

1 Introduction

L'orientation politique sécuritaire qui se met en place depuis plusieurs années (et pas seulement en France) n'aura probablement échappé à personne. Cependant, si les medias, les partis politiques, les syndicats, ... discutent, analysent, dénoncent beaucoup les mesures qui concernent la « vie réelle » (par exemple, les sans-papiers, la répression policière, plus largement la politique économique, sociale, ...), on parle finalement assez peu de ce qui concerne les technologies. On évoque parfois « Big Brother », généralement sur des mesures considérées de façon isolée, sans détailler, surtout que l'on tombe rapidement dans des considérations techniques ou juridiques. Depuis quelques mois, les mesures et projets semblent se multiplier, de façon de plus en plus précipitée (peut être n'est-ce qu'une impression personnelle), ce qui m'a poussé à essayer d'établir une liste la plus complète possible, histoire d'avoir une vue globale (et non pas chaque projet pour soi), de voir où on va. Le résultat étant plutôt impressionnant (mais prévisible), j'ai pensé qu'il serait intéressant de le partager.

2 Les lois.

2.1 Ce qui est déjà passé.

La loi DADVSI (« Droit d'auteur et droits voisins dans la société de l'Information ». [Texte](#)) a été publiée dans le Journal Officiel le 3 août 2006. C'est la transposition de l'EUCD (European Union copyright directive). Comme c'est un texte relativement complexe et déjà énormément analysé, je ne mets donc que deux liens qui résument très bien la situation : [oppositions](#) et [conséquences](#) ; ainsi qu'un sur les [DRM](#), qui sont liés à la Dadvsi.

Entre 2005 et 2007, la Commission d'Albi ([texte](#)) actualise les redevances payées sur les supports de stockage pour rétribuer les auteurs d'œuvres d'art musicales et audio-visuelles (supposées compenser les pertes dues à la copie privée). Celles-ci s'appliquent à des supports tels les clés USB, les cartes mémoires, les disques durs externes. Le principe de ces redevances est plutôt curieux : vous achetez une clé USB pour sauvegarder vos travaux, une carte mémoire pour votre appareil photos... qu'importe, vous êtes présumés coupables et vous acquitterez donc d'une taxe que les majors et quelques artistes ringards que vous n'écoutez jamais se partageront. D'une part, un véritable hold-up légalisé, d'autre part une double peine : on est taxé pour compenser une copie qui est d'un autre côté limitée par les DRM et surtout passible de poursuites (loi Dadvsi).

Le passeport biométrique a été mis en place le 30 avril 2008 ([texte](#)), [malgré l'avis de la CNIL](#) qui s'inquiète de la création d'une base de données contenant les photos et empreintes de tous les citoyens.

2.2 Ce qui concerne l'actualité.

Le vote électronique nous est de plus en plus souvent imposé. Or ce vote ne peut être contrôlé par le citoyen de base. L'anonymat du vote pourrait être cassé, les résultats modifiés (par l'organisateur du vote, ou par un pirate) à son insu et on est dépendant des fabricants d'ordinateurs de vote. Avec le vote électronique, la seule chose dont on est vraiment sûr, c'est de ne rien pouvoir contrôler.

Mardi 10 juin, Mme Alliot-Marie annonce un projet qui imposerait aux FAI (Fournisseurs d'Accès à Internet) de bloquer les sites pédophiles étrangers (mais aussi d'escroquerie, d'apologie au terrorisme et d'incitation à la haine raciale), une plate-forme de dénonciations servirait de base pour établir une blacklist. A priori, une très bonne intention. . . et très dur à critiquer sans se faire taxer de pédophilie. On institue donc le filtrage du net sous couvert d'émotion. ([Retranscription de l'allocution du 10 juin](#))

