Projet de loi Loppsi 2 sur Internet : Filtrage, fichage et piratage à tous les étages

- Les médias - Internet - Internet et libertés -

Date de mise en ligne : mercredi 20 janvier 2010

Date de parution : 18 janvier 2010

Description :

Périlleux précédents et sérieuses menaces sur les libertés numériques, la liberté d'expression et, somme toute, les libertés publiques.

Alors que, au moment où nous écrivons, deux décrets d'application de la loi Hadopi ne sont toujours pas publiés (dans l'attente d'un avis de la Cnil qui tarde à venir), les fastueux locaux ont été aménagés et les membres de la Haute autorité ont été nommés.

Mais Hadopi n'est qu'une étape dans la traque des internautes. Depuis quelques mois, le gouvernement prépare une nouvelle offensive contre les libertés numériques dans le cadre du projet de loi Loppsi 2 (« Loi d'Orientation et de Programmation Pour la Sécurité Intérieure »). Des motifs apparemment légitimes peuvent être des prétextes et des précédents redoutables, surtout quand on constate que le projet Loppsi 2 intervient au moment où l'Union européenne travaille dans la plus grande discrétion à la mise en place d'outils de surveillance du web et est partie prenante dans les négociations secrètes autour du futur Accord commercial anti-contrefaçon qui est soupçonné de vouloir étendre Hadopi à l'international.

Nous nous proposons ici de faire le point, en nous appuyant sur les critiques que ce projet a déjà suscitées. Nous en reparlerons lors du prochain Jeudi d'Acrimed : « Haro sur Internet », le 21 janvier.

Le projet de loi Loppsi 2, déposé le 27 mai 2009 et publié sur le site de l'Assemblée nationale, devrait être discuté dans le courant de l'année à l'Assemblée nationale. D'ores et déjà, il suscite réserves et inquiétudes, que ce soit du côté de la Cnil, du Syndicat de la magistrature ou [des défenseurs des libertés numériques, comme loppsi.org. Outre qu'il prévoit une inquiétante extension des possibilités d'accès aux fichiers de police et de leur utilisation (y compris à des fins d'enquête administrative, par exemple pour les personnels appelés à travailler dans des « zones sensibles » comme les aéroports), la création de nouveaux fichiers attentatoires aux libertés individuelles ou un important développement de la vidéosurveillance, il entend également introduire diverses mesures de surveillance et de filtrage du Net et de ses utilisateurs.

Le filtrage de la pornographie infantile comme cheval de Troie ?

Ainsi, le projet de loi envisage dans son article 4 de filtrer Internet, via l'élaboration d'une « liste noire » de sites interdits, au prétexte de la lutte contre la pédopornographie.

> I. - L'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est ainsi modifié :
> 1° Après le quatrième alinéa du 7. du I, sont insérés deux alinéas ainsi rédigés :
> « Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant des dispositions de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 les adresses internet des services de communication au public en ligne entrant dans les prévisions de cet article, et auxquelles ces personnes doivent empêcher l'accès sans délai. [...] »

Le motif semble légitime. Mais...

Mais partout où il a été mis en place, le filtrage en vue de lutter contre la pornographie infantile sur le Net s'est révélé d'une redoutable inefficacité. Il est même arrivé qu'il interdise l'accès à des sites qui n'ont rien à voir avec la pornographie infantile, comme par exemple en Australie, où *« environ la moitié des sites sur la liste ne sont pas liés à la pornographie pédophile, il y a un grand nombre de sites de poker, de liens YouTube, de sites gay ordinaires et de pornographie hétéro, d'entrées Wikipedia, de sites sur l'euthanasie, de sites sur des religions marginales, satanistes, fétichistes, de sites chrétiens, un site sur un tour operator et même un site d'un dentiste du Queensland »* , ainsi que le relève le blog News of Tomorrow (lien mort, janvier 2011) citant le *Sydney Morning Herald* [1].

