



Loi Création et Internet
« Le boomerang législatif »
Article de prospective
Janvier 2009 – Avril 2010
Paul Guermonprez, 23 février 2009

Entrées

1er janvier 2009, Nouvelle année nouvelles résolutions.....	2
10 février 2009, Positions en France.....	2
16 février 2009, Positions à l'étranger et au Parlement Européen	2
22 février 2009, Simple effet d'annonce ou faudra-t-il faire des exemples ?	2
4 avril 2009, Premiers exemples : 30 internautes menacés de bannissement	3
17 avril 2009, Premiers exemples : confusion et suspicion	3
20 juin 2009, Une journée dans les entrailles de Big Brother	3
15 juillet 2009, De lourdes peines pour des délits unitaires, ou profiler des internautes	5
17 août 2009, Premières estimations : le piratage en baisse !.....	5
20 août 2009, Madame Michu hésite.....	5
1 ^{er} septembre 2009, Les pirates aguerris déjà à l'abri.....	5
10 septembre 2009, Cours d'école et machines à café : le retour aux « mix tapes »	6
3 octobre 2009, La mécanique des réseaux P2P évolue.....	6
5 octobre 2009, L'attaque des zombies pirates.....	7
10 octobre 2009, Première vague de bannissements	7
16 octobre 2009, Union de médias et fournisseurs.....	8
22 octobre 2009, Annonce du filtrage d'internet en France pour lutter contre la pédo- pornographie et le terrorisme.....	8
10 novembre 2009, Nouvel audit : le piratage en hausse !.....	9
2 décembre 2009, D'anonyme le piratage devient social	9
29 novembre 2009, Qu'est ce que la neutralité du réseau ?	9
5 décembre 2009, Grogne des élus et collectivités locales	9
12 décembre 2009, Il suffit de changer de fournisseur !.....	10
15 décembre 2009, Achats de Noël ... achèterez-vous Français ?	10
5 janvier 2010, Le diable est dans les détails.....	10
18 janvier 2010, Création et Internet phase 2 : filtrage par port du réseau	11
25 janvier 2010, La BBC et CNN demandent l'arrêt du blocage par port	11
4 février 2010, Des sites légaux d'information sur la liste noire !	12
25 février 2010, Premiers sabotages de fibres et centraux.....	12
3 mars 2010, Des pirates, des pros, des vrais !.....	12
10 mars 2010, Nouveau filtrage : inspection des paquets	13
7 avril 2010, L'inspection des paquets ne suffira pas.....	13

1er janvier 2009, Nouvelle année nouvelles résolutions

Cette année sera celle de la fin du téléchargement illégal, le Président de la République l'a décrété. La volonté n'est pas d'empêcher réellement le téléchargement mais de provoquer un changement des mentalités. Ce projet de loi vise uniquement certaines technologies de téléchargement, sa portée est donc limitée dans le temps et le spectre des technologies de piratage sur internet. Effet collatéral, pour la première fois la neutralité du réseau va être cassée, ouvrant une boîte de pandore, voyons ce qu'il en sortira.

Ceci est le journal d'un observateur politique et technique.

10 février 2009, Positions en France

A quelques semaines du vote au parlement, les positions se font discrètes dans les partis politiques. Les puissants groupes de producteurs de contenus soutiennent le projet et leurs appuis sont bien répartis dans le spectre politique. Le mot d'ordre est le soutien à l'industrie contre la contrefaçon.

Les journalistes spécialisés dans les domaines techniques, les associations de consommateurs et d'internautes sont eux fortement contre et très actifs. Leurs critiques se concentrent sur 4 points : l'inefficacité technique du projet, le manque de procédure en justice, les atteintes à la vie privée et enfin l'atteinte à la neutralité du réseau. Si telle est la volonté du Président de la République, le projet passera donc rapidement devant les députés et sera voté en l'état.

16 février 2009, Positions à l'étranger et au Parlement Européen

La France assumait en 2008 la présidence tournante de l'Europe. Le Président Sarkozy avait alors tenté de faire inclure le projet de loi d'inspiration très personnelle dans le paquet télécom alors en débat au parlement. Le paquet télécom stipule que tout usager doit se voir offrir une procédure judiciaire équitable et contradictoire s'il est accusé. Or le projet du Président Sarkozy stipule que la sanction, typiquement un bannissement d'internet pour une durée allant de quelques mois à un an, était automatique et décrétée par une autorité créée pour l'occasion et hors du système judiciaire. Le parlement avait donc fermement refusé et la présidence était transférée à la Tchéquie pour 2009.

Certains gouvernements étrangers se déclarent intéressés par le concept de riposte graduée, comme l'Autriche et l'Australie (qui a déjà décidé de mettre en place un filtrage d'internet au niveau national).