La loi Hadopi (ou la « riposte graduée ») fait suite à la loi Dadvsi, elle est inspirée du [rapport Oliviennes](#) (fin 2007) ; elle a été présentée au conseil des ministres le 18 juin 2008. Elle vise à lutter contre le téléchargement illégal avec un système de riposte graduée : de l'avertissement à la suspension de l'abonnement à Internet pendant un an (suspension de l'abonnement, mais pas du paiement) pour l'internaute qui télécharge (ou sécurise mal son wifi. . .), le tout basé sur une surveillance des adresses IP. Cette loi est critiquée notamment par le [Parlement européen](#), la [CNIL](#), l'[Arcep](#) et l'[ASIC](#). Elle est de plus inefficace : des chercheurs ont par exemple réussi à faire accuser [des imprimantes](#) ! ([Dix bonnes raisons](#) de refuser cette loi).

Le fichier Edvige est apparu avec la fusion des RG et de la DST. D'après le décret portant sur sa création, il concerne les « personnes physiques âgées de treize ans et plus », c'est ce point qui fait le plus scandale, dans l'actualité. Ce n'est pourtant probablement pas le plus grave :

([source](#))

1. De centraliser et d'analyser les informations relatives aux personnes physiques ou morales ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif,

sous condition que ces informations soient nécessaires au Gouvernement ou à ses représentants pour l'exercice de leurs responsabilités ; 2. De centraliser et d'analyser les informations relatives aux individus, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, sont susceptibles de porter atteinte à l'ordre public ;

En gros, on fiche non seulement tous les présumés délinquants, mais aussi n'importe qui s'impliquant dans la vie publique. Les informations sont conservées cinq ans, largement le temps de voir un régime politique basculer.

Le projet LOPSI (loi d'orientation et de programmation pour la performance de la sécurité intérieure) fait partie de l'actualité. Il mettrait en place le fichier informatique "Périclès", qui contiendrait des données telles que les numéros de cartes grises, de puces de téléphone portable (IMEI), des factures... ce qui est plutôt inquiétant pour les libertés individuelles (sans compter que quand on sait [ce que l'État contrôle ses sbires](#)...). De plus, ce projet de loi autoriserait les policiers à mettre en place des trojans (logiciels espions) dans les ordinateurs de citoyens particuliers (enfin, cela dit, je serais membre du resf ou d'un quelconque syndicat, j'aurais tendance à me méfier de mon ordinateur, avant même cette loi...).

([source](#))

La loi devrait permettre, à l'avenir, d'introduire dans les ordinateurs des citoyens un "cheval de Troie" informatique. Il sera possible, avec l'aval d'un juge, "sans le consentement des intéressés, d'accéder à des données informatiques, de les observer, les collecter, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent pour l'utilisateur ou telles qu'il les y introduit par saisie de caractère", et ce pendant une durée de quatre mois, renouvelable une fois. Le dispositif technique pourra être mis en place à toute heure, en s'introduisant dans tout lieu, ou via "la transmission par un réseau de communications électroniques".

D'après [cet article](#) du NY-Times, l'UE semble prête à donner des infos privées aux États-Unis.

Les amendements au « paquet telecoms ». Le « [Paquet Telecoms](#) » est un ensemble de textes européens, de 2003, qui visent *grosso modo* à favoriser la concurrence, et protéger les consommateurs européens, dans le domaine des télécoms. La Commission Européenne a décidé en 2007-2008 de les actualiser. Or certains députés tentent de faire passer des amendements, dont l'objectif serait d'imposer aux internautes des filtres et des trojans qui pourraient

interdire des activités légales, ainsi que l'utilisation de logiciels libres. Il permettraient également de forcer les FAI de collaborer avec les polices privées des producteurs de contenus, ce qui revient à éjecter l'autorité judiciaire de l'histoire.

3 Notre responsabilité personnelle.

Toutes les dérives ne passent pas par des lois. À chacun de se mettre face à ses responsabilités... Quelques exemples :

Le [téléphone portable](#) qui permet de vous localiser.