Ce n'est pas tout. Une telle disposition remet gravement en cause la neutralité du Net : principe de base d'Internet, qui veut que le réseau permette à tout utilisateur d'avoir accès sans discrimination à tous les contenus qui y sont diffusés ainsi qu'à tous les protocoles permettant d'y accéder, et de diffuser librement du contenu sans discrimination, c'est-à-dire sans censure ni filtrage, en utilisant ces mêmes protocoles. Tout filtrage apparemment sélectif crée un redoutable précédent. Jérémie Zimmermann, porte-parole de La Quadrature du Net, s'en inquiète sur le blog du NouvelObs.com (« Geek c'est chic ») : *« Bientôt seront filtrés les sites de jeux interdits, les sites marchands ne payant pas la TVA, puis pourquoi pas les sites faisant offense au président de la République... Instaurer le filtrage, c'est ouvrir la boite de Pandore, ouvrir la porte à la censure du web. »* Pour lui, le filtrage de la pédopornographie est *« un cheval de Troie pour le filtrage des autres contenus »* et la volonté de filtrer le web est *« la prochaine grosse tendance législative »*. Quant à l'Asic (Association des services Internet communautaires) elle s'interroge sur la constitutionnalité d'une telle mesure, après la censure d'Hadopi première version par le Conseil Constitutionnel, soupçonnant que cette mesure, si elle était adoptée, serait elle aussi censurée pour les mêmes raisons.

Adopter le principe du filtrage ouvre la porte à tous les abus.

Par exemple, dans l'hypothèse où les FAI (fournisseurs d'accès à Internet) ne seraient pas ou que partiellement dédommagés pour leurs efforts, ils pourraient bien exiger une contrepartie de l'Etat pour la mise en place à leurs frais du dispositif : pouvoir filtrer des sites ou services offerts par des concurrents (par exemple, de la vidéo à la demande) ou certains protocoles comme le « peer-to-peer » (qui est déjà victime de ces procédés) par l'intermédiaire de ce qu'on appelle des demi-connexions. Certes, pour l'instant, les FAI, ou du moins Free, comme le relève PcInpact, s'opposent à une mesure qui engage trop leur responsabilité. Et ils semblent avoir finalement obtenu gain de cause, dans la mesure où le projet de loi inclut désormais un principe de subsidiarité (qui fait qu'il ne seront saisis qu'en dernière instance, après démarches auprès de l'éditeur puis de l'hébergeur) et supprime pour eux de l'obligation de résultats. Pourtant, il ne faut pas croire que le projet de les impliquer directement soit abandonné.

De surcroît, la mise en place de la liste noire et de techniques dites de « filtrage hybride », c'est-à-dire mariant le filtrage par nom de domaine et adresse IP présente des risques supplémentaires.

Le principe est le suivant, comme l'explique La Quadrature du Net dans une note de synthèse sur le sujet .Au travers d'enquêtes ou sur signalement d'internautes, les services de police maintiennent une liste noire d'URL pointant sur des ressources pédopornographiques. Cette liste est communiquée aux Fournisseurs d'Accès à Internet (FAI) qui empêchent l'accès à ces ressources à leurs abonnés. Concrètement, à partir de la liste noire, les FAI récupèrent la liste d'adresses IP correspondant aux noms de domaines où sont hébergées les ressources à bloquer. Puis, ils envoient une commande à leurs routeurs via le protocole Border Gateway Protocol (BGP) pour les reconfigurer, afin que toute demande d'accès à une des IP suspectes soit routée vers la plate¬-forme de filtrage, et non plus relayée directement au serveur demandé par l'utilisateur. Ainsi, lorsqu'un abonné demande à accéder à une ressource hébergée sur un site dont l'adresse IP a été associée par un FAI à celui d'une URL fichée par la police, la requête est redirigée par les routeurs du FAI vers la plate¬-forme de filtrage qui bloque la communication si

la ressource correspondante est dans la liste noire, et qui sinon relaie la communication.

