettant à disposition d'un public une connexion internet, que celle-ci soit filaire ou sans fil, sans distinction selon qu'il s'agit de son activité propre ou d'une mise à disposition matérielle dans le cadre d'une activité distincte !

Une lecture extensive de l'article L.32 CPCE permet d'assimiler à la notion de « *services de communications électroniques* » une multitude de services qui ont toujours échappé à la législation sur les télécommunications, parce qu'ils sont fournis par des entreprises qui interviennent à un stade intermédiaire du processus de communication, ou qui évoluent dans des secteurs économiques radicalement différents des télécommunications, et ne font que mettre à disposition de leurs clients un service de communication électronique en recourant à un opérateur dont c'est précisément l'activité.

3.3 Une lecture aussi extensive doit-elle être retenue ?

L'exposé des motifs de la loi du 9 juillet 2004 comportant l'article 32 du CPCE indique que l'objet principal de la réforme était de tenir compte du phénomène de *convergence technologique*, rendant obsolète la traditionnelle distinction entre réseaux de voix (téléphonie), de données (réseaux informatiques), et la diffusion audiovisuelle.

Ainsi, la réforme visait essentiellement à règlementer des activités nouvelles échappant à l'industrie classique des télécommunications, tels les fournisseurs d'accès internet, la téléphonie sur IP, la télévision sur ADSL, etc. Partant, elle pouvait être très extensive, puisqu'elle avait précisément pour propos de s'affranchir des catégories professionnelles dépassées.

Pour autant, l'article L.32 du Code peut-il, doit-il s'appliquer à toutes les entreprises qui proposent une connexion internet ? A ce compte, quelle entreprise aujourd'hui ne propose pas de connexion internet, que ce soit à ses préposés ou à ses clients ?

Sentant le risque d'extrapolation, l'ARCEP a précisé dans sa lettre périodique n°41 que la notion de « *services de communications électroniques* » de l'article L.32 visait principalement les exploitants de réseaux et les fournisseurs de services liés aux réseaux (tels que les FAI), en précisant que cette définition ne comprenait pas « *les acteurs n'intervenant pas dans l'émission, la transmission ou la réception des signes, des sons, des signaux ou images constitutifs de la communication*

électronique ».

Ainsi selon l'ARCEP, n'entrent pas dans la notion d'opérateur de services de communications électroniques « *les éditeurs de services de radio et de télévision et les distributeurs qui agrègent ces contenus sous la forme d'une offre de services accessible par voie hertzienne, par câble ou par satellite* ».

Rien n'est dit cependant sur les entreprises qui, sans intervenir dans le transit des signaux, proposent un accès internet sans fil à leurs clients, voire aux visiteurs de leurs locaux si ceux-ci sont publics...

Pour compliquer encore la situation, la législation anti-terroriste votée le 23 janvier 2006, consacrée notamment à la « *lutte contre l'utilisation à des fins terroristes de moyens anonymes de connexion à internet dans les lieux publics* », a ajouté d'autres critères d'appréciation.

4. La fourniture d'accès comme « activité accessoire » ou « principale », critère inoperant

4.1 La loi du 23 janvier 2006

Avant cette loi du 23 janvier 2006, on pouvait considérer, au regard des textes susmentionnés, qu'une entreprise qui propose un accès wifi, dans le cadre de son offre de services, mais « *sans intervenir sur les contenus accessibles* », ne devait pas être considérée comme un OCE, c'est-à-dire ni hébergeur évidemment, ni même FAI.

Mais la loi du 23 janvier 2006 a alourdi les obligations qui pèsent sur le FAI, tout en étendant encore la définition de ce qu'est un FAI !

Modifié par cette loi anti-terroriste, l'article L. 34-1 CPCE dispose que les personnes qui, « *au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article*.»

Cet article vise très clairement toutes les personnes qui offrent au public une connexion au réseau internet, « *à titre principal ou accessoire* ». Par rapport à la LCEN, qui visait les entreprises « *dont l'activité est d'offrir un accès à des services de communication au public en ligne* », l'article L.34-1 du CPCE introduit donc une interprétation très extensive, puisqu'il vise également les personnes qui proposent une connexion « *à titre accessoire* ». Au pied de la lettre, cette loi de 2006 assimile à un OCE *toute entreprise disposant d'une connexion et la mettant à disposition du public***.**

Ainsi, si on estime que le personnel d'une entreprise constitue un *public*, l'ensemble des entreprises disposant d'une connexion pourrait ainsi être soumis aux obligations d'effacement et/ou de conservation des données visées à l'article L. 34-1 du CPCE. De même, le bar du coin de la rue qui propose un hot spot serait donc, au sens de cet article, une « *personne permettant au public une communication en ligne* », et partant, serait soumise aux obligations visées plus haut.