D'autres sont contre : le Ministre Anglais à la propriété intellectuelle David Lamy ne veut pas d'un « système ou l'on parle d'arrêter les adolescents dans leur chambre » ([Times](#)), mais la plus vive critique vient de la Ministre allemande Brigitte Zipries : « **Empêcher quelqu'un d'accéder à Internet me semble être une sanction complètement déraisonnable. Ce serait hautement problématique d'un point de vue à la fois constitutionnel et politique. Je suis sûre qu'une fois que les premières déconnexions se produiront en France, nous entendrons le tollé jusqu'à Berlin.** » ([Spreeblick](#)).

22 février 2009, Simple effet d'annonce ou faudra-t-il faire des exemples ?

Le débat ne se positionne pas sur la justesse ou la faisabilité technique de la loi elle-même mais ses effets indirects. En effet le but avoué de la loi est de faire changer les mentalités, pas d'agir au quotidien.

La vraie interrogation est : l'effet d'annonce suffira-t-il ou bien faudra-t-il faire des exemples pour marquer les esprits ? Dans les deux cas l'action doit être rapide, car des contre-mesures vont rapidement être mises en pratique par les internautes.

4 avril 2009, Premiers exemples : 30 internautes menacés de bannissement

Décret d'application paru en un temps record, la Haute Autorité nommée rapidement, tout était en place. Annoncées par le président lui-même les premières lettres furent envoyées discrètement. Trois cas sont arrivés jusqu'aux médias, pour deux cas des adolescents vivant chez leurs parents, pour le 3ème une jeune adulte vivant seule. Le cœur de cible, donc.

Pour un premier essai les cibles sont bien choisies, elles clament leur innocence mais leur culpabilité semble plausible, elles répondent en tout cas au portrait robot du pirate type. Nous en sommes réduits à ces aprioris puisque la culpabilité n'est pas jugée lors d'une procédure judiciaire publique mais décrétée par la Haute Autorité sur dénonciation des sociétés détentrices des droits.

17 avril 2009, Premiers exemples : confusion et suspicion

Les débats publics ne se concentrent pas sur le fait de télécharger ou pas mais sur le fait de savoir si vous avez suffisamment surveillé votre connexion internet, ce qui est l'esprit de la loi. Des parents inquiets sont interrogés et avouent leur ignorance dans les technologies réseau qui permettraient de savoir et surveiller. Les entreprises se posent la question à propos de leurs employés, et les simples internautes à propos de leurs voisins qui pourraient utiliser leur réseau Wifi à leur insu ... la confusion et la suspicion règnent.

20 juin 2009, Une journée dans les entrailles de Big Brother

Les premiers dossiers étaient gérés manuellement pour établir la procédure et bien choisir les cas, mais tout est maintenant automatisé afin de permettre à la Haute Autorité de remplir ses objectifs : plusieurs milliers d'avertissements ou bannissements par jour.

Voici une journée dans les entrailles de Big Brother :

1. Les sociétés de protection des droits décident d'une liste d'œuvres à chercher. Elles peuvent par exemple choisir de ne pas dénoncer des internautes pour un artiste pendant sa campagne de promotion pour ne pas voir des condamnations entacher sa réputation à ce moment crucial, ou au contraire de cibler des œuvres très piratées pour casser la dynamique. Ensuite il suffit de faire comme un pirate, chercher le fichier sur un moteur de recherche spécialisé et le donner à un logiciel de téléchargement légèrement modifié pour collecter des informations. Il suffit juste de télécharger le fichier une fois pour s'assurer qu'il s'agit bien du fichier supposé. L'intervention humaine s'arrête là, en tout 20 minutes par œuvre.
2. Le logiciel modifié regarde en permanence sur des serveurs de partage "trackers" qui téléchargent et partagent quoi. En effet dans les réseaux P2P (de pair à pair) visés par la loi création et internet, une machine émet en même temps qu'elle reçoit. Le « qui » est un numéro unique et anonyme comme un téléphone, une "IP". Au mieux l'IP peut être associée à un central téléphonique. Au passage l'automate regarde quels fichiers sont disponibles en partage sur cet ordinateur pour faire une dénon-

ciation motivée par plusieurs infractions si possible. Les serveurs qui font ce travail ont accès à de multiples connections internet chez différents fournisseurs pour être le plus discret possible, le but est de ne pas se faire repérer sur le réseau d'échange P2P. Ils risqueraient d'en être bannis, un comble.