Or non seulement ce mode de filtrage, s'il est le plus probable, n'est techniquement pas sans défauts [2], mais surtout ces mesures risquent de transformer l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) en *« opérateur IP à part entière »,* comme l'explique PCInpact.

L'industrie du disque en embuscade ?

On l'a vu : des intérêts économiques sont en jeu. Parmi eux, les intérêts de l'industrie du disque. Alors que le Conseil constitutionnel a fortement restreint les possibilités de filtrage pour « atteinte au droit d'auteur et aux droits voisins » en censurant Hadopi première mouture, Jérôme Roger, porte-parole de la SPPF (Société Civile des Producteurs de Phonogrammes en France), interrogé par Pcinpact, ne s'y trompe pas : « *Le débat nous intéresse de très près car les engagements qui seraient pris concernant les contenus pédophiles peuvent effectivement passer par du filtrage. Ce sont des mesures d'engagements volontaires prises dans un projet de charte.* ». Et il ajoute « *Les problématiques de l'industrie musicale ne sont pas éloignées de ces autres préoccupations 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.* »

En attendant, la publication du « Plan en faveur de la création sur Internet », dit « rapport Zelnik » [3]., comme le sont les propositions de taxer les publicités des services en ligne (et notamment Google) ou d' étendre la « taxe copie privée » aux cartouches d'encre pour financer la numérisation des livres (et parce qu'elles peuvent potentiellement servir à imprimer des livres « piratés ?). PCInpact note à ce propos : *« Le consommateur paie sur le support DVD (pour enregistrer ses photos), paie sur l'imprimante (pour le tirage lesdites photos) et on devra en plus payer pour les cartouches (sur l'encre des dites photos). Après le triple play, le triple pay. »*

A terme, certains rêvent, sans rire, de prendre modèle sur la Chine, à l'instar du député UMP Jacques Myard qui a livré fin décembre le fond de sa pensée sur la radio d'extrême-droite Radio Courtoisie : « *La vérité est que le réseau internet aujourd'hui est totalement pourri. Et quand je dis pourri, c'est que peut-être nous avons tous dans notre réseau internet des chevaux de Troie qui vont se réveiller peut-être dans un an, peut-être dans 18 mois, peut-être demain matin. C'est un réel problème. J'espère que l'on va prendre conscience de la nécessité de nationaliser ce réseau, et d'avoir la capacité de mieux le maîtriser, les Chinois l'ont fait.* » [4] Heureux adepte des nationalisations, mais répressives... sur un réseau mondial.

Jacques Myard n'est d'ailleurs pas le seul à pousser dans le sens d'un contrôle intégral : Bono, chanteur multimillionnaire du groupe irlandais U2, chantre du « charity business » et évadé fiscal, est aussi intéressé par le système chinois. Constatant dans une tribune parue dans le New York Times, qu'*« une décennie de partage de musique et de brigandage en ligne a rendu évident le fait que les gens qui en pâtissent sont les créateurs - en l'occurrence, les jeunes auteurs compositeurs de chansons qui ne peuvent pas vivre de la vente de places de concerts et des ventes de T-shirts - et que ceux qui tirent profit de ce vol des plus pauvres sont les riches fournisseurs d'accès, dont le gonflement des profits est un miroir parfait des pertes dont souffre l'industrie musicale. »* Et de conclure, ce moquant de ces FAI sans scrupules : *« Nous sommes un bureau de poste, nous disent-ils, qui sait ce qu'il y a dans les emballages de papier brun ? Mais nous savons, grâce au noble effort entrepris par les États-Unis pour mettre fin à la pornographie infantile, sans même parler de l'ignoble effort mené par la Chine pour supprimer toute dissidence en ligne, qu'il est parfaitement possible de pister les contenus. »* [5]

L'usurpation d'identité contre la libre critique

Le projet de loi Loppsi réserve quelques autres surprises concernant la liberté d'expression sur le Net. Ainsi de son article 2, qui entend réprimer l'usurpation d'identité sur Internet est formulé en ces termes :