[Facebook](#), ou le fichage volontaire... (sans compter [l'irresponsabilité d'un nombre important d'users](#)).

RFID, ou la radio-identification : il s'agit d'étiquettes (collées ou incorporées à un objet, voire un humain) qui peuvent être lues à distance (distance variable selon les fréquences). Elles sont actuellement utilisées sur des marchandises, des animaux de companies, des badges, dans les bibliothèques... Une technologie est neutre, [c'est l'utilisation que l'on en fait qui peut être dangereuse](#).

4 Ce que l'on peut faire

Pour le Paquet Telecom, il est non seulement encore possible mais surtout [urgent d'agir](#), avant le 7 juillet.

Se renseigner... Deux bons sites : [La Quadrature du Net](#) et [Ordinateur-de-vote](#).

Le wifi est de plus en plus répandu, et beaucoup de gens sécurisent mal (voire pas du tout) leur réseau : [une clé wep se force facilement](#). Les lois récentes tendent à viser le propriétaires de la ligne (qui n'est donc pas forcément celui qui l'utilise de façon illégale), donc dans le mesure du possible, désactiver le wifi, ou au pire activer [le wpa](#).

Utiliser des logiciels libres, les diffuser, les défendre : [Firefox](#), [Thunderbird](#), [OpenOffice.org](#)... voire tout un système pour les plus motivés (Gnu/Linux, BSD... à noter que certaines distributions Gnu/Linux sont maintenant pensées précisément pour ceux qui n'y connaissent rien : [Ubuntu](#), [Mandriva](#)...

). Quelques liens : une [définition du logiciel libre](#), [Framasoft](#), avec en particulier un annuaire des logiciels libres et l'[APRIL](#), une association pour la promotion et la défense du logiciel libre.

La plupart du filtrage du Web est techniquement contournable, diffuser et populariser ces techniques peut rendre toutes ces lois caduques. Par exemple, [ce genre de document](#) (intéressant pour les moyens qu'il présente... un peu moins pour les finalités, mais bon... la technologie est neutre) montre que pour celui qui a un minimum de connaissances, on peut facilement se protéger. Les réseaux de P2P peuvent être cryptés ([GNUnet](#), [ANts](#) ou [mute](#), par exemple), ce qui rend tout contrôle impossible. Il y a également les réseaux privés (darknet...). À noter qu'il existe également des réseaux complètement anonymes et hors de contrôle, comme [FreeNet](#) ou [Tor](#) (Tor semble cependant moins sécurisé que FreeNet), mais ne comptez pas trop sur les gouvernements pour admettre leur impuissance face à un réseau que de toute façon, personne ne connaît (et c'est bien là l'enjeu : pour les gouvernements, peu importe les pédophiles, terroristes, ou voleurs qui ne sont qu'un prétexte, puisqu'au final, une grande majorité de la population se retrouve contrôlée et pense ce contrôle efficace).

[52 artistes](#) (enfin... si on peut appeler ça des artistes), auxquels ils faut ajouter une certaine Cindy Sanders, qui soutienne la loi hadopi, donc à éviter.

Utiliser des alternatives légales, la culutre ne se trouve pas que dans les rayons de la FNAC ou sur la mule : le P2P légal ([freetorrent](#) par exemple), les médiathèques (si on cherche des trucs pas trop récents, pour les films et la musique. En plus, c'est souvent de la meilleur qualité), [Jamendo](#). Quelques autres liens : [une liste de mp3 libres et gratuits](#) (et légaux...), de [la musique non libre, gratuite et légale](#), [un site de partage de vidéos libres](#).

Pour les périphériques de stockage, les disques durs internes ne sont apparemment pas concernés par les taxes de la commission d'Albi (à vérifier, tout de même...), on peut donc contourner facilement (et légalement) : en montant soi-même son disque dur externe avec un DD interne et un boîtier. Sinon, les autres pays d'Europe ne sont pas concernés, donc rien ne vous empêche d'y acheter vos clés USB.