Hugo Vainpress
Licence 3 – ADA

Cyberlog
4 rue d'Ambon 56750 Damgan
02 99 50 29 58 / 02 97 41 16 90

Impacts des lois Internet sur les professionnels offrant un accès à internet

Faculté de Finance, Banque, Comptabilité - Lille 2
25 juin 2010

Maître de stage : B.COUAPEL
Tuteur : J-G.COUSIN

Sommaire

Remerciements

Merci à Mr. Bernard COUAPEL, mon maître de stage, pour m'avoir offert ce stage et pour toute l'aide qu'il m'a apportée.

Merci également à Mme. Brigitte COUAPEL pour ses conseils avisés et son soutien.

Enfin, je souhaite remercier toutes les entreprises qui ont accepté de répondre à mes questions.

Introduction

Mon stage s'est déroulé chez Cyberlog, une entreprise Bretonne créée par Bernard COUAPEL et qui propose plusieurs services, dont la publication d'enquêtes en ligne et de rapports d'études, ainsi qu'un réseau de bornes WiFi dans le Morbihan et à Rennes.

Cette entreprise est donc directement concernée par les lois qui visent à régir Internet, telles que HADOPI, dans la mesure où l'accès au Web est l'une de ses activités, à l'instar d'un cybercafé ou d'un hôtel par exemple.

En effet, on peut considérer que la grande liberté dont jouissaient les internautes jusqu'ici a pu donner lieu à certaines dérives. C'est pourquoi, partout à travers le monde, des lois et des accords sont proposés dans le but de mettre un terme à ces comportements.

L'objectif de ce stage était donc de réaliser une étude en se posant la question suivante : quel sera l'impact de ces lois sur les établissements proposant un accès à Internet, comme Cyberlog ou les lieux publics (gares, aéroports...) ?

Ce rapport donne lieu à un questionnaire qui sera diffusé ultérieurement sur Internet (il en sera de même pour l'étude) dans le but de connaître les réactions des internautes et des professionnels concernés. Nous espérons également aboutir sur des propositions d'alternatives à la législation actuelle ou à venir, afin de trouver un système en mesure de satisfaire l'ensemble des acteurs.

Cette étude débutera sur les principales dérives qui sont imputées à Internet. Nous verrons ensuite quel est l'intérêt de ce projet. Une troisième partie sera consacrée aux lois et aux accords mis en œuvre en France ou qui sont en cours de négociations. Puis nous étudierons les aspects techniques relatifs à ces lois. Nous nous intéresserons alors aux différents acteurs concernés par la législation et à leurs intérêts. Par la suite nous porterons un regard sur les expériences qui sont menées à travers le monde. Nous verrons subséquemment la première enquête menée auprès des professionnels. Nous analyserons alors les premières propositions obtenues lors de cette enquête et des recherches réalisées au préalables. Enfin, nous terminerons par la présentation du questionnaire final.

I. Problématique générale

A l'origine, Internet était un lieu d'échange. Et pendant des années, ses utilisateurs ont bénéficié d'une liberté totale. Aucune limite n'a été fixée pour anticiper d'éventuels excès.
Or aujourd'hui, il apparaît que certains comportements sur Internet tendent à nuire à la société. Cependant, il convient de se demander si Internet est le seul responsable de ces comportements, ou si ceux-ci ne découlent pas de certaines dérives de nos sociétés actuelles.
Il y a trois thèmes sur lesquels des lois ont été proposées et ont suscité des débats : le téléchargement illégal, la pédopornographie et le terrorisme.

1. Le téléchargement illégal

En 1962, pour faire face au communisme, l'US Air Force a demandé à un petit groupe de chercheurs de créer un réseau de communication qui puisse résister à une attaque nucléaire. Le concept de ce réseau reposait sur un système décentralisé, ainsi si jamais une ou plusieurs machines avaient été détruites, le réseau aurait continué à fonctionner. Cependant, le Pentagone rejeta le projet.[1]

Quelques années plus tard, le projet fût repris pour relier quatre instituts universitaires : le Stanford Institute, les Universités de Californie à Los Angeles et à Santa Barbara et l'Université d'Utah.
Internet est né en 1968, à la demande du département américain de la défense qui souhaitait posséder un réseau permettant la transmission d'informations électroniques entre les différentes bases américaines.

En 1972, ce réseau se composait d'une quarantaine d'ordinateurs. Internet perd son caractère militaire en 1984, mais ne s'ouvrira au grand public qu'en 1995. Ce sont alors plus de 2 millions d'ordinateurs qui sont reliés, avec plus de 30 millions d'utilisateurs dans 146 pays.

Grâce à Internet, il est maintenant possible de partager tout type d'information ou de

1 http://membres.multimania.fr/djmati/informatique/internet/internet_1.htm

donnée à travers le monde dans une quasi immédiateté. Des outils ont donc été créés pour faciliter les échanges, tels que des logiciels de Peer-to-peer :
Le Peer-to-peer (abrégé « P2P ») ou pair à pair est un modèle de réseau informatique où chaque client fait également office de serveur.
Ces systèmes permettent à plusieurs ordinateurs de communiquer via un réseau et de partager simplement des fichiers sur internet.
L'utilisation d'un système pair-à-pair nécessite pour chaque ordinateur l'utilisation d'un logiciel particulier. Ce logiciel, qui remplit alors à la fois les fonctions de client et de serveur, est parfois appelé « servent » (de la contraction de « serveur »[2] et de « client »[3])

Le Peer-to-peer est donc un système qui permet de partager des fichiers à grande échelle et à grande vitesse tout en évitant le problème de surcharge des serveurs car ces derniers sont aussi nombreux que les clients.

Mais il ne faut pas confondre l'outil et les utilisations qui en sont faites.
L'utilisation de logiciels de Peer-to-peer est légale. Ce qui est illégal, c'est d'utiliser ces logiciels pour télécharger ou distribuer des oeuvres protégées par le droit d'auteur, ou d'autres fichiers dont l'objet est interdit par la loi (pornographie infantile, etc.).

Le principal problème que soulèvent donc ces échanges est celui des droits d'auteurs qui sont totalement bafoués, puisque les utilisateurs font l'acquisitions de certaines oeuvres (films, musiques...) ou logiciels, sans pour autant rémunérer les auteurs qui les ont créés.

Il paraît donc important de remédier à un tel problème, sans quoi certains artistes risqueraient de ne plus pouvoir exercer leur art. Les maisons de disques ont également mis en avant leur manque à gagner.

Toutefois, Internet n'est pas nécessairement à l'origine de cette dérive. En effet, le même problème s'était présenté par exemple lorsqu'il a été possible de copier facilement des CD.
À l'époque déjà, certains consommateurs critiquaient les maisons de disques et les distributeurs au sujet du prix de vente des CD ou des DVD.
Dans une édition de 2006, le magazine Epok (hebdomadaire distribué par la Fnac) donne

2 Le poste qui diffuse l'information
3 Le poste qui reçoit l'information

un exemple de prix de revient d'un album vendu 17,99€ en magasin[4]. Partant du postula selon lequel cette œuvre est vendue à 95 000 exemplaires, la maison de production gagne alors 5,81€ par CD, le distributeur fait une marge de 4,36€, et les artistes ne touchent que 1,70€ de royalties par vente.
Dans cet exemple, les gains pour la maison de production et pour la distribution sont donc très importants.
Etant donné que l'offre sur ce marché ne semble pas correspondre à la demande (essentiellement par rapport aux tarifs), on pourrait espérer voir les prix baisser, ce qui permettrait aux personnes les plus modestes de se procurer légalement certaines œuvres, au lieu de les télécharger.

En attendant, le téléchargement illégal peut être considéré comme une réponse à un excès de la part de l'industrie culturelle. L'offre ne correspondant pas à la demande, Internet a permis aux consommateurs de passer outre ce qu'ils considèrent comme un abus, en mettant un place un procédé tout aussi abusif.

4 http://blog.siteparc.fr/index.cfm?msg=126

2. La pédopornographie

La majorité des gens s'accorde à dire qu'il est important de protéger les enfants des dérives qui peuvent accompagner l'usage d'Internet.
La pédopornographie (définie ci-dessous) étant particulièrement inquiétante, certains pensent qu'il est nécessaire de bloquer l'accès à certains sites pour éviter aux jeunes internautes tout danger.

« La décision 2004/68/JAI du Conseil Européen, du 22 décembre 2003, relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie en donne une définition en énonçant qu'il s'agit de :

Tout matériel pornographique représentant de manière visuelle :

- un enfant réel participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne d'un enfant ; ou
- une personne réelle qui paraît être un enfant participant ou se livrant au comportement visé sous le premier tiret ; ou
- des images réalistes d'un enfant qui n'existe pas participant ou se livrant à un comportement sexuellement explicite . »[5]

Bien qu'il soit nécessaire d'agir, il subsiste une certaine appréhension à l'idée d'interdire l'accès à certains sites internet, car on pourrait craindre que la liste de ces sites ne s'étende à d'autres domaine que la pédopornographie, ce qui risquerait à terme de nuire à la liberté d'expression sur le Net.