> Le code pénal est ainsi modifié : [...]
> 2° L'article 222-16-1 est ainsi rétabli :
>
> « *Art. 222-16-1.* - Le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique l'identité d'un tiers **ou des données qui lui sont personnelles**, en vue de troubler la tranquillité de cette personne ou d'autrui, est puni d'un an d'emprisonnement et de 15 000 Euros d'amende.
>
> « Est puni de la même peine le fait d'utiliser, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, en vue de porter atteinte à son honneur ou à sa considération. »

Ainsi formulé, cet article, qui aurait pu combler le vide juridique qui entoure l'usurpation d'identité, est porteur d'ambiguïtés potentiellement attentatoires à la liberté d'expression. Non seulement le « trouble à la tranquillité d'autrui », par exemple, n'est pas précisément défini, mais il est associé à des *« actes réitérés »* alors qu'un seul acte peut être pris en compte pour déterminer l'« atteinte à l'honneur ou à la considération ». Or, qu'est-ce qu'un « acte réitéré » ? « *Un billet blog publié en 2007 puis un autre en 2009 seront-ils analysés en un acte réitéré ? »*, s'interroge l'Asic (Association des services Internet communautaires). Et PCInpact de s'interroger : *« les peines d'un an de prison et de 15 000 euros d'amende sont conditionnées à des hypothèses : il s'agit de vouloir "troubler la tranquillité" de l'usurpé ou d'un tiers "de manière réitérée" (donc plusieurs fois), ou de porter atteinte à son honneur voire à sa considération. Remarquons que ces conditions peuvent s'expliquer naturellement puisque à défaut, le seul fait d'utiliser le pseudo d'un tiers, sans le savoir, aurait pu conduire à une sanction quasi automatique. »*

Mais il y a pire, comme le note l'Asic : *« Dans la mesure où ils ne visent pas seulement l'usurpation d'identité mais aussi tout usage de toute donnée personnelle d'autrui d'une manière qui trouble sa tranquillité, les interdictions pourraient s'appliquer au fait de « tagger » quelqu'un sur une photo sur un réseau social sans son accord, au fait de critiquer qui que ce soit sur un blog, au fait de critiquer un artiste, une personnalité, une personne publique sur un forum, ou s'appliquer même à la vidéo de Sarkozy au salon de l'agriculture disant "casse-toi pauv'con" »*, voire au *« fait de poster les coordonnées d'un député sur un site en invitant les citoyens à le contacter pour exprimer leur opposition à un texte de loi (s'il s'en suit un nombre important d'appels pouvant nuire à la tranquillité du député) ! »*, comme cela a été maintes fois fait lors de la bataille contre Hadopi.

En bref, là encore, le texte manque sa cible et risque de se retourner contre les internautes [6].

Fichage en folie

Les mesures qui menacent de porter atteinte à liberté d'expression et aux libertés numériques ne sont pas les seules : le projet de loi Loppsi 2 prévoit d'utiliser les nouvelles technologies pour ficher de manière beaucoup plus étendue la population. En son article 10, après avoir modifié les dispositions relatives à l'alimentation des fichiers de police STIC et JUDEX (« fichiers d'antécédents ») qui pourront désormais conserver des données sur des personnes innocentées ou bénéficiaires d'un non-lieu (et donc sans « antécédents »), le projet de loi crée et réglemente l'usage des « fichiers d'analyse sérielle ». A leur propos, le Syndicat de la magistrature s'insurge :

« Le projet de loi prévoit d'augmenter la taille de ces fichiers dédiés aux infractions "présentant un caractère sériel", en abaissant de 7 à 5 ans le quantum des peines encourues par les personnes mises en cause pour de telles infractions (nouvel article 230-13 du Code pénal). On assiste donc à une nouvelle extension du fichage, dans un pays qui compte déjà 58 fichiers recensés... Tout se passe comme si les limites du fichage de la population étaient sans cesse repoussées, au nom d'une efficacité toujours postulée, rarement étayée. Ici, il s'agit d'inclure dans ces fichiers de rapprochement les personnes susceptibles d'être impliquées dans des affaires de plus petite délinquance. Aujourd'hui, c'est 5 ans, demain ce sera 3, jusqu'où ? Manifestement, le fichage généralisé est en marche. S'agissant du contrôle de ces fichiers, le nouvel article 230-15 renvoie aux dispositions très contestables concernant les fichiers d'antécédents. »