3. Les serveurs des sociétés de protection des droits peuvent alors transmettre l'IP de l'internaute avec le nom d'un ou plusieurs fichiers correspondant à des œuvres protégées à la Haute Autorité.
4. En pratique pour un particulier l'adresse IP peut être reliée au boîtier d'accès livré par son fournisseur d'accès à internet, et ce grâce à son fichier client et logistique. Encore faut-il qu'il soit à jour, que le bon boîtier soit livré à la bonne personne, que les déménagements et résiliations soient bien notés en regard des détails techniques ... autant de détails qui avaient peu d'importance opérationnelle (et donc mal renseignés) pour les fournisseurs jusque là et qui sont maintenant de leur responsabilité. Les informations doivent être gardées pendant au moins un an, ce qui était déjà le cas avant, mais elles étaient alors utilisées à très petite échelle sur réquisition de justice. Par contre pour les réseaux en libre accès (jardins publics de Paris ou le café du coin), ce n'est pas l'internaute qui est identifié et responsable mais le fournisseur (Mairie de Paris ou le cafetier).
5. Le serveur de la Haute Autorité accède donc au serveur qui gère le fichier client et logistique de chaque fournisseur sans passer par la justice, récupère le nom et les coordonnées correspondants à une IP puis prépare un email ou une lettre papier personnalisée.
6. Selon le cas les emails sont envoyés automatiquement ou un imprimeur reçoit la fournée de courriers à imprimer et poster (mais la version papier est facultative), elles seront reçues le lendemain partout en France.
7. De son côté le fournisseur reçoit la liste des personnes à contacter par email pour le premier ou second avertissement (s'il y a un second, il est facultatif). En effet c'est le fournisseur qui a la responsabilité de contacter et menacer son client sur injonction de la Haute Autorité. Il faut donc bien lire son email et bien régler son filtre anti spam pour ne pas les manquer.
8. Par ailleurs le fournisseur reçoit la liste des comptes à suspendre pour une durée donnée (de quelques mois à 1 an), et tous les autres reçoivent la même liste avec interdiction d'accepter une demande d'abonnement de la part de ce client. Il ne s'agit pas d'une coupure mais d'un bannissement. Par contre le paiement de l'abonnement est lui toujours dû pendant le bannissement, ou les frais de résiliation si tel est votre choix.
9. La Haute Autorité garde un historique des avertissements et dénonciations pour chaque internaute dans une base de données, afin de pouvoir retracer l'escalade des sanctions et avertissements, ou appliquer le bannissement des internautes. Les « interdits d'internet » ressemblent donc aux « interdits bancaires ».

En somme un système automatisé de bout en bout à l'image des robots flasheurs sur le bord des routes, mais qui implique plus de partenaires et doit fonctionner avec quelques approximations techniques au cours de la chaîne, l'équivalent des fausses plaques pour les

flashes. L'humain (de par l'automatisation) ou le système judiciaire (de par la loi création et internet) sont absents de cette chaîne de traitement.

15 juillet 2009, De lourdes peines pour des délits unitaires, ou profiler des internautes ?

Ce qui devait arriver est arrivé, les internautes pirates s'adaptent. Le texte avait été prévu pour un état donné, mais se révèle inadapté pour un système légèrement différent, et il change vite.

Avant le passage de la loi les logiciels de partage laissaient les fichiers partagés le plus longtemps possible, pour étendre l'offre disponibles aux suivants. Aussi le nombre de fichiers proposés par un internaute était parfois élève. Maintenant, les logiciels sont réglés pour télécharger des fichiers un par un, pour que la liste proposée à un moment donné soit réduite au minimum, idéalement 1 fichier. Ce dans le but de limiter l'ampleur de la piraterie visible, et donc avoir moins de chances d'être dénoncé.

Face à cela deux possibilités : soit la Haute Autorité doit sévir avec pour motif un seul fichier téléchargé, décision difficile à justifier et de faible portée éducative. Soit les sociétés de protection des droits doivent construire un Big Brother qui suivra dans le temps les habitudes de téléchargement de chaque internaute (par son IP si possible) pour détecter des profils fortement consommateurs et les dénoncer en priorité à la Haute Autorité. De son côté la Haute Autorité a déjà une base de données retraçant toutes les dénonciations pour un internaute.

17 août 2009, Premières estimations : le piratage en baisse !

Un premier audit de la Haute Autorité réalisé fin juillet, avant même les premiers bannissements, fait état d'une baisse significative des échanges de médias protégés français sur les réseaux P2P. Le Président Sarkozy et les sociétés de protection des droits se félicitent d'une évolution si rapide des mentalités et des pratiques.

20 août 2009, Madame Michu hésite

En l'état actuel et après seulement quelques mois les pirates aguerris ont déjà adapté leurs pratiques pour contourner la loi. Madame Michu elle pas encore, en août elle bronze. Par défaut Madame Michu hésite pour la rentrée : prendre le risque faible d'une sanction moyennement forte ou arrêter. Elle devra demander à son neveu-qui-connaît-bien-les-ordis des conseils la prochaine fois.

1^{er} septembre 2009, Les pirates aguerris déjà à l'abri

La recherche des internautes pirates ou du logiciel anti-piratage se basaient tous deux jusque là sur des mots clés du nom de fichier, ce qui dans les deux cas fonctionnait assez bien. Mais deux comportements inquiétants voient le jour.

D'un côté les contestataires qui téléchargent des fichiers légaux mais renommés pour ressembler à des fichiers pirates, dans le but d'engorger le système sans être pour autant dans l'illégalité et baisser la fiabilité du système de dénonciation/sanction. Technique déjà utilisée par l'industrie ces dernières années qui avait proposé en ligne de faux fichiers nommés comme des vrais pour tromper les pirates. Dans la même veine les « trackers », ces ser-

veurs hébergés à l'étranger donnent de fausses adresses IP. Dans les trois cas le but n'est pas d'empêcher l'autre d'agir mais de créer un bruit de fond et des « faux positifs », des actes qui ont toutes les apparences du piratage mais qui n'en sont pas.