4.2 Les travaux préparatoires de la loi du 23 janvier 2006

Certes, l'examen des motifs de la loi indique que le législateur visait essentiellement les cybercafés et les hots spots des *lieux publics*.

Ainsi, le rapport de l'Assemblée Nationale mentionne expressément :

- les « *personnes qui offrent à leurs clients, dans un cadre public, ou à des visiteurs une connexion en ligne, tels les hôtels, les compagnies aériennes...* » ;

- et les « *fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne WIFI* » que ce soit à titre payant ou non.

Les débats parlementaires montrent donc que l'article L.34-1 I vise les professionnels non pas en fonction d'un statut propre ou d'une profession particulière (« *OCE* », « *prestataire technique* »), mais uniquement en raison de leur *activité de fourniture d'une connexion, même si elle n'est pas dans leur objet social.*

Ainsi, les mairies, les aéroports, les bibliothèques ou encore les universités peuvent être concernés si leurs activités les conduisent *à titre accessoire* à fournir une prestation identique à celle d'un cybercafé. Si les travaux parlementaires visent expressément ces derniers, la loi, elle, n'a pas distingué.

A analyser les travaux préparatoires, le doute demeure entier : la notion de « *lieux publics ou commerciaux* » équipés en hot spots pourrait donc concerner un très grand nombre de professionnels.

D'ailleurs comme il en a pris l'habitude, le législateur renvoie à la charge du juge la mission de *déterminer si le lieu ou l'activité de la personne proposant le service de connexion, la rattachent à la catégorie d'opérateur de communications électroniques.*

4.3 Les interprétations subséquentes

La position de la CNIL

La CNIL, dans une délibération n°2005-208 du 10 octobre 2005 relative à la loi de 2006, a indiqué, tout en regrettant l'ambiguïté de la définition retenue, que *les entreprises et leurs salariés* devaient être exclus du champ d'application de cette loi.

C'est dire que le personnel d'une entreprise ne doit pas être perçu comme un « *public* ». Premier éclaircissement.

Mais quid des clients d'un bar ? Quid du public fréquentant un centre commercial ? Quid des visiteurs d'un musée ? Quid des visiteurs d'un site gratuit ? Quid des preneurs de bail ? Quid des simples visiteurs d'un salon professionnel ou d'un évènement culturel ? La CNIL ne s'est prononcée que sur la question précise des salariés, et il serait hasardeux d'extrapoler, à partir de sa délibération, une analogie pour les catégories d'utilisateurs qui ne seraient pas liées à l'entreprise par un lien de subordination juridique.

La position de la jurisprudence

La Cour d'appel de Paris, dans un arrêt du 4 février 2005, a estimé quant à elle qu'une banque était assimilable à un OCE. Dans l'affaire déférée, une société de presse s'était adressée à la banque après avoir découvert que des messages électroniques dommageables avaient été émis depuis le routeur de celle-ci.

La Cour d'appel a énoncé que la banque était tenue, en application de l'article 43-9 de la loi du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication,

de détenir et de conserver les données de nature à *permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire*. La Cour d'appel a également affirmé que la banque était tenue de communiquer ces données sur réquisition judiciaire.

Autant dire que la Cour d'appel a totalement assimilé la banque à un OCE. Mais il faut souligner que dans cette espèce, la banque n'avait pas contesté son rôle de « prestataire technique » par la banque. Il est donc difficile d'en inférer quoi que ce soit sur le sort qui serait réservé à d'autres professionnels.

Mais cette jurisprudence montre en toute hypothèse que la tendance est à l'interprétation extensive de dispositions légales dont la CNIL a pourtant souligné l'ambigüité. Il faudra d'autres espèces pour qu'on sache si la jurisprudence française compte étendre la notion de FAI aux entreprises qui mettent à disposition de leurs clients un accès internet...