Ce fichage devrait concerner également des témoins et victimes. Ce super-fichier peut paraître assez anodin à la lecture du projet de loi et ne pas modifier grand-chose par rapport à ce qui existe déjà. Pourtant, il constitue un bond en avant en la matière, comme l'explique PCInpact [7] : *« Il s'agit d'un système de traitement des données ouvertes (informations disponibles sur internet, Facebook, Twitter, etc.) ou fermées (IP, numéro de téléphone, données détenues par les FAI) qui pourront être exploitées dans le cadre de certaines infractions. C'est là une capacité énorme de rapprochement et de traitement de la sérialité qui est en phase d'installation. Une infraction a lieu près d'une banque et voilà la police autorisée à analyser la liste de tous les mobiles qui ont passé un appel à partir d'une borne située à proximité, les références GPS des voitures en circulation dans les alentours, les numéros de CB utilisés pour payer ou retirer de l'argent, le tout croisé avec tous les fichiers possibles comme ceux détenus par les autres administrations et tous les opérateurs privés, ou sur les réseaux internet. On veut aller très vite et ratisser très large. »* [8]

Les pirates de la police

Enfin, le projet de loi Loppsi 2 prévoit que la police pourrait, sous contrôle du juge d'instruction (par ailleurs appelé à disparaître), installer à l'insu de leur propriétaire des mouchards capables de lire tous les caractères saisis au clavier et tout ce qui apparaît à l'écran, et cela pendant une durée de huit mois, sur les ordinateurs de citoyens suspects de participer à des crimes en bande organisée ou à la préparation et la réalisation d'actes terroristes, et ce y compris en dehors des heures légales au cours desquelles une perquisition peut être menée, comme l'indique l'article 23 (qui dépend du chapitre « Protection des intérêts fondamentaux de la nation ») du projet de loi dont voici des extraits :

« *Art. 706-102-1.* - Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction.

« *Art. 706-102-2.* - À peine de nullité, les décisions du juge d'instruction prises en application de l'article 706-102-1 précisent l'infraction qui motive le recours à ces mesures, la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données ainsi que la durée des opérations.

« *Art. 706-102-3*. - Les décisions sont prises pour une durée maximale de quatre mois. Si les nécessités de l'instruction l'exigent, l'opération de captation des données informatiques peut, à titre exceptionnel et dans les mêmes conditions de forme, faire l'objet d'une prolongation supplémentaire de quatre mois.

« Le juge d'instruction peut, à tout moment, ordonner l'interruption de l'opération.

« *Art. 706-102-4*. - Les opérations prévues à la présente section ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du juge d'instruction.

« Le fait que ces opérations révèlent des infractions autres que celles visées dans ces décisions ne constitue pas une cause de nullité des procédures incidentes.

« *Art. 706-102-5.* - En vue de mettre en place le dispositif technique mentionné à l'article 706-102-1, le juge d'instruction peut autoriser l'introduction dans un véhicule ou dans un lieu privé, y compris hors des heures prévues à l'article 59, à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur celui-ci. S'il s'agit d'un lieu d'habitation et que l'opération doit intervenir hors des heures prévues à l'article 59, cette autorisation est délivrée par le juge des libertés et de la détention saisi à cette fin par le juge d'instruction. Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous l'autorité et le contrôle du juge d'instruction. Les dispositions du présent alinéa sont également applicables aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place.

« En vue de mettre en place le dispositif technique mentionné à l'article 706-102-1, le juge d'instruction peut également autoriser la transmission par un réseau de communications électroniques de ce dispositif. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction. Les dispositions du présent alinéa sont également applicables aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place. »

Seuls les ordinateurs des médecins, juges et avocats sont exclus du dispositif.