5 http://fr.jurispedia.org/index.php/Moyens_de_la_lutte_contre_la_p%C3%A9dopornographie_sur_l%27Internet_%28fr%29

3. Le terrorisme

Depuis le choc des attentats du 11 septembre 2001, le problème du terrorisme a commencé à prendre une place importante dans la vie de tous les jours du fait de sa médiatisation et des réactions des pouvoirs politiques.

La sécurité contre le terrorisme est ainsi devenue un sujet essentiel aux yeux de la population. Des mesures ont alors été appliquées là où le risque d'attaques terroristes était fort (le plan Vigipirate dans les gares par exemple) dont Internet fait partie.
La chercheuse israélienne Limore Yagil a défini le cyberterrorisme comme le fait de "détruire ou corrompre des systèmes informatiques dans le but de déstabiliser ou de faire pression sur le gouvernement", dans son livre Terrorisme et internet: la cyberguerre (publié en 2002). Cependant, à notre connaissance, ce type d'attentat ne s'est pas encore réalisé.
Mais Internet reste tout de même un outil très utile pour les groupes terroristes. Gabriel Weimann (Université de Haïfa), dont l'United States Institute of Peace a publié deux rapports en 2004, a identifié 8 types d'utilisations d'Internet par ces groupes :

- Créer une pression psychologique, en proférant des menaces et en publiant des vidéos d'exécution d'otages par exemple.
- Faire de la propagande
- Récolter des informations
- Collecter des fonds via des groupes extrémistes qui font office de relais
- La mobilisation des sympathisants
- La mise en réseau, qui permet de garder le contact entre les différents maillons d'un groupe
- Partager des informations (comment fabriquer des engins explosifs)
- Planifier des actions et se coordonner

Internet apparaît donc bel et bien comme un instrument que le terrorisme s'est approprié.

Dans ce climat d'angoisse, probablement attisé par l'omniprésence de la violence (dans les médias, le cinéma, la télévisions...), il peut paraître nécessaire d'instaurer un certain contrôle.
Mais comment faire pour ne pas empiéter abusivement sur les libertés des utilisateurs ?

II. Intérêt du projet

Les problématiques développées ci-dessus sont généralement traitées du point de vue des particuliers, utilisant Internet chez eux via leur propre connexion.
L'objectif de cette étude sera de nous placer du côté des entreprises qui proposent un accès à Internet au public, comme Cyberlog par exemple.
En effet, des mesures à la fois techniques et légales sont mises en place par différents acteurs, afin de résoudre les problèmes précédemment abordés. Le but est de savoir quelles en seront les répercussions pour des entreprises telles que des cybercafés, qui offrent un accès à Internet à un grand nombre de personnes.

Exemple de Cyberlog

Cyberlog est une entreprise bretonne de prestations de service ancrée dans la mouvance du logiciel libre depuis 1999. Son dirigeant Bernard COUAPEL souhaite mettre ses compétences dans ce domaine au service des diverses attentes des entreprises et des collectivités.

Les prestations proposées par Cyberlog sont :

- La formation et le développement du libre dans les entreprises et collectivités.
- Les enquêtes en ligne, ainsi que des rapports d'études (comme le présent document).
- Un réseau de bornes WiFi à destination des collectivités locales, campus universitaires, copropriétés, salons et manifestations événementielles.
- L'aide à l'import / export avec la Chine

→ Commerce électronique sur sa plateforme Internet à destination des entreprises bretonnes qui souhaitent présenter et vendre leurs produits sur le marché du commerce électronique, et des entreprises chinoises qui cherchent à faire connaître leurs produits sur le marché européen.

→ Mise en relation et facilitation des échanges commerciaux entre des sociétés européennes et des usines de production chinoises, grâce à une correspondante en

Chine, directrice d’une société d’import-export à Pékin.

Ainsi, cette étude s'inscrit pleinement dans le cadre de l'activité de Cyberlog, plus particulièrement dans le domaine du réseau de bornes WiFi que propose l'entreprise.

En effet, il est essentiel pour Cyberlog et pour ses collaborateurs de connaître les mesures à mettre en place pour respecter la législation et ne pas être mis en cause par la loi dans le cas où un client la transgresserait.

III. Aspects juridiques

1. 2006 : Loi contre le terrorisme

La Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme a été votée en France sous l'impulsion de Nicolas Sarkozy, alors ministre de l'Intérieur du gouvernement Villepin. Cette loi est controversée, notamment en raison de l'article 6, qui impose aux opérateurs de télécommunications, aux fournisseurs d'accès (FAI), mais aussi à tout établissement public proposant un accès à Internet, comme les cybercafés, de conserver les données de connexion ("logs") jusqu'à un an.[6]

La loi prévoit que l'accès à ces logs par les autorités policières ne soit plus soumis à l'autorisation d'un magistrat (et donc effectué sous contrôle judiciaire), mais simplement de celle d'un haut fonctionnaire de la police nommé par la Commission nationale de contrôle des interceptions de sécurité (CNCIS[7]), une autorité administrative indépendante chargée de veiller au respect de la réglementation en matière d'interceptions de communications privées, comme les écoutes téléphoniques.

Cette loi ne devait être valide que jusqu'à fin 2008, mais fut prorogée jusqu'en 2012 par la loi n° 2008-1245 du 1er décembre 2008.

Selon la CNIL qui émettait son avis sur le projet de loi, celui-ci prévoyait que « les services de police et de gendarmerie anti-terroristes pourront accéder à certains fichiers administratifs gérés par le ministère de l'intérieur (fichiers des immatriculations, des permis de conduire, des cartes nationales d'identité, des passeports, des ressortissants étrangers en France, des demandes de visas et de titres de séjour). » Suite à l'avis de la CNIL, le projet de loi a été modifié, afin que l'accès aux fichiers de l'Intérieur ne puisse intervenir que dans les conditions fixées par la loi Informatique et libertés de 1978 (le traitement de

6 http://fr.wikipedia.org/wiki/Loi_n%C2%B0_2006-64_du_23_janvier_2006_relative_%C3%A0_la_lutte_contre_le_terrorisme

7Cette commission est présidée par une personnalité désignée, pour une durée de six ans, par le Président de la République, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'Etat et le premier président de la Cour de cassation. Elle se compose également d'un député désigné par le président de l'Assemblée nationale, et d'un sénateur désigné par le président du Sénat.

l'information doit intéresser la sûreté de l'État, la défense ou la sécurité publique, et une demande doit être adressée à la commission).

La CNIL a émis un avis le 10 octobre 2005 concernant cette loi. Si certaines de ses préoccupations ont pu être prises en compte, celle-ci rappelle que d'autres ont été ignorées par le législateur. La lutte anti-terrorisme lui semble n'être qu'un motif parmi d'autres, donnant droit à l'accès aux bases de données mentionnées dans le texte. Elle a aussi regretté :

- la « prise systématique de photographie des occupants de l'ensemble des véhicules empruntant certains axes de circulation » (que le Conseil constitutionnel a validé);
- l'absence de définition des personnes offrant un accès à Internet et chargées de conserver trace des données de l'ensemble des connexions;
- enfin, la constitution d'un fichier central de contrôle des déplacements en provenance ou à destination d'Etats situés en dehors de l'Union européenne, aux contours mal définis.

En octobre 2005, la CNIL a déclaré que la lutte contre le terrorisme « conduit à mettre à la disposition des services de police et de gendarmerie, dans le cadre de leurs missions de police administrative, des fichiers et enregistrements vidéo susceptibles de "tracer" de façon systématique et permanente une très grande partie de la population, dans ses déplacements et dans certains actes de la vie quotidienne (le lieu où l'on se trouve à tel moment, l'heure d'une connexion Internet, le lieu d'où l'on passe un appel depuis un mobile, le passage à tel péage d'autoroute, la destination d'un voyage, etc.) »[8]. Certains considèrent alors que cette loi porte directement atteinte à nos libertés.

Certaines dispositions (dont ce qui relève des données de connexion), prévues pour une durée de 3 ans (à la demande de la CNIL), ont été prorogées l'échéance venue, par la loi du 1er décembre 2008, votée par le gouvernement Fillon, et ce jusqu'en 2012.

8 http://fr.wikipedia.org/wiki/Loi_n%C2%B0_2006-64_du_23_janvier_2006_relative_%C3%A0_la_lutte_contre_le_terrorisme

2. DADVSI

Droit d'Auteur et Droits Voisins dans la Société de l'Information

Ce texte a été adopté par l'Assemblée nationale et le Sénat le 30 juin 2006, avant d'être examiné par le Conseil constitutionnel qui en a supprimé certaines dispositions. Le texte, publié au Journal officiel le 3 août 2006, prévoit des amendes d'un montant de 300 000 euros ainsi que 3 ans de prison pour toute personne éditant un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés, et jusqu'à 6 mois de prison et 30 000 euros d'amende pour toute personne diffusant ou facilitant la diffusion d'un logiciel permettant de passer outre les mesures techniques de protection (DRM, pour Digital Rights Management) qui selon ses défenseurs visent à empêcher les « copies pirates ». Le projet de « licence globale », prévu en décembre 2005, n'a pas été retenu (mais reste au programme de plusieurs partis d'opposition).[9]

À cette loi a fait suite sur le même sujet le projet de loi HADOPI.

Ce texte détermine également les règles concernant le champ d'application de la copie privée, c'est-à-dire le droit pour tout usager de procéder à la copie, l'enregistrement, la duplication et la sauvegarde pour strict usage personnel, des œuvres ou documents auquel il a légalement accès (à l'exclusion des fichiers dits piratés).