La (les) position(s) de l'ARCEP

L'ARCEP, en revanche, interrogée dans le cadre des contentieux qui lui sont soumis, a déjà eu l'occasion d'affirmer qu'une entreprise « *qui ne dispose pas d'infrastructures de communications électroniques et qui est reliée au réseau internet à l'aide de liaisons louées auprès d'opérateurs de communications électroniques et dont les activités se limitent à assurer la configuration, l'administration, la surveillance et la maintenance des serveurs informatiques* **ne peut être considérée comme un opérateur de communications électroniques et être soumise aux dispositions de l'article L. 34-1 du CPCE »**.

L'ARCEP va directement à l'encontre de la décision de la Cour d'appel de Paris, et précise les critères qui, selon elle, doivent départager un véritable OCE d'une entreprise qui propose du wifi à ses clients. L'ARCEP rappelle que si l'entreprise se borne à configurer, surveiller voire maintenir les serveurs, et qu'elle loue des liaisons auprès d'un OCE, elle n'est pas elle-même un OCE.

Dans les faits, à l'évidence, un restaurateur ou un organisateur de salons professionnels qui propose une connexion wifi, prend rarement en charge la configuration ou la maintenance de l'installation. Et surtout, il achète effectivement le service proposé par un « *OCE* » dans le cadre d'un contrat, et s'en remet à cet opérateur pour la définition, le niveau et la maintenance du service.

Mais malgré cette évidence, l'ARCEP a souligné que la loi de 2006 visait essentiellement les cybercafés, ainsi que « *les personnes qui offrent à leurs clients, dans un cadre public, ou à des visiteurs une connexion en ligne, tels que hôtels, compagnies aériennes* », ainsi encore que les « *fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne wifi, généralement par l'utilisation de cartes prépayées permettant d'accéder au réseau, mais parfois également à titre gratuit* ».

En reprenant et en complétant les travaux préparatoires de la loi de 2006, l'ARCEP introduit une nouvelle complexité dans les critères de distinction. On retrouve le risque d'assimilation aux OCE de tout professionnel proposant une connexion wifi à ses clients.

C'est donc la notion de « *public* » qui est à analyser, afin de savoir si n'importe quel professionnel peut être considéré comme un OCE.

5. La notion de « public », le chainon manquant ?

En effet, l'ensemble des textes susvisés vise systématiquement la « *mise à disposition du public* »

d'un accès sans fil. Quiconque offre une connexion à un public risque d'être considéré, à l'instar d'un cybercafé, comme un fournisseur d'accès « *indirect* ».

Afin d'échapper au régime légal des FAI, il est finalement nécessaire pour ce professionnel de combattre la notion de « *mise à disposition du public* ».

Et comme il revient finalement au juge de décider si l'entreprise est un FAI ou pas, c'est devant le juge qu'il faudra argumenter pour éloigner le risque d'assimilation.

Il est possible pour cela d'en revenir aux définitions de l'article L.32 du CPCE, qui distingue « *réseau ouvert au public* » (*tout réseau de communications électroniques établi ou utilisé pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique*) et « *réseau interne* » (*réseau de communications électroniques entièrement établi sur une même propriété, sans emprunter ni le domaine public - y compris hertzien - ni une propriété tierce*).

A partir de cette distinction, il semble possible de définir une casuistique en fonction des situations :

- Dans le cas de clients bénéficiant de la connexion wifi *dans un cadre privatif* (ex : les locataires d'un complexe immobilier), il peut être soutenu que les occupants des locaux ne constituent en aucun cas un *public*, mais plutôt des occupants *à titre privatif* dans le cadre de contrats de bail, et qu'à ce titre il s'agit d'un réseau interne. Le bailleur n'est donc pas un OCE, même s'il fournit internet *à titre accessoire*. D'ailleurs, il ne viendrait à l'idée de personne de considérer que ce bailleur est un distributeur d'eau courante ou d'électricité ;

- La question est beaucoup plus difficile pour les visiteurs d'un salon professionnel, les clients d'un restaurant, les clients d'une compagnie aérienne, ou les usagers d'une administration. Leurs locaux, bien que propriétés privées, reçoivent un « *public* », et peuvent entrer dans les hypothèses visées aux travaux préparatoires de la loi de 2006, en particulier des « *lieux publics ou commerciaux, via des bornes d'accès sans fil (WIFI)* ». Ces zones font courir le risque à leur exploitant d'être qualifié de « *fournisseur d'accès* » ;

- On peut considérer que les clients d'un restaurant ou d'un bar ne sont pas simplement un « *public* », mais des cocontractants qui viennent acheter des biens ou des services, dans le cadre d'une relation de droit privé ;

- De même, on peut considérer que les administrés qui visitent une administration ou un établissement public et profitent d'un hot spot ne constituent pas un « *public* », mais les usagers d'un service public.