D'autres internautes, eux de vrais pirates, optent pour la discrétion. Les noms de fichiers illégaux sont changés pour des noms aléatoires et inoffensifs. Le plus efficace reste la protection par un mot de passe en plus du changement de nom. Ne reste ensuite qu'à partager sur des sites sociaux ou anonymes la correspondance entre nom de fichier véritable et discret ou les mots de passe. Cette technique était déjà utilisée sur les réseaux sociaux et les réseaux newsgroup pour se protéger depuis bien des années.

10 septembre 2009, Cours d'école et machines à café : le retour aux « mix tapes »

Face à une complexification des échanges en ligne, certains sont tentés de rentrer dans le jeu de l'escalade technique d'autant que les parades sont simples. D'autres prennent la voie humaine et se souviennent qu'avant la fibre optique il y avait la cour d'école ou la machine à café. Qu'avant de télécharger depuis le disque dur d'un inconnu à l'autre bout de la terre, les humains s'échangeaient de main à main des sélections concoctées avec amour et enregistrées sur cassette. Convivial en plus d'être efficace, la clé USB en guise de cassette.

Jusqu'à présent pratiqué en privé et anonymement, le piratage s'affiche maintenant dans le cercle semi privé. Non seulement l'arrivée de la loi création et internet n'a pas provoqué un changement des mentalités, mais l'échange de musique de main à main est devenu un acte symbolique anti-Sarkozy et anti-grands-groupes très à la mode dans cette période de crise économique.

3 octobre 2009, La mécanique des réseaux P2P évolue

En plus du piratage hors réseaux P2P en augmentation, la mécanique interne des réseaux P2P évolue. Elle reposait jusqu'à présent sur des serveurs en libre accès qui mettaient en relation les ordinateurs entre eux. Le logiciel anti-piratage utilise aussi ces serveurs pour trouver les pirates. L'évolution de ces serveurs a pris au cours des derniers mois différentes voies :

1. Polluer le serveur avec de fausses informations (de fausses IP par exemple), non gênantes pour les pirates mais provoquant de nombreux « faux positifs » pour le logiciel anti-piratage qui va dénoncer des internautes non pirates.
2. Décentraliser, faire sans serveur. La technologie DHT existait déjà, intégrée dans les logiciels de téléchargement mais n'était utilisée qu'en complément des serveurs. Elle devient maintenant la norme. Inconvénient pour le pirate : il doit attendre quelques minutes au début du lancement du logiciel. Inconvénient pour le système anti-pirate : Il doit faire partie des quelques ordinateurs connectés à un pirate pour le détecter.
3. Pour éliminer les risques, les pirates se regroupent par des sites sociaux en groupes cooptés de taille réduite pour échanger des fichiers entre eux. Soit le groupe a un petit serveur à usage privé soit la technologie DHT leur permet de faire sans serveur du tout. La protection est totale mais le choix légèrement réduit. Par contre le choix correspond mieux aux goûts des membres.
4. Faire sans P2P. Le P2P était certes une méthode en vogue grâce à sa simplicité de mise en œuvre pour le pirate débutant mais d'autres méthodes plus anciennes reviennent à la mode : les serveurs de news, ou pire de simples serveurs d'échanges d'archives. Pour ces derniers l'anonymat est total et le trafic réseau transparent.

5 octobre 2009, L'attaque des zombies pirates

Il ne manquait plus que l'entrée en scène des hackers. La loi création et internet avait pour cible un internaute lambda sans grandes connaissances techniques. Mais voilà que Madame Michu a son ordinateur infecté par un vers informatique qui a pour but de participer à son insu au réseau P2P. Dans le jargon un ordinateur « zombie ».

Son ordinateur utilise donc sa connexion internet à son insu pour aider le reste des autres ordinateurs à télécharger. De plus il expose Madame Michu à une dénonciation pour piratage. La loi spécifie bien qu'elle est responsable de l'usage qui est fait de son accès internet et que le fait de télécharger elle-même ou pas n'est pas le sujet.

10 octobre 2009, Première vague de bannissements

Devant l'évolution peu positive des mentalités mais motivés par la baisse de fréquentation des réseaux P2P, la Haute Autorité durcit le ton et décide de bannir les premiers internautes après les messages d'avertissement envoyés quelques mois plus tôt. La Haute Autorité a prévenu que les bannissements concernaient des cas de piratage multiples et répétés.