9 http://e-plug.net/accueil.html

3. HADOPI :

a. HADOPI 1

L'objectif de cette loi est de mettre un terme ou du moins d'endiguer les échanges d'œuvres (musiques, films, logiciels,…) qui ont lieu sur les réseaux Peer-to-Peer, sans l'accord des ayants-droits. Cette loi comporte la création d'une autorité administrative (la Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet) chargée de mettre en œuvre les dispositifs de surveillance et de sanction des pratiques d'échanges de fichiers de pair à pair.

Cette loi rend responsable les intermédiaires mettant à disposition des accès gratuits à Internet. Les accès Wi-Fi gratuits ou payants sont très développés dans les restaurants, les bars, les hôtels, les bibliothèques, les jardins publics, les universités et dans de nombreux autres lieux par l'intermédiaire d'acteurs privés, publics ou associatifs. Cette loi demande la mise en place de moyens techniques pour empêcher l'accès à des œuvres protégées.[10]

La HADOPI a le pouvoir de réclamer aux FAI les coordonnées des personnes suspectées de piraterie, afin de leur envoyer deux avertissements dans l'espoir de les dissuader de perpétrer leurs activités. Le premier avertissement se fait par courrier électronique, puis si les présumés pirates sont suspectés de récidive, le deuxième est envoyé sous forme de lettre recommandée. Enfin, si ces avertissements n'ont aucun effet, la HADOPI peut alors exiger que la connexion Internet des accusés soit suspendue pendant une durée maximale de un an, avec l'incapacité de souscrire à un nouvel abonnement chez un autre FAI tout au long de la peine.

Selon l'Association de Lutte contre la Piraterie Audiovisuelle (ALPA) qui a réalisé une surveillance de 8 mois sur les principaux réseaux peer-to-peer entre novembre 2007 et juin 2008, en moyenne 450 000 films étaient téléchargés chaque jour en France. On a donc bien affaire à une pratique de masse, qu'il serait impossible d'éradiquer en procédant au cas par cas.

10 http://fr.wikipedia.org/wiki/Loi_Cr%C3%A9ation_et_Internet

La loi HADOPI semble donc être la mieux adaptée pour mettre un terme au téléchargement illégal, dans la mesure où grâce à un système de filtrage (voir l'exemple de l'Irlande, partie VI.1), il est possible de se procurer rapidement un grand nombre d'adresses IP de présumés pirates, ceci de manière automatisée.

Cependant, lors de la présentation du premier texte, certaines personnes s'inquiétaient déjà du risque que cette loi faisait courir pour certains principes fondamentaux de notre société démocratique. Le Conseil constitutionnel a donc rejeté une partie du projet, considérant qu'il portait atteinte au principe de séparation des pouvoirs en octroyant à une autorité administrative la possibilité de priver des personnes de droits et de libertés garantis par la Constitution, à savoir la liberté d'expression et de communication.
De plus, le Conseil constitutionnel a pointé du doigt la présomption de culpabilité pesant sur les internautes accusés hâtivement de ne pas avoir sécurisé leur réseau.
Enfin, les membres du Conseil ont considéré que l'accès à Internet était lié à la liberté d'expression et de communication reconnue par la Constitution.

La première version de la loi HADOPI était donc confrontée à un obstacle de taille. Elle perdait ainsi son atout principal (savoir sa capacité à faire face à un comportement de masse en automatisant les sanctions) du fait que chaque condamnation devait passer par un juge.

b. HADOPI 2

Un deuxième texte a alors été proposé (HADOPI 2), afin d'essayer de minimiser cet écueil. Cette nouvelle version propose un recours au juge unique et aux ordonnances pénales en matière de délits de contrefaçon, c'est à dire qu'il n'est plus nécessaire de procéder à une enquête complexe dans le but de trouver des preuves.
En effet, le simple constat d'un agent de police suffit à établir qu'il y a une infraction. Le parquet peut ainsi saisir le juge qui statue sans débat contradictoire. L'ordonnance pénale est généralement appliquée dans le cas d'infractions au code de la route.

Néanmoins, pour que le délit soit constaté par des officiers de polices, ces derniers vont devoir procéder à des perquisitions chez les personnes soupçonnées de piratages, afin de vérifier sur les disques durs que ces personnes sont bien en possession d'œuvres

numériques. Il faudra par la suite prouver que ces fichiers ont été obtenus sans que les auteurs n'aient reçu de compensation.
Si cette procédure n'est pas respectée, le juge n'aura d'autre possibilité que de renvoyer le dossier au parquet.

4. LOPPSI :

Loi d'orientation et de programmation pour la performance de la sécurité intérieure

Le dispositif initialement proposé par le Gouvernement, vise à la mise en place d'un système de blocage de sites Internet présentant du contenu pédopornographique. La liste des sites bloqués serait secrète et les mesures de filtrage édictées par arrêté du ministère de l'Intérieur.

On reproche à ce dispositif de faire courir de grands risques, tant sur le plan technique que du point de vue des libertés fondamentales, alors que l'efficacité du filtrage n'a pas été démontrée. En effet, le blocage de sites Internet porte gravement atteinte à la neutralité du Net, qui est un principe fondateur d'Internet excluant toute logique de contrôle centralisé du réseau et qui est inhérent à la liberté de communication permise par ce nouveau moyen de communication.
Selon le projet initial, les Offices Centrales Spécialisés pour la Répression des Violences aux Personnes (OCRVP) et de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) étaient habilités à dresser une liste secrète des sites catalogués comme pornographiques et à enjoindre aux fournisseurs d'accès Internet (FAI) d'en bloquer l'accès.
La censure administrative d'Internet qui aurait ainsi été mise en place présentait un risque réel d'inconstitutionnalité. En effet, le Conseil constitutionnel a estimé dans sa décision du 10 juin 2009 concernant la loi HADOPI que seule l'autorité judiciaire était habilitée à prononcer des mesures visant à restreindre ou empêcher l'accès à des sites Internet. En effet, seul le juge judiciaire, garant des libertés fondamentales, a la capacité de s'assurer de la pertinence des mesures de filtrage de sites Internet, qui vont à l'encontre de la liberté de communication constitutionnellement garantie.
Le 27 janvier dernier, lors de l'examen du projet LOPPSI 2, la Commission des lois de l'Assemblée nationale a donc jugé nécessaire que ces filtrage soient soumis à une décision préalable de l'autorité judiciaire.

Le dispositif de filtrage tel qu'il ressort de l'examen du projet de loi par la commission des lois est loin d'être satisfaisant. En effet, à ce stade du processus législatif, le risque de sur-filtrage de sites Internet n'est pas du tout pris en compte. Les expérimentations menées à l'étranger montrent que les techniques du filtrage peuvent mener au blocage de sites parfaitement légaux.

Au Royaume-Uni, par exemple, l'intégralité du site Wikipedia s'est ainsi retrouvée bloquée pendant près de trois jours fin 2008 car un article relatif à un groupe de musique contenait une reproduction d'une pochette d'album considérée comme relevant de la pédopornographie par l'organisme en charge de la liste noire, l'Internet Watch Foundation. Des dérives similaires ont été constatées dans de nombreux pays.

Devant l'incapacité du dispositif à remplir l'objectif de lutte contre la pédopornographie, on peut craindre que le gouvernement n'utilise ce sujet extrêmement sensible pour ensuite étendre, voire systématiser, le filtrage de l'Internet.

Le filtrage pourrait être ainsi être utilisé pour tenter de combattre le partage d'œuvres culturelles en ligne. En juin 2008, interrogé par PCINpact, le directeur général de la SPPF, Jérôme Roger, qui représente les producteurs indépendants français, a déclaré :

« Les problématiques de l'industrie musicale ne sont pas éloignées de ces autres préoccupations [la pédophilie] qui peuvent paraître évidemment beaucoup plus graves et urgentes à traiter. Bien évidemment, les solutions de filtrage qui pourraient être déployées à cette occasion devraient faire l'objet d'une réflexion à l'égard des contenus, dans le cadre de la propriété intellectuelle ».

Le risque, s'il devenait interdit de partager une œuvre culturelle en ligne, serait que les artistes souhaitant le faire gratuitement n'y soient même plus autorisés.

5. ACTA :

a. Principes

L'Anti-Counterfeiting Trade Agreement (ACTA) est un traité international en cours de négociation depuis 2007. Les participants sont l'Australie, la Corée du Sud, la Nouvelle-Zélande, le Mexique, la Jordanie, le Maroc, Singapour, les Etats-Unis, l'Union Européenne, la Suisse, le Japon, les Emirats arabes unis et le Canada.
L'objectif de cette négociation, dont le contenu a longtemps été tenu secret, est d'harmoniser la lutte contre la contrefaçon et le non respect des droits d'auteur dans le monde (principalement au sujet des faux médicaments et du téléchargement illégal).
Notons que la Chine et l'Inde ne font pas partie des négociations et même s'opposent à ce traité, car les Etats-Unis et l'Union Européenne souhaiteraient appliquer l'ACTA aux pays du monde entier, même ceux qui n'ont pas participé à son élaboration.

