document publié sur http://blog.rom1v.com/2009/06/attention-loppsi/
— *16 juillet 2009* —

Les articles de la loi LOPPSI[1] qui concernent la lutte contre la cybercriminalité (CHAPITRE II) et le renforcement de la lutte contre la criminalité et l'efficacité des moyens de répression (CHAPITRE V), c'est-à-dire l'article 2, l'article 3 et l'article 4 d'une part, et l'article 23 d'autre part, me paraissent très inquiétants vis-à-vis de la démocratie, de la liberté d'expression et de l'égalité devant la loi.

1 Sur l'article 2

D'après l'énoncé des motifs, l'article 2 *« crée l'incrimination d'utilisation frauduleuse de données à caractère personnel de tiers sur un réseau de télécommunication »*.

Il instaure une peine d'un an d'emprisonnement et de 15 000 € d'amende *« 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 troubler la tranquillité de cette personne ou d'autrui »* (si ces données ont été utilisés de manière réitérée) ou *« en vue de porter atteinte à son honneur ou à sa considération »* (sans que ces données n'aient besoin d'être utilisées de manière réitérée).

L'utilisation de données personnelles *« en vue de troubler la tranquillité d'une personne »*, comme le fait remarquer l'ASIC[2], permet une interprétation très large. Ainsi, cet article pourrait s'appliquer dans les cas suivants :

- le fait de « tagger »quelqu'un sur une photo sur un réseau social sans son accord ;
- le fait de critiquer qui que ce soit sur un blog (beaucoup de personnes perdent leur tranquillité dès qu'ils lisent des propos non-élogieux) ;
- le fait de critiquer un artiste, une personnalité, une personne publique sur un forum ;
- la vidéo de Sarkozy au salon de l'agriculture disant « casse-toi pauv'con » ;
- le fait de poster les coordonnées d'un député sur un site en invitant les citoyens à le contacter pour exprimer une opposition à un texte de loi (s'il s'en suit un nombre important d'appels pouvant nuire à la tranquillité d'un député)...

Le flou juridique ainsi instauré met en danger la liberté d'expression, et ne se cantonne pas à punir l'usurpation d'identité sur Internet... dont les peines existent d'ailleurs déjà, comme le conclut l'association : *« On notera, au surplus, que les abus dans l'usage de données personnelles sont déjà punis par la loi Informatique et Liberté de 1978, de sorte que la rédaction proposée n'apporte pas de réelle évolution, si ce n'est une insécurité juridique due à son imprécision. »*.

2 Sur l'article 3

L'article 3 propose d'aggraver les peines des délits si ceux-ci ont été commis par la communication au public en ligne : ces peines s'aligneront sur celles des délits commis en bande organisée.

Je rejoins également l'avis de l'ASIC sur ce point, qui conclut ainsi : *« Il n'existe pas de raison objective de punir plus sévèrement une activité contrefaisante exercée via un service de communication au public en ligne, par rapport à la même activité exercée par le biais d'un support hors ligne (ex : mailing, catalogues, affichage public, téléphone, etc.). Il s'agit d'une violation du principe d'égalité. »*.

3 Sur l'article 4

D'après l'énoncé des motifs, l'article 4 *« protège les internautes contre les images de pornographie enfantine »*.

La lutte contre les actes de pédophilie est extrêmement importante : il faut trouver et punir les personnes qui font subir de tels agressions à des enfants. Le sujet pourrait provoquer des débats passionnés à propos de la position du curseur entre liberté et sécurité (quelles libertés pourraient être sacrifiées pour trouver ces criminels)...

Cependant, ici, ce n'est pas de cela dont il s'agit. Il s'agit de *« protéger les internautes contre les images de pornographie enfantine »* : cette loi veut combattre l'*immense danger* que courent les internautes à tomber malencontreusement sur des images de pornographie enfantine sans le vouloir.

Trois objectifs sont en fait annoncés, j'y reviendrai après avoir mis au clair certains points.

3.1 Contenus toujours accessibles

Pour bien cerner l'objectif du texte de loi, il faut préciser que les mesures de filtrage préconisées ne bloqueront pas les criminels qui veulent accéder à ces contenus.

En effet, il est très simple d'accéder de manière anonyme et chiffrée à un contenu (qui par définition passe au travers de toutes les surveillances et les filtrages), par exemple en mettant en place très simplement un proxy *tor*[3].

