Rapport Olivennes : première pression à froid
Par Jean-Marie Chauvet

Publié le 29 November 2007

Comme anticipé dès le moment même de la remise de la lettre de mission du Ministère de la Culture à Denis Olivennes, le rapport intitulé « *Le développement et la protection des oeuvres culturelles sur les nouveaux réseaux* », salué la semaine dernière avec des accents lyriques par le Président de la République, provoque un brouhaha de réactions. Les opinions se divisent évidemment en deux camps, déployant la rhétorique, le sarcasme et parfois l'invective :

- les pour, dans lesquels on trouvera sans surprise le Syndicat national de l'édition phonographique (SNEP), la Société civile des producteurs phonographiques (SCPP), la Société des auteurs et compositeurs dramatiques (SACD), l'Union des Producteurs phonographiques Français Indépendants (UPFI), les responsables à l'UMP des nouvelles technologies et de l'audiovisuel, ainsi que la Sacem ;

- les contre, parmi lesquels se sont manifestés l'Association pour la promotion et la recherche en informatique libre (APRIL), le Mouvement des jeunes socialistes, l'UFC-Que Choisir, et...deux députés apostats de l'UMP.

Clivage apparemment net, économique (producteur/consommateur) et politique (droite/gauche).

Cependant, la lecture du rapport Olivennes, si elle confirme qu'il y a amplement matière à exprimer de tels clivages – comme une évidence, partie émergée d'un iceberg dont la masse confuse et sombre est reléguée dans les renvois en bas de page, nombreux, et dans des annexes, jargonnantes – suscite aussi d'autres interrogations. Premier commentaire : DailyMotion, YouTube/Google pourtant auditionnés par la mission et Kewego, non consulté, ont approuvé mais n'ont pas, pour l'instant signé, ce rapport mettant en avant une contradiction avec le régime de responsabilité de l'hébergeur redéfini par la Directive européenne Commerce électronique et la Loi de confiance dans l'économique numérique (LCEN) de 2004.

La *Nouvelle surveillance*

Force est de constater que le rapport reprend à son compte une évolution graduelle vers ce que, dès 2004, Sonia Katyal de la Fordham School of Law appelait très justement les « nouveaux réseaux de surveillance ». Il s'agit d'instaurer progressivement un régime extrajudiciaire de contrôle et de sanction des infractions aux réglementations de la contrefaçon et du copyright, dont l'inspiration rappelle inévitablement la métaphore du *Panopticon* de Jeremy Bentham lumineusement employée par Michel Foucault dans « *Surveiller et punir* ». Reporters sans frontières avait également publié un rapport signalant l'avant garde de cette dérive en 2004 : « *L'Internet sous surveillance* ». Mais à l'époque on s'alarmait plutôt de ces tendances, depuis vivement exacerbées, chez les régimes autoritaires et dictatoriaux ou bien de la sournoise mise sous tutelle de l'Internet dans les démocraties bien installées et de tradition libérale au motif impeccable de la lutte contre le terrorisme.

En effet, le rapport fait d'abord le tour des arsenaux juridiques et technologiques existants et recommande leur emploi à des fins prophylactiques, « inciter l'offre légale » et « désinciter (*sic*) l'offre illégale ». Cet emploi relève de deux plans, à la Foucault : *surveiller* d'une part, par un filtrage des contenus qui peut être préventif ou répressif, et *punir*, d'autre part, par un dispositif « d'avertissement et de sanction ».

Pour mettre en oeuvre ce programme, le rapport constate d'abord que certains pays comme les Etats-Unis et le Royaume Uni ont mis en place un mécanisme d'avertissement et de sanction uniquement contractuel, qui ne repose que sur des acteurs privés et sur des obligations résultant des seuls contrats d'abonnement. L'exemple classique est celui de la RIAA aux Etats-Unis qui a, en 2002, contacté Verizon, un FAI américain, pour exiger les identités d'abonnés dont les sites hébergés par l'opérateur constituaient, de son point de vue, des noeuds de piratage et qui, devant le refus du FAI, l'a attaqué en justice – premier procès d'une longue suite déroulée depuis par les RIAA (Recording Industry Association of America) et MPAA (Motion Picture Association of America). Le rapport note avec justesse qu'une base uniquement contractuelle est difficilement envisageable en droit français : où serait la base juridique à une sanction prise par un FAI sans intervention d'un juge ou d'une autorité publique, ni imposition d'une obligation légale ?