Pendant un certain temps, les seuls informations sur le contenu de l'ACTA à disposition du grand public provenaient de fuites publiées sur des sites comme Wikileaks (spécialisé dans la publication anonyme de documents confidentiels).
Parmi ces informations, on pouvait commencer à entrevoir des mesures qu'instaurerait ce nouveau traité :
«

- L'obligation pour les fournisseurs d'accès à Internet de fournir l'identité du propriétaire d'une adresse IP (Internet Protocol), sans mandat judiciaire, aux organismes de défense des ayants-droit.
- La possibilité pour les douaniers et gardes-frontières de confisquer ordinateurs, baladeurs ou disques durs contenant des fichiers contrefaits, comme des morceaux de musique téléchargés illégalement.
- Le durcissement des sanctions pour la violation des mesures techniques de protection (Digital rights management systems, DRM), comme les logiciels anti-copie présents sur les DVD. »[11]

11 http://www.lemonde.fr/technologies/article/2010/01/25/l-acta-le-traite-secret-qui-doit-reformer-le-droit-d-auteur_1296265_651865.html

b. Les critiques

La Quadrature du Net, une organisation de défense des droits et libertés des citoyens sur Internet, a publié sur son site en mars dernier une version de travail de l'ACTA datant du 18 janvier 2010. Elle a alors mis en avant plusieurs points qui lui semblaient particulièrement inquiétants, à savoir (entre autres) :

- D'une part, le fait de traiter ce texte comme une négociation internationale de manière à réaliser un « blanchiment de politique », ce qui « consiste à utiliser les organisations internationales pour mettre en place des politiques que se heurtent à la résistance des institutions nationales. Adoptées comme des décisions auxquelles les Etats sont tenus de se conformer, ces politiques échappent au débat démocratique »[12]. Ainsi, les parlements devront soit ratifier soit rejeter l'acte dans son ensemble et aux Etats-Unis, le Congrès pourrait même ne pas être consulté.
- D'autre part, l'ACTA semble généraliser la présomption d'infraction et mettre au même niveau la contrefaçon commerciale de masse et le partage de fichiers numériques sous copyright.

Selon l'organisation Free Software Foundation qui promeut le monde du libre en informatique et qui défend les droits des utilisateurs de logiciels libres (type OpenOffice par exemple), ce traité qui vise à renforcer le pouvoir du copyright pourrait menacer directement les logiciels libres en freinant leur distribution.

En outre, l'ACTA obligerait les hébergeurs de contenus générés par les utilisateurs à faire « la police du copyright »[13] en supprimant toute donnée ne respectant pas les droits d'auteur, sous peine de se voir infliger une amende.

Enfin, certains s'inquiètent de la façon dont seront (ou non) différenciés les médicaments génériques et ceux issus de divers trafiques. Si les génériques ne peuvent plus passer les douanes, cela risquerait de porter atteinte à l'accès aux soins dans les pays pauvres.

12 http://www.laquadrature.net/fr/trois-raisons-de-rejeter-lacta
13 http://www.politis.ch/carnets/2010/01/20/acta-le-traite-qui-fera-de-vous-un-criminel-de-linternet/

Ce traité a donc déjà suscité une levé de boucliers dans plusieurs secteurs partout dans le monde. Peut-être que les participants aux négociations l'avaient anticipée, ce qui pourrait expliquer cette méthode de « blanchiment de la politique ». En évitant les voies démocratiques habituelles, cet accord a certainement plus de chances de voir le jour pour la fin de l'année (puisque tel est l'objectif).

IV. Aspects techniques

1. Sécuriser sa connexion

a. Pourquoi sécuriser

Pour les débutants comme pour les experts en informatique, il est très difficile (voire impossible) de sécuriser parfaitement son installation Internet, ou plus précisément, son WiFi.

Aujourd'hui, cette technologie qui permet d'avoir une connexion sans fil est très répandue chez les utilisateurs. Tous les fournisseurs d'accès à Internet la proposent, tant elle est utile.

Cependant, l'avantage de ce système fait également sa faiblesse en matière de sécurité. En effet, étant donné qu'aucune liaison physique n'est nécessaire entre le modem et l'ordinateur (il n'y a plus de câble) et que les ondes du WiFi peuvent s'étendre en dehors du bâtiment dans lequel se trouve la point d'accès à internet, il suffit de se trouver non loin de la borne pour capter la connexion de quelqu'un d'autre (son voisin par exemple).

Une personne peut alors utiliser un WiFi voisin afin de télécharger de la musique illégalement sans être inquiété par la loi, puisque ce sera le propriétaire de la connexion qui sera identifié.

Il va donc être nécessaire pour les établissements offrant un accès WiFi de mettre en place un système d'identification avant d'autoriser la connexion, sans quoi ils seront considérés comme coupables des forfaits des utilisateurs.

De plus, lorsqu'une personne s'introduit sur un réseau sans fil, il lui est possible d'avoir accès aux documents partagés (voire ceux qui ne le sont pas si elle a les connaissances nécessaires) qui se trouvent sur les ordinateurs de tous les autres utilisateurs. Dans le cas d'un ordinateur de travail contenant des dossiers importants et/ou confidentiels, les répercussions peuvent être conséquentes.

b. Moyens de sécurisation

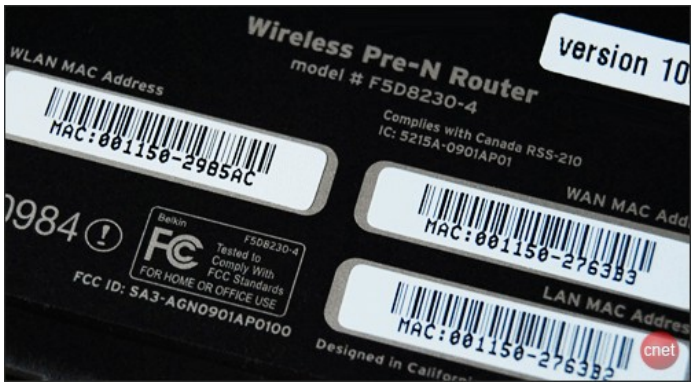
**** Le cryptage des communications***

Afin de remédier à ces problèmes, les constructeurs ont très rapidement proposé des protocoles de chiffrement des communications et d'authentification. Le plus ancien et le plus connu se nomme WEP (Wired Equivalent Privacy). C'est celui qui est utilisé sur certaines box par exemple, requérant un mot de passe pour avoir accès au réseau.

Ces protocoles peuvent bien sûr être piratés (parfois facilement), mais ils créent tout de même une barrière non négligeable.

**** Le filtrage par adresse MAC***

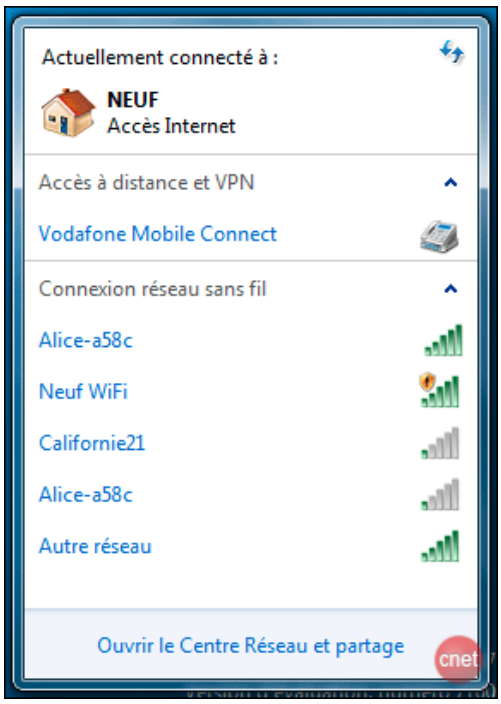
Chacun des éléments de votre réseau tel que le routeur, les cartes WIFI ou cartes réseau possèdent une adresse unique attribuée par le fabricant : l'adresse MAC. On trouve cette adresse soit sur une étiquette à l'arrière de l'objet, soit grâce à la commande ipconfig sous Windows.



Ce filtrage permet donc d'interdire l'accès à un réseau à tout équipement dont l'adresse MAC ne fait pas partie de celles que l'on a répertoriées.

**** Changer et cacher le SSID***

Le SSID est le signal envoyé par la box ou le routeur et qui permet d'identifier le réseau. C'est ainsi qu'avec l'outil de gestion du WiFi sur Windows, ou avec AirPport sur Mac, il est possible de voir tous les réseaux voisins.



Il est possible de masquer le SSID de son réseau, ce qui permet d'être invisible pour AirPort ou l'outil de Windows. Il faut alors être capable de configurer sa connexion en indiquant le SSID manuellement.