Sur les bannis quelques cas problématiques arrivent jusqu'aux medias, le premier est Monsieur F., 62 ans. Monsieur F. n'a que la télévision et le téléphone par ADSL, n'est pas porté sur la technologie et ne possède pas d'ordinateur. Il a bien de la musique chez lui mais pour moitié sur cassette audio, moitié CD pour la chaîne du salon plus quelques vinyles. Le titre pirate qui lui est reproché est de la musique écoutée généralement par des adolescentes, or il n'a pas de fille et vit seul. La Haute Autorité assure lui avoir envoyé 2 emails avant la coupure par l'intermédiaire de son fournisseur d'accès. Email que monsieur F. ne lit pas, Monsieur F. est pour son malheur encore à l'heure du papier et des timbres, en violation des conditions d'utilisation de son abonnement ADSL qu'il n'utilise que pour la télévision et le téléphone. Conditions qui stipulent depuis le passage de la loi création et internet qu'il doit lire son email.

Le premier cas met en évidence un aspect de la loi création et internet : elle ne pénalise pas le téléchargement lui-même mais le fait de ne pas empêcher les autres de le faire avec son accès internet. Or cette personne ne savait même pas que son appareil de réception de télévision par ADSL emmétrait un réseau sans fil Wifi par ailleurs. Réseau protégé par mot de passe en norme WEP et pas en WPA2. Ce système d'authentification n'est pas suffisant et peut facilement être hacké. C'est son tort.

L'autre cas médiatisé est une petite imprimerie à Lyon qui avait depuis des années un routeur Wifi non protégé par mot de passe, ce qui jusque là ne les avait jamais gênés. Au contraire les clients pouvaient venir dans leur établissement et ainsi envoyer les données à imprimer par le réseau. La PME n'avait pas de spécialiste réseau pour s'occuper des réglages du routeur et ne savaient pas que la loi création et internet s'appliquait aussi à eux.

Les deux, très remontés, envisagent leurs options juridiques. Le premier contre son fournisseur parce qu'il lui a fourni un matériel en location qui s'est avéré pas assez sécurisé pour se protéger contre un accès pirate.

Le second ne peut faire de même, le routeur a été acheté et branché par ses soins, c'est donc de sa faute, il le découvre. Il propose de laisser examiner ses disques durs par la justice pour constater l'absence de fichiers contrefaits, mais cette offre ne règle pas le problème de sa responsabilité et est donc rejeté, il a fait preuve d'un manque de vigilance. Et la justice n'entre pas en jeu dans ce système de sanction. De plus la Haute Autorité n'est composée

que de quelques personnes, dont seulement 1 au savoir technique permettant de réaliser l'expertise.

Le troisième cas, un jeune couple, est encore plus simple et déroutant, une simple erreur de suivi. Le fournisseur avait mal entré un déménagement dans son système de suivi matériel et le mauvais propriétaire était indiqué pour un boîtier de connexion ADSL, tout en fonctionnant très bien pour les deux clients. Les fournisseurs se rendent compte que leur système de suivi client et logistique, jusque là notoirement imprécis mais sans grande conséquence si ce n'est des clients mécontents de temps en temps, fait maintenant partie d'un processus répressif majeur automatisé qui les expose à des représailles juridiques de la part de leurs clients.

Des cas similaires avaient déjà été rapportés aux Etats-Unis en 2008 et 2009, ou un client s'était vu accuser à la place d'un autre à cause d'une erreur de logistique.

Pour tous ces internautes la sanction est le bannissement d'internet pour 3 mois. Ils sont inscrits sur le fichier d'interdiction d'abonnement à internet pendant cette période. Pas de conséquences gravissimes pour les quelques cas médiatisés : le retraité ne savait pas avoir internet mais est bien content de ne plus l'avoir. L'imprimeur lira les mails de ses clients à la maison et a débranché son routeur pour l'avenir. Pour le couple l'abonnement était au nom de la femme, son conjoint va s'abonner sous son nom et résilier (à ses frais) l'autre abonnement.

16 octobre 2009, Union de médias et fournisseurs

Jusqu'à présent les fournisseurs s'occupaient de donner accès à internet et les sociétés productrices de médias s'occupaient de produire et vendre des œuvres. Les clients avaient un accès identique à tous les médias, et les sociétés productrices pouvaient toucher tous les clients.

Il y avait bien des préoccupations sur le manque de concurrence, ou des exclusivités entre sociétés et fournisseurs fragmentaient l'offre accessible par le client. La tendance actuelle va bien plus loin. Les sociétés productrices réalisent que prendre le contrôle d'un fournisseur pourrait résoudre bien des problèmes. Pour commencer elles sont responsables de la dénonciation des pirates mais ont besoin des informations et de l'infrastructure des fournisseurs pour le faire plus efficacement. Ensuite cela leur permet de proposer librement leur contenu payant aux internautes captifs et refuser les offres des autres sociétés productrices.

L'effet collatéral est que la production d'œuvre en dehors des grands groupes producteurs et distributeurs ne trouve pas de débouché chez les clients, captifs de leur fournisseur. Et que tout nouveau fournisseur indépendant ne trouvera aucun contenu à proposer à ses clients.