En France, le Code de la propriété intellectuelle prévoit en effet que toute violation, comme la contrefaçon numérique, est un délit et relève du pénal. La clause de la loi DADVSI d'août 2006 qui prévoyait d'en exclure les téléchargements réalisés à des fins personnelles ou à des fins non commerciales (et de les reclasser en simples contraventions) a été, rappelons-le, censurée par le Conseil constitutionnel. Quant à la prévention de la mise à disposition de contenus illégaux sur des sites légaux (sous entendu hébergés par les FAI nationaux), la LCEN prévoit déjà des recours pour les ayants droits, qui doivent saisir l'autorité judiciaire qui prescrit ensuite aux FAI et opérateurs les mesures techniques propres à prévenir ou faire cesser le dommage, en clair résilier d'autorité l'abonnement de l'indélicat. Cette prescription d'autorité fait néanmoins encore débat, en particulier sur la possibilité pour les sociétés de perception et de répartition des droits d'auteur de mettre en place des dispositifs de recherches, les « radars » de la *Nouvelle surveillance* : le Conseil d'Etat durcit le ton, qui vient d'annuler, par exemple, une décision d'octobre 2005 de la CNIL qui estimait que le contrôle que les sociétés d'auteurs (la SACEM, la SCPP, la SDRM, et la SPPF en l'occurrence) entendaient mettre en place était disproportionné aux objectifs poursuivis.

L'Autorité publique de la *Nouvelle Surveillance* : Résiliator !

La solution est donc d'une désarmante simplicité suivant les préconisations du rapport Olivennes : reprendre et améliorer l'arsenal technique du mécanisme d'avertissement et de sanction, mais pour préserver les bonnes consciences le confier non pas aux seuls acteurs privés mais à une Autorité administrative publique. Tout au plus fera-t-on le subtil distinguo entre une Autorité qui avertirait le titulaire de l'abonnement Internet et déciderait elle-même de la sanction en cas de répétition des mêmes actes et une Autorité qui assurerait l'avertissement mais se contenterait d'une médiation obligatoire en amont de l'intervention d'un juge, qui déciderait, au final, de la sanction.

Dans un cas comme dans l'autre l'Autorité prendrait une sanction administrative distincte de la sanction pénale que le titulaire continuerait à encourir. Le vocabulaire employé dans le rapport a ici son importance : la sanction administrative de l'Autorité vise « le défaut de sécurisation du poste » et la sanction pénale vise « l'acte de contrefaçon », considérés comme violations de deux règles différentes du Code de la propriété intellectuelle.

Cette Autorité dont la mise en place pourrait se faire dans l'année 2008 se profile donc dans la ligne directe de l'institutionnalisation de la *Nouvelle surveillance*. Au-delà des réactions que le rapport commence à susciter, il sera intéressant de suivre, dans la période qui s'ouvre, avec quelle vitesse le dispositif législatif sera adopté. La célérité, déjà promise par Mme Albanel, laisse à penser que les dés sont jetés. Et pourtant pour que cette Autorité que le rapport appelle de ses voeux puisse fonctionner, il faut quand même s'accommoder de quelques entorses au droit :

- le suivi de la procédure d'avertissement et la prise de sanction requièrent d'une façon ou d'une autre le rapprochement entre une adresse IP et un nom de titulaire d'un abonnement. Aujourd'hui ce rapprochement n'est possible que par le recours à l'intervention d'un juge, ce que le Conseil constitutionnel a précisé à propos de la LCEN en 2004. Il faudrait donc modifier le Code des postes et communications électroniques pour autoriser l'Autorité à effectuer ce rapprochement sans recours judiciaire. (Le rapport juge cette modification « acceptable » compte tenu « des garanties d'indépendance et d'impartialité présentées par une autorité réunissant des agents dotés de prérogatives de puissance publique » – on appréciera.)

- le suivi et la sanction nécessitent l'établissement de fichiers des contrevenants, puisque la répétition déclenche la sanction, ce qui doit être, aux termes du droit, être expressément autorisé par la CNIL.

- l'autorisation de la CNIL est également indispensable pour conserver pour une durée définie les données de connexion. C'est un sujet très délicat : Google avait cédé en juin dernier aux pressions de la Commission européenne, acceptant de rendre anonymes les traces de connexions que le moteur de recherche conserve et archive, au bout de 18 mois plutôt qu'à la fin des 24 mois auxquels il s'était vaguement engagé.

