

Note sur la « riposte graduée » et le « paquet télécom »

François Pellegrini (pelegrin@labri.fr)

Version 1.0, 04/08/2008

Résumé

Plusieurs amendement insérés dans le « paquet télécom » n'ont rien à y faire. Ils ont été écrits par les membres et les sympathisants de l'industrie culturelle, afin de surveiller et contrôler la circulation des flux numériques, et d'orienter le comportement des usagers de l'Internet vers l'usage de leurs plateformes de contenu par l'utilisation d'outils de surveillance et de filtrage, violant ainsi le paradigme de la « neutralité de l'Internet ».

L'impact de ces amendements d'intérêt privé est considérable : en plus de transformer la ressource publique mondiale qu'Internet est devenu en un réseau de distribution privé pour le bénéfice de quelques acteurs, ils permettent aux autorités de régulation de mettre en œuvre, sans aucun contrôle démocratique, des outils automatiques de surveillance du comportement des usagers de l'Internet, jusqu'au sein même de leurs propres ordinateurs (une pratique parfois appelée « informatique de confiance », « *trusted computing* » en anglais), et de les bannir de cette ressource mondiale sans aucune décision de justice (approche appelée « riposte graduée », ou parfois en anglais « *three-strikes approach* »).

Tous ces amendements furtifs doivent être retirés du « paquet télécom », auquel ils ne devraient pas appartenir. De plus, ils représentent sur le fond une telle menace contre le développement de la société de l'information qu'ils ne devraient jamais être votés ni même considérés, mais au contraire rejetés en bloc.

Cette note s'attache à expliquer pourquoi.

La révolution de l'accès, abondance contre rareté

Lorsque les œuvres de l'esprit étaient liées à leur support matériel, comme les livres imprimés, les disques en vinyle ou même les CD, il était difficile aux artistes de toucher leur public. C'est pourquoi des agents qui n'étaient pas eux-même des artistes ont pris en charge la tâche de dupliquer et de diffuser les œuvres originales, agissant en médiateurs entre les artistes et le public. Du fait de la concentration industrielle, et parce que toutes les œuvres éditées ne pouvaient être distribuées, les éditeurs se sont trouvés en position de contrôler le succès commercial des artistes, et au final ont fusionné avec les producteurs de façon à ce que les décisions de production et d'édition puissent être prises globalement : soit un artiste était produit et distribué de façon à maximiser le retour sur investissement, soit il n'était pas produit du tout. La concentration de ces acteurs a maximisé leur revenu, mais à diminué la diversité culturelle perceptible par le public, puisque seul un nombre limité d'artistes pouvaient bénéficier de publicité à grande échelle. De plus, être en situation de contrôler les circuits de distribution leur permettait de fixer des prix élevés, ce qui augmentait encore plus leur profit¹

La situation a été complètement bouleversée par l'Internet. En permettant un contact direct entre les artistes et leur public pour un coût nul², celui-ci permet de transformer la rareté en abondance : les

1 On considère que les auteurs gagnent en moyenne 7 % du prix de détail des CD, c'est-à-dire, pour un CD de 13 chansons vendu 13 Euros, 7 centimes d'Euro par chanson.

2 Alors qu'aux premiers temps de l'Internet les usagers étaient facturés en fonction du volume de données échangées, les

petits groupes de musique peuvent trouver des auditeurs loin de leur région d'origine en diffusant certaines de leurs œuvres sur leurs sites web personnels ou sur des sites mutualisés comme Myspace Music ou Jamendo, et peuvent vendre et expédier directement leurs disques, avec des bénéfices par exemplaire bien supérieurs à ceux qu'ils pouvaient obtenir de la part des éditeurs et distributeurs traditionnels.

Toute révolution technologique favorise certains acteurs et en fait disparaître d'autres. La révolution de l'accès rend les éditeurs sans objet, alors que la fonction de producteurs est toujours nécessaires, mais avec des coûts bien moindres par la généralisation de logiciels de traitement audio et vidéo maintenant disponibles sur de simples ordinateurs domestiques. De ce fait, les grands éditeurs se sont mis en tête de ralentir, voire d'arrêter, ce processus. Ceci ne peut se faire qu'en réintroduisant une rareté artificielle là où l'abondance est la règle ; il s'agit en l'espèce de mettre en place des moyens de discriminer entre les types de contenus et de ralentir ou de filtrer les contenus ne provenant pas des sites des grands éditeurs, de façon à ce que les usagers soient incités à acheter leurs contenus seulement à partir de ces derniers.

Le moyen qui a été trouvé est de définir certains contenus et actions comme « illicites » et, lorsque ces actions sont « illicites », de refuser aux usagers tout droit à un service normal et à l'absence de filtrage. Par contraposée de cette proposition logique, il est clair que tous ces amendements furtifs visent à légaliser la surveillance et le filtrage des contenus en retirant aux usagers « illicites » tout droit à se plaindre de telles mesures.