22 octobre 2009, Annonce du filtrage d'internet en France pour lutter contre la pédopornographie et le terrorisme

L'opinion était prête à accepter cette mesure, plus pour agir que réellement être efficace. Le filtrage ne sera pas facultatif par abonné mais obligatoire pour tous et mis en place par les opérateurs. En même temps qu'une liste de 150 sites web connus, seront ajoutés 20 sites d'information sur la censure proposant des méthodes techniques permettant de passer outre les filtres de ce type. Ces sites étaient surtout visités par des internautes Chinois en quête d'une solution pour passer outre la grande muraille numérique.

10 novembre 2009, Nouvel audit : le piratage en hausse !

Le précédent audit réalisé en plein été montrait une baisse sensible de l'utilisation des plus grands réseaux P2P. Le dernier audit a décidé de prendre en compte les nouveaux réseaux P2P décentralisés qui se sont développés depuis la mise en application de la loi création et internet. Est aussi prise en compte la pratique grandissante d'échange de médias de stockage portatifs (clés USB ou disques durs).

Le nouvel audit montre que l'ensemble du trafic P2P est resté stable, mais a muté dans sa composition. L'échange de médias portatifs est lui la nouvelle mode de la rentrée 2009, mode d'autant plus préoccupante que son effet est radical : là où un pirate choisissait des albums un par un à télécharger, il reçoit en une opération toute la collection de son correspondant.

2 décembre 2009, D'anonyme le piratage devient social

Sites fermés multiples à la place de sites mondiaux, par centre d'intérêt, où pour avoir un compte il faut montrer pate blanche et émettre un certain quota. De longues étapes manuelles viennent compliquer et ralentir la procédure de recherche et de dénonciation.

De plus ceux qui veulent détecter des pirates sont maintenant obligés d'être pirate au début et d'envoyer un certain quota de fichiers avant de pouvoir télécharger.

29 novembre 2009, Qu'est ce que la neutralité du réseau ?

La neutralité du réseau, c'est le fait de ne pas discriminer les messages selon la source, la destination, ou le protocole utilisé.

Par exemple ne pas faire qu'un email à destination de gmail soit plus prioritaire qu'un autre à destination de hotmail. Que ponctuellement deux serveurs aient des problèmes et dégradent la performance pour se protéger soit, mais pas de manière constante ni même régulière. Si le problème est régulier c'est que l'infrastructure est à améliorer.

Autre exemple sur les ports. Si pour des raisons d'amélioration du service votre fournisseur vous annonce que les échanges peer2peer sont coupées, c'est que vous avez un réseau non neutre. Beaucoup pensent que le peer2peer se résume au piratage de mp3. La technologie est aussi à la base du visionnage de la BBC et CNN en ligne, ou même du fonctionnement de Skype. En fonction de la méthode de blocage de votre fournisseur, vous pourrez ou pas accéder à ces services.

En voulant éviter le piratage, une technologie a été visée en bloc et pas son usage. Les effets collatéraux apparaissent aux yeux des consommateurs et entreprises. Les fournisseurs internet et téléphonie se retrouvent au milieu de conflits qu'ils ont créé dont ils n'ont pas l'habitude. Des batailles d'expertises florissent pour savoir ce qui est réellement bloqué ou permis, par qui et si cela correspond aux conditions de vente.

5 décembre 2009, Grogne des élus et collectivités locales

Ce n'est pas le fait de télécharger mais de manquer de vigilance qui est observé et condamné. Les opérateurs de réseaux publics sont donc responsables des utilisations du réseau qu'ils offrent gratuitement à la population qui s'y connecte anonymement. La ville de Paris avait depuis quelques années développé un parc de bornes Wifi dans les jardins, des conseils généraux avaient déployé des réseaux WiMax pour couvrir de larges régions rurales non couvertes par l'ADSL.

Jusqu'en 2008 la question était de savoir comment développer un réseau sans fil couvrant des villes entières, la question en 2009 est comment s'en débarrasser et expliquer l'investissement déjà effectué.

Une alternative envisagée mais complexe à mettre en œuvre est de fermer les réseaux et de fonctionner comme tout fournisseur payant, avec un compte pour chaque utilisateur, validé par une pièce d'identité.

Les élus locaux ne sont pas les seuls. Bien des particuliers ou des commerçants avaient installé des réseaux Wifi gratuits. Ils devront les fermer.

12 décembre 2009, Il suffit de changer de fournisseur !

La rumeur grandit, pour échapper au système de profilage des internautes par leur IP il suffit de changer de fournisseur ! A moitié vrai. En effet les sociétés de protection des droits profilent les internautes par leur IP, seule la Haute Autorité peut accéder aux informations nominatives. Or cette IP peut être fixe pour toute la durée de votre abonnement comme l'est un numéro de téléphone, mais elle peut vous être attribuée pour 24 heures par exemple. C'est à votre fournisseur de faire ce choix technique. L'IP fixe était jusqu'à présent un avantage que certains fournisseurs préféraient réserver pour une offre « pro ».

Désireux de se faire repérer le moins possible par le système de profilage basé sur l'IP, certains internautes préfèrent passer chez des fournisseurs à IP variable.