L'éternelle absente : la question des moyens

Plus généralement, se pose aussi la question, éludée dans le rapport, des moyens donnés à une telle Autorité. Sentant poindre l'éventuel bât blessant, le rapport suggère d'ailleurs d'étendre le périmètre de la toute nouvelle Autorité de régulation des mesures techniques (ARMT), prévue par la loi DADVSI d'août 2006 et intronisée en avril dernier, plutôt que de créer une nouvelle Autorité de toutes pièces. Les moyens de l'Autorité décideront en effet immédiatement de la volumétrie que peut atteindre le *Nouveau réseau de surveillance* : face à des FAI nombreux et, pour certains, financièrement armés, il conviendrait que cet opérateur d'un nouveau genre, le CAI (Coupeur d'accès Internet) ne soit pas démuni !

Le *filtrage préventif* pour empêcher l'infraction est bien sûr trop cher. Le déploiement à large échelle des technologies de filtrage implique d'une part nécessairement les FAI - mais qui paye ? - et d'autre part des solutions techniques diverses, récentes et, note le rapport, « relativement performantes mais encore perfectibles ». D'autant plus que, ne s'agissant exclusivement que de contenus et de productions français sous l'autorité républicaine du CAI hexagonal, les prestataires techniques ne sauraient être que nationaux, ce qui en réduit forcément le nombre ! De fait, tous les prestataires de solutions techniques auditionnés sont d'origine française : AdVestigo, LTU Technologies, I-Tracing, Qosmos, Thomson - derrière lesquels les paranoïaques qui ont survécu reconnaîtront l'INRIA, le LIP6 de l'Université Pierre-et-Marie-Curie, le CEA/LETI, la DGA, Cyber Networks et curieusement

JASTEC le géant japonais de l'électronique et des services - l'INA, qui a développé son système d'empreinte numérique, Signature, repris pas Canal + et par DailyMotion, mais également les beaucoup plus insaisissables et voilés de mystère Communications SA (tatouage numérique) et CoPeerRight Agency (peut-être une émanation sulfureuse du SELL, qui s'était illustrée en 2005 avec l'autorisation de la CNIL par l'envoi d'avertissements menaçants aux internautes repérés sur des réseaux P2P). Seule exception l'américain Audible Magic qui, il est vrai, fournit le *fingerprinting* pour DailyMotion initialement prévu comme signataire du rapport.

Le *filtrage répressif*, quant à lui, soulève évidemment des questions sur la protection des correspondances et de la vie privée. L'aspect légal de ces questions est du ressort de la CNIL en France. Mais plus indirectement, ce que pourrait également craindre le gouvernement serait que le renforcement du filtrage répressif - contrairement à ce qui se passe pour la sécurité routière - entraîne une généralisation puis une banalisation de l'usage de la cryptographie dans les échanges. Et là, danger ! On rentre sur le terrain miné de l'intérêt national, de l'intelligence et du patriotisme économique et ses 11 secteurs stratégiques protégés ! (*128 bits or not 128 bits, that is the question?*) Il ne s'agirait pas que l'on ne puisse plus se faire contrôler. Tiens ! On ne parle plus beaucoup des *hackers* rouges qui défrayaient encore la chronique il y a quelques semaines : des réseaux directement liés au service de l'Etat français avaient été visés selon le secrétaire général de la Défense nationale. Pensez donc, même le portail Internet du Ministère de la Défense avait ainsi fait l'objet de plusieurs intrusions…

Il y a quelques semaines encore, par exemple, Bruce Schneier, expert mondialement reconnu en sécurité informatique, s'étonnait de constater que parmi les trois algorithmes de génération de nombres aléatoires, indispensables en cryptographie, retenus officiellement par le NIST (le National Institute of Standards and Technology, l'agence américaine de réglementation dépendant du Ministère du Commerce), celui proposé par la NSA (National Security Agency) était bizarrement le plus lent à l'exécution. De là à penser qu'il contient une « *backdoor* » qui rendrait toutes les implémentations commerciales, du coup obligatoires pour obtenir l'approbation du NIST, vulnérables aux vérification du gouvernement américain...ou d'autres, le sang se glace d'effroi !

Ne doutons pas qu'en France aussi, ces questions agitent bien d'autres cercles que ceux des seuls Ministère de la Culture et de la mission Olivennes.