[1] http://www.assemblee-nationale.fr/13/pdf/projets/pl1697.pdf
[2] http://static.pcinpact.com/pdf/ASIC-note-loppsi-15062009.pdf
[3] Mise en place de *tor* sous Ubuntu : http://doc.ubuntu-fr.org/tor

Les criminels ne seront donc aucunement gênés par ce filtrage, et ceux qui accédaient à ces contenus « en clair »et qui basculeront « en chiffré »seront mieux protégés.

De toute façon, le texte est clair là-dessus, il ne s'agit aucunement d'empêcher les criminels d'accéder à ces contenus (tout au plus complexifier l'accès), le but est d'éviter que les internautes tombent sur ces contenus « par hasard ».

Je pense que ce rappel est important.

3.2 Mesures inquiétantes

3.2.1 Contre la neutralité du réseau

La neutralité du réseau est un principe qui, pour résumer, dit que lorsqu'une information est véhiculée sur Internet, aucune discrimination n'est appliquée en fonction de l'émetteur, du destinataire, ou de la nature de cette information. Ce principe est intimement lié à celui du secret de la correspondance privée. C'est cette neutralité du réseau qui est à la base d'Internet et a permis sa croissance rapide, mettant à égalité tous les acteurs, quelle que soit leur taille, leurs choix techniques, ou leur rôle.

Ce principe joue, dans le monde du numérique, un rôle similaire à celui de la séparation des pouvoirs. Ce n'est pas une liberté en soi, c'est la garantie de toutes les autres.

À ce propos, le texte dit que « cette obligation ne heurte pas le principe de la neutralité de ces opérateurs par rapport aux contenus puisque l'identification des contenus illicites est à la charge des services de police »(page 109). Cela ne change rien au problème, cet argument est fallacieux : que ce soit tel ou tel service qui soit chargé de l'identification des contenus à filtrer, la neutralité est atteinte...

Le filtrage, par définition, va à l'encontre de la neutralité du réseau.

3.2.2 Inefficacité et risques de sur-blocage

Les mesures de filtrage sont, quasiment par définition, inefficaces, comme l'explique Christophe Esperm dans une note intitulée « Principe, intérêts, limites et risques du filtrage hybride à des fins de blocage de ressources pédopornographiques hébergées sur des serveurs étrangers »[4].

Plus grave, elles provoquent des risques de sur-blocage (blocage de sites qui ne devraient pas l'être), liées aux techniques de filtrage.

3.2.3 Dérives inévitables

À ces problèmes techniques de sur-blocage viennent s'ajouter les dérives vers une censure non contrôlée d'Internet. En effet, la liste des sites filtrés ne sera pas rendue publique, laissant libre cours à l'ajout de sites qui n'ont rien à y faire, comme des sites pornographiques légaux, des sites anti-censure, des sites de jeux-vidéos déconseillés aux moins de 15 ans[5], des sites de paris en ligne[6], des sites permettant l'accès à des contenus protégés par le droit d'auteur, des sites politiques, des sites « susceptibles »de troubler l'ordre publique ou « la tranquillité du pouvoir en place »...

Comme l'indique l'étude d'impact, des mesures similaires ont déjà été mises en place dans d'autres pays, et justement ces dérives y ont été observées. Par exemple, en Australie, la liste noire secrète ne contenait que 32% de sites effectivement pédopornographiques[7], ou en Thaïlande, où des sites bloqués portaient la mention *« lese majeste »*[8] (portant atteinte à la famille Royale). Comme le précise *Wikileaks* : « HISTORY SHOWS THAT SECRET CENSORSHIP SYSTEMS, WHATEVER THEIR ORIGINAL INTENT, ARE INVARIABLY CORRUPTED INTO ANTI-DEMOCRATIC BEHAVIOR. »[9].

Les mêmes prétextes sont d'ailleurs souvent utilisés pour mettre en place une surveillance et un contrôle de l'information par la censure dans tous les pays, par exemple en Chine, qui a déjà le filtrage de cœur de réseau, et qui veut rajouter, sous prétexte de lutter contre la pornographique qui pourrait choquer les plus jeunes, des mouchards filtrants obligatoires sur tous les ordinateurs vendus, comme le relate PCInpact[10].

3.3 Danger inexistant

Le danger de tomber par hasard sur une image pédopornographique est inexistant : en 10 ou 15 ans d'utilisation d'Internet, quasiment personne n'est jamais tombé malencontreusement sur un tel contenu. Pourtant, l'étude d'impact affirme le contraire. Pourquoi ?

L'étude d'impact du projet de loi présente *« le succès des mesures prises »* (page 107) dans différents pays (Norvège, Suède et Danemark), en se basant sur le nombre de connexions effectivement filtrées.