15 décembre 2009, Achats de Noël ... achèterez-vous Français ?

Les sociétés de gestion collective et organismes professionnels choisissent quels œuvres sont tracées puis leurs pirates dénoncés.

Les pirates comprennent bien vite que certaines œuvres sont à risque puisque leurs confrères sont menacés ou bannis pour les avoir téléchargées. Le côté positif est que ces artistes sont moins téléchargés par les réseaux P2P classiques. Le côté négatif est que ces artistes sont stigmatisés comme étant « anti-internautes » et boycottés. Cet effet était attendu.

Un effet collatéral qui était lui peu attendu, c'est le manque à gagner dû au non piratage d'une œuvre. Le succès d'une œuvre dans le circuit commercial classique est souvent le résultat d'une visibilité sur les médias classiques. Les jeunes générations passant plus de temps sur internet que devant la télé, le téléchargement est de plus en plus considéré comme une forme d'écoute participant au succès commercial. Des exemples frappants avaient bien commencé à marquer les esprits, comme le film « Taken » qui en 2008 connu un succès sur internet qui ne trouva d'égal que dans les salles, et ce simultanément. Ou les « Ch'tis » dont l'énorme succès sur internet ne l'empêcha pas de voir ses ventes de DVD battre des records.

Un nouvel indice d'audience voit même le jour, composé du nombre de téléchargements sur divers sites pirates. Cet indice a l'avantage d'être ultra précis à la fois géographiquement, par la localisation des IP, et dans le temps. Là où l'achat en magasin ne pouvait pas forcément être attribué à une opération de communication, l'instantanéité du téléchargement est parlante.

5 janvier 2010, Le diable est dans les détails

Suite à la menace de bannissement du retraité dont le matériel loué par le fournisseur avait été piraté faute de cryptage suffisant, la Haute Autorité vient de décréter que tout point d'accès sans fil devait être sécurisé en WPA2-PSK ou mieux. Techniquement, la déci-

sion est juste et la norme bien choisie. Le but était de limiter le recours à l'argument du réseau Wifi piraté par une tierce personne, même s'il n'exonérait pas l'internaute de sa responsabilité de surveillance et n'empêchait pas son bannissement.

Réponse alarmée des fournisseurs, dont certains ont livré pendant des années des points d'accès en WEP non configurables. Le texte de la Haute Autorité demande donc expressément à leur clients de changer le matériel loué, configuré (voire dans certains cas installé) par le FAI. Les FAI concernés mettent en balance d'un côté le risque économique et logistique de remplacer une grande partie de leur parc matériel installé chez leurs clients par du matériel plus récent et mieux configuré, l'autre le risque de voir leurs clients dont l'accès sera coupé pour piratage se retourner contre eux faute d'avoir fourni un matériel correspondant aux demandes de la Haute Autorité.

Les PME sont inquiètes elles aussi, elles ont parfois du matériel acquis par leurs soins, simple mais permettant le plus souvent le nouveau cryptage. Le problème est de savoir ce qu'elles utilisent et comment le changer, ce qui demande une prestation facturée +/- 500 euros pour un tout petit réseau, bien plus que le prix de l'équipement initial. Elles n'avaient pas pour l'instant considéré la loi création et internet comme leur problème, elles découvrent qu'elle équivaut à un passage au bug de l'an 2000 ou un contrôle technique automobile pour leur réseau interne, avec des frais à la clé. L'alternative est de prendre le risque de ne pas savoir si le réseau est assez sécurisé et d'être banni d'internet.

La loi avait certes prévu que la responsabilité ne pouvait être retenue dans le cas d'une utilisation frauduleuse de l'accès, mais encore faut-il que le titulaire prouve qu'il est innocent, ce qui est un renversement de la charge de la preuve, qui plus est techniquement presque impossible.

De plus si l'internaute déclare de lui-même qu'il utilise une norme de cryptage efficace il prouve par là même que seul lui peut avoir téléchargé d'après les critères de la Haute Autorité, alors que la conclusion n'était pas si simple techniquement.

18 janvier 2010, Création et Internet phase 2 : filtrage par port du réseau

Devant les contremesures des pirates confrontés à la loi création et internet et le peu d'efficacité des bannissements, le Président Sarkozy a annoncé que d'ici quelques semaines la Haute Autorité procéderait à un filtrage par port du réseau des internautes et mettrait en liste noire les serveurs pirates.

En effet le texte prévoyait que la Haute Autorité pouvait demander des limitations à la connexion lors du rétablissement après une période de bannissement. La limitation choisie est le filtrage par port couplé à une liste noire.

En effet pour se connecter entre eux et aux serveurs les logiciels pirates utilisent un port, l'équivalent d'une fréquence pour une radio. Il suffit de bloquer ce port pour empêcher uniquement ce logiciel de fonctionner sans gêner les autres. Ce procédé avait déjà été utilisé dans la lutte contre le spam, mais de manière facultative pour l'internaute.