2. HADOPI, une loi déjà facilement contournable

Voici des exemples de solutions de téléchargement qui ne sont pas détectables par Hadopi (ou par les ayants droits plus précisément), qui sont basées sur l'utilisation d'outils légaux, et donc qui rendent Hadopi inefficace.

a. Internet anonyme

Cette solution ne demande pas de connaissances très développées de la part de l'utilisateur, mais le débit peut être très limité. Cela consiste à rejoindre un réseau de communications anonyme sur Internet. Le plus connu d'entre eux est Tor. Ce réseau regroupe un grand nombre de routeurs à travers le monde par lesquels circulent les requêtes TCP-IP des utilisateurs sans qu'aucun contrôle ne soit possible. Les chemins pour aller d'une adresse IP source à une adresse IP destination par l'intermédiaire des routeurs de Tor sont aléatoires et chaque communication d'un routeur à un autre est chiffrée. Un message qui passe par x routeurs est ainsi chiffré x fois.
L'inconvénient est que ce réseau dépend des ressources que les utilisateurs mettent à disposition, dans ce genre de cas la demande des utilisateurs tend toujours rapidement à excéder les capacités du réseau. Ainsi, cette solution est efficace pour télécharger des fichiers de petites tailles, mais n'est pas approprié pour obtenir rapidement de gros fichiers. Ce service est légal s'il n'est pas utilisé pour télécharger illégalement du contenu payant.

b. Le Peer-to-peer sécurisé (ou VPN)

C'est une solution imparable une fois installée, et d'utilisation relativement aisée. Il existe des services gratuits mais pour avoir un service de qualité les offres payantes peuvent être mieux adaptées. Il s'agit d'établir une connexion chiffrée pour accéder à un serveur situé à l'étranger jouant le rôle de passerelle vers les réseaux P2P. Cette technique, dite de tunnel sécurisé ou de VPN (réseau privé virtuel), est souvent utilisée par les entreprises pour accéder de manière sécurisée à leur intranet depuis l'extérieur. Son

utilisation ne permet pas aux agents chargés par l'Hadopi d'identifier l'adresse IP des pirates puisque que c'est le site passerelle, généralement basé à l'étranger, qui joue les intermédiaires. Même le FAI de l'internaute ne sait pas ce que fait son abonné. Il existe plusieurs sites qui proposent ces services VPN, par exemple peer2me qui est gratuit, ou alors des services payants comme par exemple Steganos, Pirate Bay IPREDator, ... Ce service est légal s'il n'est pas utilisé pour télécharger illégalement du contenu payant.[14]

c. Les newsgroups

L'utilisation des newsgroups est une solution pour utilisateur moyennement averti, accessible gratuitement. Usenet est un système en réseau de forums de discussions, inventé en 1979 et basé sur le protocole NNTP. Cette solution est inviolable et le risque d'être poursuivi est d'autant plus faible que les serveurs sont généralement hébergés à l'étranger dans des pays peu coopératifs. La connexion étant chiffrée en SSL il n'y a aucun moyen pour le FAI de savoir ce que télécharge l'utilisateur, et le seul moyen pour la France de savoir ce que l'utilisateur télécharge est de perquisitionner son ordinateur (difficilement réalisable sans preuve, sans compter que là aussi le disque dur de l'utilisateur peut être crypté) ou de perquisitionner le serveur (d'autant plus difficile s'il est à l'étranger, surtout s'il ne conserve aucun log ce qui est fort probable). Les newsgroups n'ont rien d'illégal en soit, ils servent sur le principe à échanger des fichiers et des messages tout à fait légaux. Ce service est légal s'il n'est pas utilisé pour télécharger illégalement du contenu payant.

d. Les sites de stockage en ligne

Assez faciles d'accès, catalogue très important, indétectable pour Hadopi. Voici les 2 principaux sites de stockage :

- Rapidshare : Site web de nationalité allemande et hébergé en Suisse, proposant un service d'hébergement de fichiers en un clic
- Megaupload : Site d'hébergement de fichiers en un clic. Il permet aux utilisateurs de

14 http://www.developpez.net/forums/d736173/club-professionnels-informatique/actualites/politique/hadopi-loi-hadopi-efficace-solutions-techniques-contourner/

mettre à disposition des internautes des fichiers d'une taille maximale d'1 Go. Ce service est légal s'il n'est pas utilisé pour télécharger illégalement du contenu payant.

e. Les sites de musique en ligne

Ces sites sont très simples d'emplois et proposent généralement un grand nombre de titres. Il suffit de faire une recherche sur le site pour trouver un artiste ou un album que l'on veut écouter, puis de lancer la lecture.
De cette manière, l'utilisateur ne télécharge pas les musiques sur son ordinateur et il ne peut pas les partager. Il peut ainsi profiter de ces œuvres gratuitement et sans risquer d'être détecté par les ayants droits.
Parfois, certains titres sont retirés des sites, mais il suffit généralement d'en consulter un autre (jamendo, deezer, jiwas) pour retrouver lesdits titres.

En option il existe des logiciels à télécharger pour récupérer les fichiers mp3 écoutés, ce qui n'est pas légal et pourtant non détectable.

f. Streaming video

Ceci reprend le même système que les sites de musique en ligne.
Les sites de streaming (MégaVidéo, Allostreaming) proposent un grand catalogue de films et de séries que l'on peut regarder directement dessus.
Là encore rien n'est partagé entre les utilisateurs, cela ne relève donc pas du Peer-to-peer.
Des programmes permettent de télécharger les vidéos que l'on regarde, mais leur utilisation n'est pas légale si l'on sort du cadre du streaming pour télécharger et stocker illégalement du contenu payant. Cela reste tout de même indétectables.

V. Les acteurs

Les lois et les accords qui sont proposés englobent plusieurs types d'acteurs qui ont des intérêts différents, et sur qui les répercussions d'une telle législation ne doivent pas être négligées.
Essayons d'identifier certains de ces acteurs ainsi que les conséquences que la loi aura sur eux.

1. Les artistes et créateurs de logiciels

Dans le cas de la loi HADOPI, on a vu que l'objectif était entre autres de préserver les droits d'auteur, et ainsi de protéger toute personne qui crée un bien ou une œuvre intellectuelle.
Cette loi permettrait donc théoriquement de mettre un terme au téléchargement illégal, dans l'espoir de voir les anciens pirates se réorienter vers des offres légales.
Dans ce cas, les ventes seraient relancées et les auteurs toucheraient davantage de royalties.

Cependant, comme l'a démontré l'étude de Sylvain Dejean, Thierry Pénard et Raphaël Suire nommée « Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français », on remarque que les personnes qui téléchargent illégalement représentent la moitié des acheteurs numériques sur Internet.
Donc si HADOPI, pour éradiquer le téléchargement illégal, supprimait l'accès des pirates à Internet, c'est 50% du chiffre d'affaires qui s'envolerait par la même occasion dans ce secteur.

De plus, si l'offre actuelle (sur le marché du disque par exemple) ne convient pas à la demande des pirates car trop onéreuse, il est peu probable que ces derniers se retournent vers les solutions légales sous prétexte qu'ils ne peuvent plus télécharger.

Il n'est donc pas certain pour le moment que l'intérêt des auteurs soit sauvegardé par une loi telle que HADOPI.

2. La CNIL

La Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante française qui fut créée le 6 janvier 1978. Son but est de protéger les données à caractère personnel traitées par informatique en France.

Cette commission doit être consultée avant que des lois comme HADOPI ne puissent être appliquées, afin de déterminer si ces lois portent ou non atteinte à la vie privée et aux libertés individuelles.

De plus, toute entreprise ayant un fichier client informatisé doit le déclarer auprès de la CNIL, afin que celle-ci puisse contrôler que les informations personnelles ne portent pas atteinte à la vie privée des personnes fichées.

Le 11 juin dernier, la Société Civile des Producteurs de Phonogrammes en France (SPPF) a annoncé que la CNIL lui donnait l'autorisation de commencer à collecter les adresses IP de personnes mettant à disposition (de manière illicite) sur les réseaux peer-to-peer des enregistrements audio ou vidéo déclarés à son répertoire.

La CNIL ne semble donc pas s'opposer à HADOPI, et ainsi ne considère pas que cette loi porte atteinte aux libertés des utilisateurs d'Internet.

3. Les commerçants

a. Les cybercafés

Les cybercafés sont des établissements qui proposent un accès à Internet. Mais étant donné que de plus en plus de foyers sont équipés et qu'il devient possible de se connecter de n'importe où grâce à son téléphone portable, d'autres services sont généralement proposés (photocopie, jeux en réseaux...).

Les lois et projets que nous avons vus précédemment s'appliquent évidemment à ces établissements, qui doivent garder une trace de chaque personne qui utilise Internet.
Mais tous les cybercafés ne mettent pas en place cette mesure. Certains pensent qu'elle n'est même pas applicable, car trop fastidieuse.
De plus, pour que ces informations soient utiles, encore faudrait-il s'assurer qu'elles ne sont pas erronées. Il deviendrait alors nécessaire pour les responsables de cybercafés de demander une pièce d'identité à chaque personne qui souhaite utiliser d'Internet, ce à quoi certains se refusent, jugeant que cela porterait atteinte à la vie privée des clients. En outre, certains pensent que le fait de demander un justificatif d'identité pourrait indisposer les utilisateurs, et ainsi créer un préjudice commercial.

Les lois étudiées semblent donc apporter un certain nombre de contraintes à ce type de commerce.

Concernant la loi HADOPI, il est prévu que les intermédiaires (cybercafés, bornes WiFi...) soient tenus responsables si un utilisateur a téléchargé des fichiers illégalement via leur réseau et qu'ils n'ont pas mis en place de mesures de protection contre le piratage.
Lesdits intermédiaires courent donc un grand risque s'il ne savent pas comment sécuriser leur réseau informatique.

b. Les hôtels et campings

Aujourd'hui, de nombreux hôtels proposent un accès à Internet à leurs clients.