Il y aurait, dans ces pays, entre 12000 et 30000 connexions filtrées par jour. Pourquoi pas. Mais il serait faux d'interpréter ceci comme « un succès contre la pédopornographie », pour deux raisons.

[4] http://www.laquadrature.net/files/note-quadrature-filtrage-hybride.pdf
[5] http://www.numerama.com/magazine/13291-L-Australie-veut-etendre-sa-censure-facon-Loppsi-aux-jeux-video.html
[6] http://www.numerama.com/magazine/12774-Filtrage-les-sites-de-paris-en-ligne-bientot-bloques-par-les-FAI.html
[7] http://wikileaks.org/wiki/Australian_government_admits_a_mere_32%25_of_secret_censorship_list_is_related_to_underage_images
[8] http://wikileaks.org/wiki/797_domains_on_Finnish_Internet_censorship_list%2C_including_censorship_critic%2C_2008
[9] L'histoire montre que les systèmes secrets de censure, quelque soient les intentions originales, mènent toujours à des dérives anti-démocratiques.
[10] http://www.pcinpact.com/actu/news/51252-logiciel-integrer-machines-bloquer-sites.htm

Tout d'abord, comme nous l'avons vu, les *listes noires* contiennent une majorité de sites qui ne devraient pas s'y trouver, et qui n'ont aucune raison d'être bloqués. Il paraît très probable que l'immense majorité des tentatives de connexions (initiées par des humains) filtrées étaient en direction de ces sites légitimes (sites dénonçant la censure ou présentant des opinions divergentes avec le pouvoir en place par exemple).

Ensuite, une connexion n'est pas forcément humaine, énormément de connexions sont automatiques, effectuées par des bots (légitimes comme ceux des moteurs de recherches, ou moins comme ceux recherchant des cibles à spammer). Je vais vous donner un exemple avec les connexions sur mon blog personnel[11].

J'ai mis en place un outil de statistiques[12] utilisant *JavaScript* (les bots n'exécutent jamais le *JavaScript*) pour analyser le trafic, et entre le 14 et le 21 juin, il y a eu 1926 visites, et **3443 pages vues** (un visiteur peut visiter plusieurs pages). Maintenant, comparons avec le nombres de connexions reçues par le serveur web, pour les mêmes dates : 51126. Il y a eu un peu plus de 50000 « connexions »à mon blog entre le 14 et le 21 juin, soit 7300 par jour. Si l'on retire les 3500 pages vues, et même en prenant une marge d'erreur, ça fait dans tous les cas **plus de 6000 connexions par jour effectuées sans intervention humaine**, pour mon seul blog... Alors, certes, les blogs (et forums de discussion) subissent plus de *scans* de la part des bots que d'autres sites car ils sont la cible de spams. Mais avec une liste de 5000 noms de domaine sur la liste noire, en ne comptant que les bots provenant du pays en question, il n'est pas étonnant d'avoir autant de connexions filtrées, même si personne n'a jamais voulu accéder à un seul de ces sites.

Le nombre de connexions filtrées n'apporte aucune information sur le nombre de connexions humaines ni sur le succès des mesures prises.

3.4 Objectifs annoncés

Les 3 objectifs de l'article 4 sont énoncés page 104.

a) prévenir l'accès involontaire aux sites pédopornographiques

Bien que le danger soit inexistant, pour combler la soif d'illusion de sécurité de certains, **on peut atteindre cet objectif en déportant le filtrage au niveau logiciel, typiquement de contrôle parental** (alimenté par la liste noire du ministère de l'intérieur), plutôt qu'en mettant en place des mesures de filtrage et de censure au niveau des routeurs de cœur de réseau. Ce logiciel serait sous contrôle de l'utilisateur, et garantirait de ne pas tomber sur les sites en liste noire par accident. Cette solution a l'avantage de respecter la neutralité du net et d'éviter le sur-blocage et les dérives anti-démocratiques.

D'ailleurs, des outils qui bloquent des sites présents dans une liste noire, beaucoup d'internautes en utilisent, par exemple le plug-in Adblock Plus[13] (gratuit et open-source) pour *Firefox*, qui bloque une majorité des publicités indésirables sur les pages visitées.

b) complexifier l'accès volontaire de certains internautes à des sites pédopornographiques

Les gens ne sont pas idiots, utiliser un proxy est à la portée de quiconque sait lire, ça ne va pas décourager des criminels.

c) réduire les bénéfices illicites des organisations criminelles

Cet argument est intéressant, et aurait mérité une étude sérieuse afin de savoir dans quelle mesure un tel filtrage pourrait réduire ces bénéfices. Mais vu que ces bénéfices proviennent (j'imagine) des criminels qui accèdent à ces contenus volontairement, je pense que le filtrage ne peut pas y changer grand chose.