Cependant, aucun texte légal ou réglementaire ne vient pour l'heure conforter cette distinction entre « *public* » et « *clientèle* ». D'autant qu'un OCE fournit lui-même son service à des clients, dans le cadre d'une relation de droit privé également. La distinction est donc fragile.

Il existe donc aujourd'hui une zone très large d'incertitude, entre la mise à disposition d'une connexion wifi dans le cadre d'un *réseau interne*, sur une propriété *privée*, et à titre *privatif*, (exemple du bailleur) d'une part, et la mise à disposition d'un service de connexion wifi par un opérateur dont c'est *l'activité principale* (exemple de Free) d'autre part.

Entre les deux se situent l'ensemble des professionnels qui proposent un accès wifi à leur clientèle, aux visiteurs de leurs locaux, sans pour autant qu'il s'agisse de leur activité principale, ou que leur clientèle soit assimilable ipso facto à un « *public* ».

Une clarification légale, plus encore que jurisprudentielle, est donc nécessaire, afin d'éviter que les restaurants, les administrations ou les hôtels rejoignent SFR, Orange, Iliad ou Numéricâble au sein de l'Association Française des fournisseurs d'Accès...
Thomas Beaugrand

http://www.quickspot.biz/products-legislation.html
La législation sur la fourniture d’un accès WiFi - Responsabilités

La fourniture d’un accès Internet sans fil dans un lieu public, nécessite que vous soyez possession des droits d’exploitations des fréquences sans-fil utilisées : 2,4Ghz pour le WiFi. Cette autorisation d’exploitation des ondes WiFi est délivrée sous forme de licence par l’ARCEP (Autorité des Régulations des Communications Electroniques et des Postes).

Responsabilité - explications :

En souscrivant à une offre de service d’accès Internet auprès d’un FAI (Fournisseur d'Accès Internet) vous devez savoir que ce dernier enregistre tout le trafic effectué depuis votre connexions, et ce pour des raisons légales liées à la sécurité.

En fournissant un accès Wi-Fi à partir de votre connexion Internet vous endossez de fait les mêmes responsabilités - auprès de votre clientèle ou visiteurs - que votre Fournisseur d’Accès Internet car vous devenez vous même Fournisseur d’Accès Internet Sans-Fil. En effet votre FAI se contente d’enregistrer le trafic effectué sur l’accès qu’il fournit (jusqu’à la prise téléphonique). Cela signifie que le trafic effectué sur l’accès Internet Sans-Fil que vous fournissez n’est pas identifié par ce dernier.

Dans cette mesure, en cas de malversation sur votre Hotspot, votre Fournisseur d’Accès Internet, ne pouvant identifier les différents utilisateurs qui font usage de votre connexion Internet, portera directement la responsabilité sur son client, vous!

Quelques risques concrets d’usage de votre connexion internet en accès WiFi :

* Utilisation de votre accès pour des téléchargements illégaux.
* Activité pédophile (Connexion à des site d’échanges de fichiers, usurpation d’identité sur des forums ou des messageries instantanées...).
* Diffusion de propos diffamatoires, xénophobe, antisémite sur internet.
* Usage de votre accès internet pour des actions de Spam, de piratage, de diffusion de virus.