Une foi inébranlable en la technologie

La question des moyens financiers touche rapidement celle de l'équilibre entre protection des données de la vie privée et intérêt public, entre contrefaçon et copie (unique) pour usage privé, entre système judiciaire et autorité administrative extrajudiciaire. Mais avant tout, le rapport, semble professer une foi inébranlable en la technologie et en la mise en place d'un arsenal technique et automatisé se présentant alors comme solution à un vaste problème de comportements et de système économique.

Pas un instant ne sont évoqués un monde virtuel de communications électroniques, courrier électronique, messagerie instantanée, IRC, réseaux P2P, VoIP où la cryptographie individuelle se serait banalisée au point de devenir la règle et non plus l'exception, la réglementation hâtant de provoquer ce qu'elle cherchait à éviter.

Pas un instant n'évoque-t-on les usages inattendus et, comment dit-on ? « inappropriés » qui pourraient être faits d'un fichier centralisé des contrevenants : nos amis britanniques, grands promoteurs de la *Nouvelle surveillance* par exemple, ont laissé s'évanouir dans la nature des données confidentielles concernant quelque 25 millions de personnes, a reconnu mardi dernier devant le Parlement le ministre des Finances Alistair Darling.

Laissons aussi à votre imagination les usages créatifs d'un fichier centralisé des empreintes numériques des contenus que devraient utiliser les « radars » du *Nouveau réseau de surveillance*. Le rapport suggère d'ailleurs une sorte de portail coopératif des sociétés d'auteurs et de productions où seraient publiés des tableaux de bord statistiques sur la décroissance inéluctable de la piraterie après ces mesures et qui centraliserait ces empreintes. À ce sujet je propose le nom de domaine www.exceptionculturelle.fr qui est inexplicablement encore libre ! (Gracenote, pour les CD, et Kaleidescape pour les DVD, deux *startups* américaines, ont ainsi construit des fichiers centralisés leur permettant de reconnaître à distance les contenus audio et vidéo joués sur vos lecteurs de salon connectés au Web, sans parler du couple par qui le scandale est arrivé iPod/iTunes - pourrait-on « planter » d'autorité votre iPod ou votre iPhone s'il venait à contenir des morceaux considérés comme piratés ?).

Et que penser du curieux dévoiement qui en miroir de ce qui se passe aux Etats-Unis où le contournement des mesures de protection installées par des acteurs et des opérateurs privés est illégal, verrait ici rendre illégal l'absence de sécurisation du poste de l'abonné ? L'affaire récente du DRM que BCG-Sony avait installé sans avertissement sur certains de ses supports qui, basés sur un *rootkit* rapidement exploité indûment par des *hackers* pas très bien intentionnés, détruisaient alors efficacement le PC sur lequel d'aventure l'utilisateur avait choisi de les écouter, n'a pas porté apparemment.

Et *quid* des contenus non identifiés par l'Autorité comme produits français : l'identification pose question en soi. C'est le Conseil d'Etat qui a du confirmer que le film « *Un long dimanche de fiançailles* », super production de Jeunet, était un film...américain !

Pour édulcorer le message, le rapport préconise un inventaire de mesures « politiquement correctes » et difficilement critiquables : ramener la fenêtre VOD de disponibilité des films de 7 mois à 4 mois après la sortie en salle, abandonner au nom de l'interopérabilité, droit qui deviendra bientôt constitutionnel n'en doutons pas, les mesures de protection (DRM) - Apple fait décidément bien de l'ombre à certains rentiers assoupis !-, subordonner les aides à la production du CNC à l'engagement de la mise en disponibilité des films en VOD - le nerf de la guerre, vous dis-je !-, généraliser le taux de TVA réduit aux produits et services culturels - invoquer l'Europe -, regrouper les ayants droits en une agence unique - l'union fait la force, mais les querelles de chapelles s'y opposent -, et si l'on obtient la baisse de la TVA, élargir l'assiette des abonnements *triple play* soumis à ce taux réduit en contrepartie d'une nouvelle taxe alimentant des fonds de financement de la création et de la diversité musicales (bien oubliée dans tout le discours juridico-technologique) - un jeu à somme nulle pour les FAI.

Alors pistes sincères et originales pour débroussailler un sujet qui se complexifie avec le temps et ne peut se satisfaire de jugements à l'emporte-pièce ou bien agit-prop médiatique et opération de communication savamment orchestrée pour une inclinaison politique déjà prédéfinie ?