3.5 Conclusion sur l'article 4

La pédopornographie sert ici de prétexte au filtrage du net (qui ne résout rien au problème de la pédophilie). M. Copé l'a d'ailleurs déclaré sur RTL, *Hadopi* n'était que le *« point de départ »*. *« Car il y aura un sujet plus large qui est la régulation sur Internet »*.

Certaines personnes à l'origine de ces textes (*Hadopi* et *Loppsi*) déclarent qu'*« Internet ne doit pas être une zone de non-droit »*. Et effectivement, le droit s'applique sur Internet. Mais ces projets de lois tentent justement d'en faire une zone de non-droit : comme l'a rappelé le Conseil Constitutionnel, la loi Hadopi bafouait — excusez du peu — la présomption d'innocence, les droits de la défense, la séparation des pouvoirs, la liberté d'expression et le respect de la vie privée. Certaines dispositions de la loi *Loppsi* mettent en place les dispositifs techniques permettant la censure et mettant en danger la démocratie et la liberté d'expression.

Si l'objectif réel était de lutter contre la pédopornographie, il faudrait mettre plus de moyens pour remonter aux sources et faire arrêter les criminels.

Si l'objectif était de ne plus permettre l'accès à de tels sites, il faudrait les faire retirer des serveurs (beaucoup plus efficace que le filtrage, et sans risque de sur-blocage). À titre d'exemple, en partant d'une liste de sites bloqués révélée par *Wikileaks*, Alvar Freude, un internaute allemand, a réalisé un script qui envoie automatiquement une demande de

[11] http://blog.rom1v.com
[12] **Piwik**, accessible sur http://blog.rom1v.com/stats
[13] https://addons.mozilla.org/fr/firefox/addon/1865

retrait de contenus aux hébergeurs des sites bloqués. Sur 348 hébergeurs contactés, 250 ont répondu, et **61 ont retiré le contenu illicite en moins de 12 heures**.[14]

Et si, vraiment, le choix final était d'empêcher l'accès aux sites (choix qui paraît assez peu judicieux), il serait possible d'atteindre cet objectif par d'autres moyens (logiciel de contrôle parental par exemple) qui préservent les libertés fondamentales et évitent la censure et les dérives anti-démocratiques.

4 Sur l'article 23

4.1 Captation des données informatiques

L'article 23 autorise l'installation de chevaux de troie[15] à distance par la police sur les ordinateurs d'internautes (à leur insu), avec l'autorisation d'un juge.

Des problèmes restent pour l'instant sans réponse.

Le premier concerne les anti-virus et autres logiciels de protection : devront-ils volontairement laisser passer ces acte de piratages effectués par la police ? Un accord avec les éditeurs de ces logiciels est-il prévu ?

Le second concerne la baisse de sécurité du poste informatique de l'internaute incriminé : les chevaux de troie ainsi installés, laissant ouverte une porte dérobée, pourraient être utilisés par des pirates (d'autant plus si les anti-virus ferment les yeux) pour écouter tout ce que fait l'utilisateur (récupération des données personnelles, écoute des touches tapées pour récupérer mots de passes et codes de carte bancaire, prise de contrôle de l'ordinateur à distance...).

4.2 Interdiction des dispositifs techniques

L'article 23 ajoute également les mots *« ou de dispositifs techniques »* à l'article 226-3 du code pénal.

Comme le fait remarquer ecrans.fr[16], le texte vise ainsi à punir l'utilisation de logiciels permettant *« d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »*, que ça soit *« la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente »* de ces *« dispositifs techniques »*.

En tant qu'ingénieur en développement informatique, ces logiciels me sont très utiles ; ils le sont encore plus pour les ingénieurs réseau, qui utilisent ces outils quotidiennement (ou presque).

D'après cette loi, tous les outils fournis par la distribution BackTrack[17] (et disponibles dans le gestionnaire de paquets des autres distributions) seront donc illégaux ? Les écoles et les entreprises spécialisées en informatique risquent d'apprécier... Les développeurs de ces outils indispensables aussi...

[14] http://www.numerama.com/magazine/13167-Le-filtrage-du-net-facon-Loppsi-fait-polemique-en-Allemagne-MAJ.html
[15] http://fr.wikipedia.org/wiki/Cheval_de_Troie_(informatique)
[16] http://ecrans.fr/Loppsi-Diminuer-la-securite-pour,7379.html
[17] http://www.remote-exploit.org/backtrack.html