Amère ironie : au moment ou la lutte contre le « piratage » de la musique, des films et bientôt des livres sur Internet semble être une priorité, la police et la justice pourraient être habilitées à « pirater » des ordinateurs et réseaux appartenant à des particuliers, des organisations ou des entreprises et ce sans leur accord. En effet, l'installation de ces « mouchards », que ce soit par le biais de logiciels espions (assimilables à des virus) ou de puces branchées directement sur la carte mère des machines concernées, ne saurait être qualifiée autrement que de techniques de « piratage », au sens le plus commun donné à ce mot, et ce même s'ils ne permettent que des captures d'écran et pas l'accès à des données non lues sur la machine concernée.

Ceci est d'autant plus inquiétant qu'à chaque fois que des mesures exceptionnelles ont été prises sous couvert de lutte contre les crimes les plus graves, elles ont ensuite été étendues à la lutte contre des crimes et délits beaucoup plus commun, voire à de simples suspects de ces crimes et délits, à l'image du fichage génétique, destiné au départ aux délinquants sexuels, mais qui à force d'extension à toutes sortes de catégories touche aujourd'hui 2 % de la population française. Les notions mêmes de bande organisée (*« tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions »* selon l'article 132-71 du code pénal) et de terrorisme (*« une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur »* selon l'article 421-1 du même code) étant définies en droit français de manière suffisamment floue pour que ces concepts puissent être le cas échéant étendus à beaucoup de monde, les citoyens soucieux de la défense des libertés individuelles devraient avoir du souci à se faire.

Fourre-tout, le projet de loi Loppsi n'en est pas moins dangereux. Il confirme le rapport paranoïaque qu'entretient le gouvernement de Nicolas Sarkozy aux nouvelles technologies de l'information et de la communication dont il est incapable de comprendre les enjeux, et qui sont vues tantôt comme un danger qu'il faut circonscrire, tantôt d'un point de vue purement utilitaire comme suppléantes au politiques sécuritaires du gouvernement.

Or, cette position est pour le moins paradoxale, les mesures de contrôle du Net et de répression des internautes « tous coupables » (filtrage, surveillance passive) risquent de généraliser l'usage par tout un chacun des technologies de contournement et de cryptage, rendant particulièrement difficile le travail de la police dans sa lutte contre la cybercriminalité, qu'on prétend pourtant renforcer (et créant du même coup de nouveaux marchés, comme le suggère un article récent de ReadWriteWeb à propos d'Hadopi).

Mais laissons le mot de la fin au Syndicat de la magistrature :

« [...] l'exposé des motifs du projet de loi "d'orientation et de programmation pour la performance de la sécurité intérieure", en dressant la liste exhaustive des prétendues "menaces" intérieures et extérieures, révèle une conception de la société à la limite de la paranoïa. Il en résulte un aggloméré de mesures sans liens particuliers entre elles, visant tantôt à créer de nouvelles incriminations ou à aggraver les anciennes, tantôt à permettre à l'Etat d'instituer un régime d'impunité pour ses agents de renseignements ou de mieux avoir à l'oeil des populations ciblées. Comme si le contenu de ces dispositions alarmantes n'était pas suffisant, le projet de loi est rédigé (sciemment ?) de manière si complexe et si obscure qu'il sera inintelligible pour le justiciable et les professionnels en charge de le mettre en application. »

Marie-Anne Boutoleau

---

[1] Selon le site Read Write Web, ce taux atteindrait même les deux tiers : *« A moins qu'il ne s'agisse d'une erreur, mais avec un taux d'erreur de*

68%, on peut légitimement se demander si toute cette histoire de censure est une bonne idée. Une chose est certaine : ce ne sont pas les pédophiles qui sont visés, bien au contraire, ils seront grâce à cette loi, qui les obligera à adopter des usages plus sécurisés de l'internet (VPN, cryptage, etc), bien plus à l'abri des forces de police qu'ils ne l'ont jamais été. »