Lors d'un entretien avec le gérant d'un hôtel (voir VII), ce dernier m'a présenté ce service comme une obligation pour lui, dans la mesure où Internet fait partie de la vie courante et qu'il est donc nécessaire de s'adapter aux besoins des clients. Cependant, ce service ne lui semblait pas très rémunérateur, étant donné que la demande n'était pas très forte dans cet établissement (6 connexions pour 39 chambres).

Contrairement à une personne qui tient un cybercafé, il est impossible pour le gérant d'un hôtel de contrôler directement de quelle manière un client utilise internet. En effet, une chambre d'hôtel est un lieu privatif au même titre qu'une maison.
Le même type de problème se pose pour le campings, pour qui il serait bien trop fastidieux de vérifier que personne ne consulte un site litigieux.
Les hôtels et campings se doivent donc de mettre en place des mesures techniques afin de ne pas mettre en jeu leur responsabilité si un client venait à enfreindre la loi.
Or il est probable que certains ne savent pas comment procéder, peut-être préfèreront-ils alors ne pas proposer d'accès à Internet plutôt que risquer une amende.

VI. Expériences menées dans d'autres pays

1. L'Europe

En **Suède**, les tribunaux ont ordonné la fermeture du site The Pirate Bay, le plus gros portail d'indexation de fichiers Bittorrent[15] et une loi permet désormais aux ayants droits de contacter les fournisseurs d'accès pour obtenir l'identité des internautes pirates.[16]

En **Italie**, le décret Romani prévoit de contrôler la mise en ligne et la diffusion de contenus vidéos par un système d'autorisation préalable. De plus, il est déjà fréquent dans ce pays que les personnes doivent présenter une pièce d'identité pour avoir accès à Internet dans un lieu publique.

En **Allemagne**, la cour régionale de Hambourg a obligé le site RapidShare à supprimer les 5 000 musiques qu'il offrait en téléchargement.
La riposte graduée n'a pas été votée dans ce pays. La ministre de la justice considère en effet qu'une telle loi aurait trop de mal à passer et que le fait de couper l'accès à Internet n'est pas acceptable.

Au **Royaume-Uni**, la riposte graduée a été votée lors de l'été 2008, mais le parlement britannique est revenu sur sa décision. Le ministre de la propriété intellectuelle David Lamy a jugé que la sanction était excessive.

En **Irlande**, une loi identique à HADOPI a récemment commencé à être appliquée. Les pirates détectés recevront trois avertissements : un simple courrier de mise en garde, puis un second courrier accompagné d'une suspension de la connexion pendant sept jours, pour finir par une coupure d'Internet pendant une année.
Le principal FAI, Eircom, a commencé par envoyer une cinquantaine de courriers pour la première semaine d'application.
Pour localiser les personnes qui téléchargent illégalement et qui partagent des données protégées, les maisons de disques utilisent un programme de filtrage développé par Dtecnet. Elles ont ainsi envoyé une liste de plusieurs milliers d'adresses IP au FAI, qui

15 Les bittorrent utilise le système de peer-to-peer. Ils sont donc concernés par la loi HADOPI.
16 http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf

enverra de plus en plus de courriers chaque semaine.
Certaines études ont démontré que 80% des internautes arrêteraient de télécharger après le premier avertissement. Reste à savoir si cela portera profit aux majors de la culture.

En **Norvège**, une association de l'industrie phonographique a menacé de soutenir une action en justice contre les fournisseurs d'accès à Internet si ces derniers refusaient de bloquer l'accès à certains sites (tels que Pirate Bay à l'époque). Le ministre de l'Education et de la Recherche, Bard Vegar Solhjell, n'a pas été favorable à ce passage en force et s'intéresse davantage à la solution de la licence globale, qui permettrait de télécharger légalement en payant chaque mois une somme forfaitaire.
Les lobbyes de l'industrie culturelle proposent eux une autre approche, très critiquée par une partie des internautes, à savoir le filtrage des contenus et la suppression de certains sites Internet. Mais les FAI Norvégiens s'y opposent.

2. La Chine

L'Assemblée nationale chinoise a voté des lois sur la censure de l'Internet. Avec ces lois, selon les FAI, le gouvernement a mis en place différents systèmes de censure, détenus par les provinces, des sociétés privées ou des associations. Ce projet a pour nom « Bouclier d'or ».[17]

Concrètement, cette censure se vérifie par certains sites totalement inaccessibles, certaines censures temporaires mais le plus souvent facilement contournables : un site anonymiseur permet en effet d'accéder à une majorité des sites bloqués.

La coopération active de certains acteurs occidentaux majeurs du Web comme Microsoft Live ou Yahoo est critiquée.

En revanche, le 12 janvier 2010 Google a menacé de quitter la Chine après des agressions informatiques massives « venant de Chine » envers des chinois militants pour les droits de l'homme. Google indique avoir les preuves que ces attaques devaient permettre d'investir les comptes gmail de ces militants. Google a décidé de rendre publique cette situation car il s'agit d'un « débat mondial sur la liberté d'expression ». Hillary Clinton a demandé des explications au gouvernement chinois concernant ces attaques informatiques. Entre mars et juillet 2010, Google.cn (la version chinoise du moteur de recherche Google) a été fermé. L'accès à ce site se traduisait par une redirection vers Google.com.hk, la version Hong-Kongoise qui, elle, n'est pas soumise aux mêmes demandes de censure qu'en Chine continentale.
Cependant, depuis juillet Google s'est engagé à respecter la loi chinoise et a ainsi rouvert le site.

La partie pare-feu de ce système est connue à l'extérieur de la Chine continentale sous le nom de Grande Muraille pare-feu de Chine en double référence à son rôle de pare-feu réseau et à la Grande Muraille. Constitué de pare-feux standards sur les serveurs proxy (passerelles Internet), ce système bloque les contenus en empêchant certaines adresses IP d'être routées. Cependant le gouvernement ne peut examiner à chaque instant l'Internet entier, cette méthode est donc limitée.

Deux niveaux de blocage des serveurs extérieurs sont mis en œuvre. La plupart des

17 http://internet-chine.blogspot.com/2009_09_01_archive.html

serveurs sont « filtrés » ; l'internaute attend indéfiniment, comme si le site était saturé. Certains serveurs sont « bloqués » ; tout se passe comme si le site refusait la connexion. Les sites filtrés sont accessibles à travers les sites relais anonymiseurs. Pour accéder aux sites bloqués, il faut faire appel à d'autres techniques. La plupart des sites anonymiseurs commerciaux ne sont pas eux-mêmes filtrés.[18]

18 http://fr.wikipedia.org/wiki/Censure_de_l%27Internet_en_R%C3%A9publique_populaire_de_Chine

3. L'Amérique du Nord

Au **Canada**, les personnes qui téléchargent illégalement via le Peer-to-peer sont repérées par leur fournisseur d'accès à Internet, qui ralentit alors le débit de données. Mais cette mesure est apparemment contestée.
Ce pays envisage également de procéder comme l'Irlande et la France à une riposte graduée.

Aux **Etats-Unis**, l'Etat n'a pas encore légiféré à ce sujet. De ce fait, les dispositions mises en place ne sont que des accords entre les représentants des ayants droits et les FAI. Ces derniers ont accepté d'envoyer des courriers électroniques à leurs clients repérés comme des pirates, mails ils refusent tout de même de couper la connexion à ces personnes, même en cas de récidive, car ils considèrent que cette décision relève de la justice.

VII. Enquêtes

1. Première partie : entretien

Afin de connaître l'avis des entreprises concernées par ces lois et de me familiariser avec les problématiques, j'ai réalisé une première enquête en me rendant directement sur le terrain.
Cette enquête s'est déroulée sous forme d'entretiens avec les gérants ou les employés de huit commerces proposant un accès à Internet, sur la base de questions prédéfinies (voir annexe 1).

Tout d'abord, il a été intéressant de constater que très peu de personnes avaient entendu parler d'HADOPI depuis que le conseil constitutionnel l'avait rejetée en partie. Cette loi commençait à être oubliée de tous.
La loi de 2006 relative à la lutte contre le terrorisme était quant à elle totalement inconnue des commerçants, et donc quasi inappliquée.
En effet, bien que certaines enseignes aient déjà mis en place un système d'identification. Ces derniers permettent de récolter les noms et prénoms des clients qui utilisent Internet, ou encore leurs coordonnées bancaires (en guise de caution) dans le cas d'un hôtel.
Cependant, ce système d'identification n'était pas mis en place en vertu de la loi de 2006, mais uniquement dans un cadre commercial.
De plus, les utilisateurs n'avaient pas à fournir de carte d'identité, et pouvaient ainsi donner un faux nom s'ils le souhaitaient.

Or, pour qu'une telle mesure soit efficace, il serait nécessaire de s'assurer que les informations enregistrées ne sont pas erronées. Le fait de demander une pièce d'identité soulève des avis partagés. La moitié des personnes interrogées y voient une procédure fastidieuse (trop long lors des heures de pointe) et certaines pensent que cette mesure serait mal perçue par les clients, ce qui porterait préjudice aux commerces. Le reste des personnes interrogées ne voient aucun problème à appliquer ce genre de procédure.
À ma grande surprise, malgré l'aversion que quelques-uns ont exprimée pour jouer le rôle de policier, la quasi totalité des commerçants rencontrés demanderaient un justificatif d'identité aux utilisateurs si la loi le leur imposait.
On note donc que malgré certaines réticence, il n'y a pas chez les commerçants une

franche opposition au fichage des utilisateurs d'Internet.