De plus les serveurs sont des points de rendez-vous qui facilitent les échanges. Une liste noire de ces serveurs a donc été établie et leur adresses interdites à l'accès. Cette limitation est mise en pratique par le fournisseur d'accès. Ce système assez simple est du même type que le filtrage mis en place en Chine par exemple.

25 janvier 2010, La BBC et CNN demandent l'arrêt du blocage par port

L'intitulé de la loi création et internet est "Projet de loi favorisant la diffusion et la protection de la création sur internet". En pratique, il s'agit de protéger les créations portées

par des supports physiques contre leur piratage sur internet et pas la création portée ou distribuée par internet.

Depuis plusieurs années des diffuseurs de vidéo comme BBC et CNN avaient mis en place un service de diffusion de vidéo sur internet qui ne repose plus sur un serveur unique très coûteux, mais sur les qualités technique du P2P, ou tous les internautes mutualisent leurs connections pour visionner le même programme.

Or ce système de diffusion est totalement bloqué par le nouveau blocage par port, qui a vocation à devenir la norme en France. Les deux diffuseurs demandent donc l'arrêt du blocage de la technologie P2P qui leur est vitale.

4 février 2010, Des sites légaux d'information sur la liste noire !

Il a fallu peu de temps avant que la liste noire des sites filtrés soit connue. Parmi ces sites les classiques attendus, annoncés : les principaux serveurs de peer2peer. Mais aussi certains sites d'information sur le filtrage, au contenu totalement légal mais critique et informatif sur les mécanismes de la censure. Ces sites étaient aussi utiles aux pirates qu'aux dissidents chinois. Ce scénario n'avait pas été anticipé en France, mais s'était déjà réalisé dans d'autres pays Européens à la réputation démocratique.

25 février 2010, Premiers sabotages de fibres et centraux

Le projet de loi création et internet avait certes mobilisé une partie de l'opinion et des associations contre lui avant son vote, et une grande partie des internautes depuis sa mise en application, mais le sabotage des infrastructures est lui nouveau. Jusqu'à présent le réseau propageait les idées de tous bords et était reste neutre politiquement.

Avoir rompu sa neutralité technique l'a polarisé politiquement, involontairement. Avoir permis le filtrage des contenus a aussi provoque un déséquilibre dans les opinions qui sont transportées. Les cas sont certes rares, comme le filtrage de sites légaux d'information sur le filtrage lui-même, mais emblématiques.

Le résultat est le sabotage de certains câbles transcontinentaux enterrés à faible profondeur ainsi que des incendies détruisant 2 centraux ADSL dans Paris et un à Lyon. Le but était autant de protester contre la prise en main du réseau vécue comme politique que de provoquer la population dans une logique anarchique. Après les TGV, les fibres. Au lieu de retarder 200 utilisateurs d'un TGV et risquer d'en blesser quelques uns pourquoi ne pas s'attaquer à une fibre, vitale pour des entreprises et touchant la multitude des internautes chez eux.

3 mars 2010, Des pirates, des pros, des vrais !

Face à un réseau dont la neutralité n'est plus qu'un souvenir, les internautes ont vite évolué. Face au blocage par port : changer le port de leurs logiciels était facile pour les plus expérimentés et s'est fait automatiquement après une simple mise à jour pour les autres. Face au blocage par IP sur liste noire : des serveurs d'anonymisation et de renvoi, des « proxys ». Ces serveurs sont d'autant plus frustrants qu'ils sont aussi payants qu'efficaces pour passer outre le blocage. Ils existaient déjà avant la mise en application de la loi mais n'avaient pas rencontré un grand succès jusque là. Le plus éthiquement problématique est le fait qu'ils soient payants, pour la première fois bon nombre d'internautes vont payer un intermédiaire spécialisé pour faciliter ou permettre le piratage. Il ne s'agit plus d'une démarche passive mais active de piratage de la part de l'internaute. Pour le proxy c'est une

activité fortement rémunérateur, moyens qui lui permettent d'offrir une très bonne protection à ses clients.

10 mars 2010, Nouveau filtrage : inspection des paquets

Devant l'inefficacité du filtrage par port ou par IP, et par soucis de ne pas abdiquer dans l'escalade technique, les promoteurs de la loi internet et création demandent l'inspection des paquets pour mieux filtrer. La méthode consiste à analyser le contenu d'un message « paquet » pour voir de quel type il est. Passer un colis aux rayons X si vous voulez. Ensuite selon le type de contenu, bloquer ou pas.

Les premiers à réagir sont les fournisseurs, qui se voient en charge de cette inspection. Or comme pour les rayons X, l'inspection est extrêmement couteuse en terme matérielle.

La riposte automatique des proxy payants ou gratuits fut de crypter tout le trafic.

7 avril 2010, L'inspection des paquets ne suffira pas

La neutralité du réseau n'était depuis un an qu'un souvenir, mais l'usage de la cryptographie permettait de retrouver un semblant de neutralité, le fournisseur étant incapable de savoir quel en était le contenu. La prochaine étape dans l'escalade sera donc l'interdiction de la cryptographie à usage privé.