[2] Dans son étude d'impact, le ministère lui-même reconnaît les risques de « surblocage » liés à l'utilisation des techniques de filtrages par IP, DNS ou hybrides (le blocage par proxy étant trop coûteux pour être sérieusement envisagé), c'est à dire le risque que des sites légaux mais partageant le même serveur et donc la même IP et/ou le même nom de domaine qu'un site interdit soient pénalisés, mais aussi le risque que les serveurs en question soient saturés. D'autre part, le protocole BGP qui est utilisé pour rediriger les routes en vue de filtrer des contenus n'a pas été conçu pour cela et son utilisation dans ce but peut rendre perméable à des attaques susceptibles de perturber tout le réseau et mettre en jeu la sécurité nationale, comme l'explique dans sa note La Quadrature du Net.

[3] Du nom de son rapporteur, Patrick Zelnik, fondateur de Virgin France et du label Naïve (qui a édité Carla Bruni, femme de l'actuel président de la République, n'y voyons aucun rapport...) et ex-président du Syndicat national de l'édition phonographique (SNEP)à , syndicat patronal affilié au Medef qui, comme le relève PcInpact, défend aujourd'hui le filtrage d'Internet , de l'Union des producteurs phonographiques français indépendants (UPFI) de 2000 à 2004 et actuel président d'Impala, (syndicat européen des sociétés phonographiques indépendantes) depuis juillet 2006. Voir son CV complet sur Wikipédia], devrait le combler d'aise : ce projet ne propose la création d'une carte « Musique en ligne » qui serait remise aux *« jeunes internautes »* pour l'achat de musique en ligne, en guise d'offre légale. Autrement dit, de faire subventionner les majors par les consommateurs et le contribuable.

Dans sa note de synthèse sur ce rapport, PCInpact précise : *« Concrètement, on préconise l'instauration d'une carte d'une valeur faciale (par exemple) de 50 euros à dépenser sur les plateformes légales et payantes. 20 à 25 euros seraient payés par l'internaute (jeune), 20 euros par l'État, et 5 à 10 euros par les professionnels. Cette carte serait utilisable sur tous les sites participants à l'opération. »* Une mesure vivement critiquée[[À titre d'exemple, le NouvelObs.com liste les critiques adressées à ce rapport en France, tandis que lefigaro.fr souligne à juste titre que « L'idée d'une "taxe Google" suscite l'ironie à l'étranger ».

[4] Propos rapportés par PCINpact.

[5] *A decade's worth of music file-sharing and swiping has made clear that the people it hurts are the creators â€" in this case, the young, fledgling songwriters who can't live off ticket and T-shirt sales like the least sympathetic among us â€" and the people this reverse Robin Hooding benefits are rich service providers, whose swollen profits perfectly mirror the lost receipts of the music business. We're the post office, they tell us ; who knows what's in the brown-paper packages ? But we know from America's noble effort to stop child pornography, not to mention China's ignoble effort to suppress online dissent, that it's perfectly possible to track content. »*

[6] Pour un historique de cette article du projet de loi, consulter les articles que PCInpact avait précédemment consacrés au sujet, ici, ici, et là.

[7] Voir aussi le blog de Georges Moréas pour un historique et une explication détaillée.

[8] Comme le note par ailleurs PCInpact, ce système, qui devrait s'appeler Périclès, tombe à point nommé. En effet, la Direction générale de l'armement devrait se doter d'une technologie similaire (toutefois limitée à des données ouvertes). Et l'Union européenne finance Indect, un programme de recherche sur la *« détection automatique de menaces, de comportements anormaux ou de violence »* qui vise entre autres la *« surveillance continue et automatique »* non seulement d'Internet, mais aussi des *« systèmes informatiques individuels »*. Lire à ce propos l'article rédigé par l'auteure du présent article sur le blog « Le pot de colle ».