Par ailleurs, d'un point de vue technique, aucune restriction n'était mise en place quant à l'utilisation d'Internet. Aucun site n'était bloqué, et il était possible d'installer un logiciel de Peer-to-peer si on le souhaitait. Sur le plan théorique donc, il était facilement possible de se rendre sur un site pédopornographique ou de télécharger un film en utilisant la connexion de ces enseignes.
Cependant, aux dires des personnes qui tiennent ces commerces, le problème ne s'est quasi jamais présenté car elles ont toujours un oeil sur ce qui se passe sur leurs ordinateurs. En effet, soit le commerçant est placé de manière à voir l'ensemble des écrans, soit il se déplace à travers la salle pour contrôler rapidement ce que font les utilisateurs. Parfois, ce sont les clients eux-mêmes qui exercent un contrôle en informant le gérant du magasin.
Certains utilisent aussi un système de vidéo surveillance, permettant de vérifier ce qui s'affiche sur l'écran du client. Dans un cas, les caméras ont permis d'identifier une personne suspectée par la police. Le responsable de ce cybercafé gardait en effet les enregistrements sur un disque dur pendant trois mois, et se disait parfaitement d'accord pour transmettre ces video aux services de police, mais uniquement dans le cas où cela concerne une personne déjà suspectée.

En conséquence, bien que les moyens de contrôle soient relativement artisanaux, ils ont tout de même montré leur efficacité.

En ce qui concerne le blocage de certains sites Internet, 7 personnes sur 8 m'ont répondu qu'elles y étaient favorables, principalement par rapport à la pédophilie. Mais la seule personne qui s'y opposait pensait que justement, la pédophilie et le terrorisme servaient de prétexte (car personne ne cautionne ces deux actes) au gouvernement pour produire des lois qui s'attaquent aux libertés et qui seront modifiées ultérieurement pour être de plus en plus strictes, et pour contrôler de plus en plus Internet. Selon cette personne, mieux vaut laisser Internet s'autoréguler grâce à ses utilisateurs.
En revanche, aucun commerçant n'avait foi en ces lois qui sont proposées ou déjà en place comme HADOPI ou LOPPSI. En effet, aucune ne leur semblait applicable efficacement, et ils savaient qu'elles seraient facilement contournées par les internautes qui avaient quelques connaissances nécessaires.
Concernant HADOPI plus précisément, l'avis général était que cette loi n'atteindra que les

personnes les plus faibles qui ne sauront pas la contourner, tandis que le téléchargement continuera à se développer.

Les entretiens que j'ai ainsi menés m'ont permis de constater que parmi les professionnels qui proposent un accès à Internet, déjà les opinions pouvaient être radicalement différentes, allant d'une personne qui trouve que les lois sont trop souples, à une autre personne qui pense qu'aucune loi ne devrait restreindre les libertés sur le Web.
L'objectif de cette première étape était également de m'aider à mettre en place un questionnaire plus précis à soumettre aux entreprises.

2. Deuxième partie : questionnaire (aux professionnels uniquement)

L'intérêt de ce questionnaire (voir annexe 2) résidait dans le fait qu'il était plus précis que les questions posées dans les entretiens précédent. Il était donc suffisamment pertinent pour pouvoir me permettre de le proposer à un grand nombre de professionnels et ainsi d'analyser mes résultats via des statistiques.

J'ai donc envoyé ledit questionnaire par E-mail à plus de 60 établissements, essentiellement des cybercafés, des campings et des hôtels, mais aussi un centre commercial et un centre culturel à Rennes avec qui j'avais pris contact au préalable.

Cependant, après deux séries d'envois, seulement 2 réponses m'ont été retournées (un camping et un cybercafé). Il m'est donc impossible de fournir une analyse intéressante avec si peu de résultats.
Ces quelques informations m'ont tout de même conforté dans l'impression que les cybercafés et salles de jeux sont ceux qui ont le plus de connaissances et qui se tiennent davantage informés sur les lois.
En effet, la personne du cybercafé qui a répondu à ce questionnaire connaissait toutes les lois citées, y compris LOPPSI. De plus, elle semblait être parfaitement au fait des moyens de contournements de ces lois.
Les cybercafés sont les commerçants qui s'opposent le plus à une identification des clients. La tâche leur paraît à la fois fastidieuse, mais aussi rédhibitoire pour leur type de clientèle. Certains arguent que les personnes qui se rendent dans un cybercafé arrivent parfois avec seulement de quoi payer et que donc, dans le cas où il faudrait présenter une carte d'identité pour utilisé Internet, il y a un risque pour le commerce de perdre des ventes.

Ces deux réponses ont également confirmé le scepticisme qui règne autour de ces tentatives de contrôle d'Internet. Connaisseurs en informatique ou non, tous s'accordent pour dire que les utilisateurs connaissent les moyens de contourner les lois, ce qui généralement les rend obsolètes à leurs yeux.
Étant donné que ces lois sont loin de faire l'unanimité, voyons quelles sont les propositions avancées par les autres acteurs.

VIII. Propositions

1. La contribution créative

Cette proposition reprend exactement le même concept que celui de la licence globale, rejeté lors des débats sur la loi DADVSI.
La contribution créative constituerait donc un aménagement du droit d'auteur, comme on a pu en voir dans les années 1970 lorsque les industries télévisuelle et radiophonique se sont développées. En effet, c'est à cette époque que la rémunération équitable a été instaurée, à savoir une somme forfaitaire versée à la Société de Perception de la Rémunération Equitable (qui la reverse ensuite aux artistes) lorsque un programmateur décide de diffuser une œuvre.

La contribution créative permettrait ainsi d'échanger des œuvres sur internet sans que cela soit illégal, et tout en respectant les droits d'auteurs.
Cependant, la mise en place de procédé impliquerait une perte de contrôle qu'ont les grands groupes de l'industrie culturelle sur la circulation des œuvres. On peut donc supposer qu'ils ne seraient pas favorable à un tel aménagement des droits d'auteurs.

2. L'avis de Richard Stallman

Richard Stallman est un est un programmeur et militant très réputé dans le domaine du logiciel libre.
Celui-ci a proposé deux solutions pour s'opposer à HADOPI :
D'une part, que les droits d'auteurs durent 10 ans à partir de la publication. Stallman préconise une telle durée car selon lui, aux Etats-Unis beaucoup de produits culturelles sont vendus à prix réduits au bout de 2 ans, et deviennent introuvable au bout de 3. Une durée de 10 ans semble alors raisonnable.
D'autre part, Stallman suggère la mise en place d'un paiement volontaire : “ Si tu avais un bouton pour envoyer un euro très facilement à l’artiste, tu le ferais. ”. Il prend ainsi l'exemple de la chanteuse canadienne Jane Siberry qui reçoit en moyenne plus d’un dollar par morceau téléchargé. “ C’est plus que les 99 cents demandés par les maisons de disques ”,

3. Aide de l'Etat

Lors de mes entretiens, j'ai entendu à plusieurs reprises des gérant dire qu'ils ne s'opposeraient pas à un durcissement des règles, mais il faudrait pour cela que l'Etat fournisse une aide financière ou matérielle.

En effet, s'il est nécessaire de renforcer la sécurité de son réseau, cela peut avoir un coût que les professionnels n'ont pas envie d'assumer. Certains ont donc préconisé que l'Etat apporte un soutien financier afin que tout le monde puisse protéger son équipement.

De plus, par rapport à l'identification des utilisateurs, plusieurs personnes ont avancé que l'Etat devrait fournir un logiciel qu'il suffirait de lancer sur les ordinateurs pour que le système d'identification soit mis en place. Une personne a par ailleurs précisé que dans ce cas, les informations devraient être directement envoyées chez l'autorité compétente, afin que les commerçants n'aient pas à se préoccuper de ces données.

Grâce à un faible nombre d'entretien et à quelques recherches sur Internet, il est déjà possible d'entrevoir de nouvelles possibilités ou des améliorations à apporter aux lois actuelles. Afin de recevoir davantage de propositions, il paraît intéressant de demander leur avis à un maximum de personnes. C'est pourquoi cette étude débouche sur le questionnaire suivant.

IX. Questionnaire

Grâce à ce questionnaire, nous espérons déterminer si, selon les professionnels et les particuliers, les lois précédemment présentées auront un réel impact sur les comportements des utilisateurs et donc sur l'activité de certaines entreprises. L'objectif final est d'obtenir un maximum de nouvelles propositions.

Le questionnaire sera programmé de manière à adapter les questions en fonctions des réponses précédentes. C'est pourquoi, au début de certaines questions on peut lire « **[Professionnels] »,** ce qui signifie que la personne aura coché une autre réponse que « Un particulier » à la première question.

Voici donc le questionnaire qui sera prochainement mis en ligne :

Vous êtes (Votre activité)

- Un particulier
- Un hôtel ou camping
- Un cybercafé ou professionnel de l'informatique
- Autre :

Vous tenez-vous informé(e) sur les lois et projets de lois relatifs au terrorisme, au téléchargement illégal et à la pédophilie sur internet ?