La législation :

* http://www.service-public.fr/accueil/loi_lutte_terrorisme.html
* http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/2006-64/terrorisme.htm
* http://www.arcep.fr/index.php?id=9269#12921
* http://www.cnil.fr/index.php?id=1953

Les sujets d’actualité :

* http://www.pcinpact.com/d-108-1-mission_olivennes_engagement_interprofessionnel.htm
* http://www.pcinpact.com/s/LOPSI.htm
* http://www.pcinpact.com/actu/news/41827-LOPSI-cybercriminalite-loi.htm

Les instances :

* ARCEP
* CNIL

Quelques liens :

* http://www.interieur.gouv.fr/sections/a_l_interieur/le_ministre/interventions/lutte-cybercriminalite
* http://www.01net.com/editorial/371670/le-gouvernement-va-devoiler-son-arsenal-contre-la-cybercriminalite/
* http://www.foruminternet.org
* [Article de Me Olivier Sanviti Avocat au barreau de Paris spécialiste NTIC sur la mise en place d'un Hotspot. en CHR.] Victime?
http://www.clusif.asso.fr/fr/production/cybervictime/

Nos produits QuickSpot Partagé - Liberté face à ces obligations :

SpotCoffee SAS, détenteur d'une licence opérateur déclaré auprès de l'ARCEP , a développé les produits QuickSpots afin d'une part de pouvoir répondre techniquement à ces obligations légales vous permettant de vous déresponsabiliser de l'usage fait par vos utilisateurs sur votre Hotspot et d'autre part de pouvoir proposer aux établissements souhaitant fournir un accès WiFi à leurs clients ou visiteurs, des produits Hotspots conformes en nous engageant à prendre les Hotspots (QuickSpot Partagé et Liberté) sous notre licence d'opérateur.

La législation étant amenée à évoluer vers une obligation d'identification plus poussée les echos SpotCoffee a d'ores et déjà développé les moyens techniques permettant de vérifier l'identité de l'utilisateur.
SpotCoffee, en tant qu'opérateur WiFi, s'engage à se tenir informé quotidiennement de l'évolution de ces obligations légales afin de les appliquer sur ses produits QuickSpot Partagé et Liberté dès que les projets gouvernementaux relatifs aux opérateurs de télécommunication entrent en vigueur.

Le produit QuickSpot (QuickSpot Solo) vous laisse néanmoins la possibilité de devenir votre propre opérateur en mettant en place les moyens vous permettant d'être en conformité avec la loi.

SpotCoffee ne pourra en aucun cas être responsable du non respect des obligations juridiques et techniques à respecter pour la fourniture d'un accès Internet sans-fil (WiFi) dans des lieux publics. SpotCoffee n'a aucune obligation de prévention sur les nouveaux décrets d'applications relatifs aux opérateurs auprès des Sociétés ayant fait l'acquisition du QuickSpot Solo.

Rappel des obligations légales liées aux opérateurs WiFi :
* Pour la fourniture d'un accès Internet WiFi ouvert public, vous devez être détenteur d'une licence opérateur délivrée par l'ARCEP (Autorité des Régulations des Communications et des Postes) permettant d'exploiter les fréquences WiFi 2,4 Ghz.
* Vous devez mettre en place les moyens permettant d'identifier techniquement et authentifier tous les utilisateurs qui fréquentent et se connectent sur vos Hotspots.
* Vous devez enregistrer tout le trafic effectué sur Internet par tous les utilisateurs se connectant depuis vos Hotspots et conserver ces données pendant une période d'un an (nécessite le déploiement et la configuration d'un serveur de logs chez un hebergeur). Vous devez être capable de fournir ces informations sur commission rogatoire ou réquisition judiciaire.
* Vous devez déclarer votre système d'authentification et de logs de vos Hotspots à la CNIL (Commission nationale de l'informatique et des libertés).
* Vous devez déployer et configurer un serveur de mail ANTISPAMS afin d'éviter les envois de SPAMS depuis vos Hotspots.
* Vous devez veillez à pouvoir interdire le téléchargement illégal depuis vos Hotspos.
* Vous devez vous maintenir informé et appliquer toutes nouvelles obligations légales appliquées aux opérateurs.

Quelque liens sur internet

http://www.numerama.com/magazine/9854-10-bonnes-raisons-de-dire-NON-a-la-loi-Hadopi.html
http://www.numerama.com/magazine/15210-une-etude-indique-que-la-loi-hadopi-augmente-le-piratage.html
http://www.lemonde.fr/technologies/article/2009/10/23/la-loi-hadopi-2-n-est-pas-applicable_1257807_651865.html
http://www.pcinpact.com/dossiers/loi-hadopi-riposte-graduee-anefe/162-1.htm
http://www.zataz.com/news/19011/HADOPI--anonyme--anonymat--tracer--telechargement.html