- Oui
- Non

Connaissez-vous la loi de 2006 relative à la lutte contre le terrorisme ? Loi qui oblige les établissements offrant internet à garder les logs des utilisateurs pendant un an

- Oui
- Non

[Professionnels] : Êtes-vous d'accord pour demander une pièce d'identité à vos clients ?

- Oui
- Non

[Professionnels] [Si réponse = « non »] : Pourquoi ?

[Professionnels] : Pensez-vous que cela porterait préjudice à votre commerce ?

[Professionnels] : Si la loi l'impose, l'appliquerez-vous ?

- Oui
- Non

[Particuliers] : Seriez-vous disposé à donner votre carte d'identité et à figurer sur un listing informatique ?

- Oui

- Non

[Particuliers] : Pensez-vous que la majorité des clients accepteront de présenter leur carte d'identité ?

- Oui
- Non

CNIL

Connaissez-vous la CNIL ?

- Oui
- Non

[Professionnels] : Avez-vous un fichier client ?

- Oui
- Non

[Professionnels] [Si réponse = « oui »] : L'avez-vous déclaré auprès de la CNIL ?
[Particuliers] : Êtes-vous d'accord pour que les fichiers clients soient déclarés auprès de la CNIL ?

- Oui
- Non

HADOPI

Connaissez-vous la loi HADOPI, contre le téléchargement illégal ?

- Oui
- Non

[Professionnels] Avez-vous mis en place des mesures techniques pour éviter que les utilisateurs téléchargent illégalement ?

- Oui
- Non

[Professionnels] : Pensez-vous que certains clients arrivent tout de même à utiliser votre connexion pour télécharger illégalement ?

- Oui
- Non

[Professionnels] : Pourquoi ?
[Particuliers] : Avez-vous déjà téléchargé illégalement dans un lieu public ?

- Oui
- Non

[Particuliers] [Si réponse = « oui »] : Continuerez-vous si on vous demande une pièce d'identité ?

- Oui
- Non

Pensez-vous que cette loi permettra de contrôler internet efficacement ?

- Oui

- Non

[Si réponse = «non»] : Pourquoi ?
Connaissez-vous les moyens de contournement de ces lois ?

- Oui
- Non

[Professionnels] : Pensez-vous que vos clients les connaissent ?

- Oui
- Non

[Professionnels] : Seriez-vous prêt à suivre une formation pour mieux gérer la sécurité de votre système informatique ?

- Oui
- Non

LOPPSI

Connaissez-vous le projet de loi LOPPSI ? Projet de loi qui vise à filtrer certains sites (pédopornographie...)

- Oui
- Non

Êtes-vous favorable à un filtrage de certains sites internet ?

- Oui
- Non

[Si réponse = « oui »] : Quels types de sites ?

[Si réponse = «non»] : Pourquoi ?

Avez-vous des propositions ou un commentaire à faire sur les lois abordées par ce questionnaire ?
Pertinence de ces lois, idées de mesures alternatives...

Conclusion

Que ce soit dans la lutte contre la pédopornographie, le terrorisme, ou le téléchargement illégal, il semble nécessaire d'établir de nouvelles règles afin d'endiguer tout problème à venir.
Cependant, la culture d'Internet est basée sur une grande liberté, ce à quoi sont encore attachées un grand nombre de personnes. Ces dernières auront donc tendance à entrer immédiatement en opposition avec les lois qui ont pour objet le contrôle du Web.
Or ce n'est pas en étant en conflit que les différents acteurs arriveront à faire entendre leur point de vue par le côté adverse.
De plus, aujourd'hui les lois n'ont pas même le temps d'être votées que les hackers ont déjà trouvé une solution pour les contourner.
On peut donc penser que, tant que les hackers auront l'ascendant et que ce climat de conflit perdurera, toute nouvelle tentative ne sera que perte de temps et d'argent.

Il est donc important de trouver des solutions, en écoutant les propositions de chacun et en les synthétisant, dans le but de trouver un compromis acceptable pour tous.

La solution de l'enquête diffusée sur Internet, basée sur cette étude, semble être un bon moyen de toucher un grand nombre de personnes et ainsi recueillir différentes opinions et propositions.
Cependant on peut craindre un manque d'intérêt et de mobilisation de la part de la population, comme en a attesté ma tentative avec mon premier questionnaire diffusé.

Sources

http://www.cyberlog-corp.com

http://fr.jurispedia.org

http://www.zdnet.fr

http://www.laquadrature.net

http://forums.cnetfrance.fr

http://hadopinfo.fr

http://www.lefigaro.fr

http://www.lemonde.fr

http://fr.readwriteweb.com

http://www.adami.fr

http://www.01net.com

http://fr.wikipedia.org

http://www.numerama.com

http://eco.rue89.com

http://www.terrorisme.net

http://www.web-libre.org

http://membres.multimania.fr

http://www.marsouin.org

http://internet-chine.blogspot.com

Annexes

1. Guide d'entretien de la première enquête (1ère étape)

Savez-vous en quoi HADOPI vous concerne ?
Connaissez-vous la CNIL ?
Ces deux entités ne vous semblent-elles pas en désaccord, dans la mesure où l'une demande de conserver des informations personnelles sur les clients, tandis que l'autre exige le respect des libertés informatiques ?
Avez-vous été informé sur les lois et projets de lois comme HADOPI ou LOPPSI ?
Utilisez-vous un système d'identification pour vos clients qui utilisent Internet ?
Demandez-vous les coordonnées des personnes qui viennent chez vous ? Si oui, quelles info demandez-vous (nom adresse) ? Faut-il montrer une pièce d'identité ?
Est-ce que vous autorisez tous les services d'Internet ?
Comment agissez-vous pour prévenir le téléchargement par vos clients ?
Autorisez vous les clés usb ?
Est-ce que ces lois vous dissuaderaient de proposer d'autres services (comme le WiFi) ?

Etes-vous favorable à une restriction des libertés sur Internet de manière générale ?

Pourquoi ouvrir des WiFi ? Est-ce que cela présente un avantage commercial ? La demande est-elle importante ?

2. Questionnaire soumis aux professionnels (2ème étape)

Vous êtes (Votre activité)

- Cybercafé
- Hôtel
- Camping
- Autre :

Vous tenez-vous informé(e) sur les lois et projets de lois relatifs au terrorisme, au téléchargement illégal et à la pédophilie sur internet ?

- Oui
- Non

Connaissez-vous la loi de 2006 relative à la lutte contre le terrorisme ? Loi qui oblige les établissements offrant internet à garder les log des utilisateurs pendant un an

- Oui
- Non

Êtes-vous d'accord pour demander la pièce d'identité de vos clients ?

- Oui
- Non

Sinon, pourquoi ?

Pensez-vous que cela serait préjudiciable à votre commerce ?

- Oui
- Non

Si la loi l'impose, l'appliquerez-vous ?

- Oui
- Non

En tant que clients ailleurs, seriez-vous disposé à donner votre carte d'identité et à figurer sur un listing informatique ?

- Oui
- Non

CNIL

Connaissez-vous la CNIL ?

- Oui
- Non

Avez-vous déclaré votre fichier client à la CNIL ?

- Oui
- Non

HADOPI

Connaissez-vous la loi HADOPI, contre le téléchargement illégal ?

- Oui
- Non

Avez-vous mis en place des mesures techniques pour éviter que les utilisateurs téléchargent illégalement ?

- Oui
- Non

Pensez-vous que certains clients arrivent tout de même à utiliser votre connexion pour télécharger illégalement ?

- Oui
- Non

Pourquoi ?

Pensez-vous que cette loi va permettre de contrôler internet efficacement ?

- Oui
- Non

Sinon, pourquoi ?

Connaissez-vous les moyens de contournement de ces lois ?

- Oui
- Non

Pensez-vous que vos clients les connaissent ?

- Oui
- Non

Seriez-vous prêt à suivre une formation pour mieux gérer la sécurité de votre système informatique ?

- Oui
- Non

LOPPSI

Connaissez-vous le projet de loi LOPPSI ? Projet de loi qui vise à filtrer certains sites (pédopornographie...)

- Oui
- Non

Êtes-vous favorable à un filtrage de certains sites internet ?

- Oui
- Non

Si oui, quels types de sites ?

Sinon, pourquoi ?

Avez-vous des propositions ou un commentaire à faire sur les lois abordées par ce questionnaire ? Pertinence de ces lois, idées de mesures alternatives...

3. Exemple de demande d'informations personnelles dans un commerce

ENREGISTREMENT OBLIGATOIRE

Vous vous connectez pour la première fois sur notre réseau, la loi du 23 Janvier 2006 relative à la lutte contre le terrorisme nous oblige référencer nos utilisateurs.

Si vous utilisez le même ordinateur ou PDA pour vous connecter vous n'aurez plus à ressaisir ce formulaire.

Vous nous voyez désolé de cette nouvelle contrainte, ces données ne sont collectées qu'a des fins légales, elles ne seront pas utilisées à des fins commerciales ni transmises à des tiers.

Ce fichier fait l'objet d'une déclaration à la Commission Nationale de l'Informatique et des Libertés.

Nom* :
Prénom* :
Adresse* :
Code postal* :
Ville* :
Région* :
Pays* :
Email* :

* Champs obligatoires

VALIDER

Table des matières