Comment peut-on déterminer ce qui est licite ou pas ?

Tous les amendements en question créent une distinction entre ce qui est « licite » et « illicite ». Par exemple, l'amendement de compromis 5 sur l'Article 22(3) vise à préserver « raisonnablement » (!) la qualité de service de l'Internet pour « *l'accès à, ou la distribution de contenu licite* »³ ainsi que pour « *l'exécution d'applications et de services licites* ».

La question clé est donc : comment peut-on savoir si un contenu ou une application est « licite » ou non ? C'est un point essentiel, car l'entité décidant de ces sujets a le pouvoir de façonner l'Internet à sa volonté, par exemple en excluant tous les services innovants qui pourraient mettre en danger les intérêts représentés par cette entité. La réponse, d'un point de vue purement technique, est : il n'y a aucun moyen. Même un utilisateur envoyant des fichiers audio couvert par les droits d'auteur de l'une de ses adresses courriel à une autre peut juste être en train d'exercer son droit à la copie privée, en transférant ces fichiers depuis l'ordinateur de sa maison à celui de son bureau. Ce n'est qu'à travers le jugement humain qu'une action peut être comprise comme licite ou illicite.

Cependant, les promoteurs des amendements semblent plutôt sûrs de pouvoir débusquer les « contenus illicites » et les « applications et services illicites », dont la qualité de service ne serait pas garantie. Comment peuvent-ils donc le faire ?

Les deux seuls moyens pour y parvenir sont soit d'effectuer un filtrage *a priori* en discriminant certaines technologies et protocoles de communication comme les systèmes pair-à-pair sans considérer leur usage (comme si toutes les automobiles étaient bannies parce que certaines peuvent être utilisées comme voitures bélier contre des magasins) et en brisant de ce fait la neutralité de l'Internet, soit au vol en espionnant le contenu des données échangées, enfreignant les lois sur la correspondance privée.

Les deux sont inopérants : le cryptage des communications empêche les agents intermédiaires

offres dites « *triple-play* » permettent de disposer de la connectivité téléphonique et Internet à un coût mensuel fixe. On peut donc considérer que ce paiement couvre les frais téléphoniques, et que l'accès Internet est gratuit, indépendamment de la quantité de données transférée.

3 Ces amendements n'étant pas encore officiellement traduits en Français, leur version française est de mon fait.

d'analyser le contenu des données échangées, et des systèmes de transfert de données peuvent être bâtis au dessus de, par exemple, du système de courrier électronique, de façon à ce que des fragments de fichiers soient envoyés lorsque des en-têtes spécifiques de courrier sont utilisés. La surveillance de ces échanges, surtout si elle est effectuée par des entités privées, entrera nécessairement en conflit frontal avec le droit à la correspondance privée. Cette dernière doit-elle être subordonnée à des intérêt privés ?

La riposte graduée à la Française est une voie sans issue

Les tentatives d'ouvrir la voie à quelque version de la riposte graduée à la Française oublient de considérer un point important : elle est impraticable, tant en principe qu'en pratique, tout en portant atteinte aux libertés individuelles d'une façon considérable.

Ce dispositif a été conçu par l'industrie culturelle pour remplacer les longues procédures judiciaires nécessaires à l'identification et à la poursuite des usagers partageant des fichiers musicaux, par un système automatique permettant de les identifier, de les sermonner et, après le troisième avertissement, de les bannir de l'Internet pour une période de temps donnée, sans possibilité pour eux de s'abonner à un autre fournisseur (au moyen d'un fichier de liste noire). Ce dispositif pose un certain nombre de problèmes de droit sérieux qui devraient empêcher de pousser en avant les amendements furtifs du « paquet télécom ».

- En ce qui concerne l'imputabilité, toutes les mesures d'envoi de messages se basent sur ce qu'on appelle l'« adresse IP » de l'ordinateur de l'utilisateur, telle que vue depuis l'Internet, et qui est en quelque sorte équivalente au numéro de la rue à partir de laquelle le trafic provient ou doit parvenir. Le problème est que plusieurs membres de la même famille utilisent la même adresse ou même, pour une entreprise, que tout le trafic induit par les ordinateurs de l'entreprise est souvent vu comme provenant de l'unique adresse IP de l'entreprise. Qui sera alors poursuivi ? L'entreprise entière sera-t-elle bannie de l'Internet ? Tout ceci est négligé et, comme il est prévisible, amène à des conséquences disproportionnées bien qu'amusantes : en Finlande, le premier usager de l'Internet a avoir été banni a été... le gouvernement du territoire autonome de l'île d' Åland ! Dommage pour l'avancée de l'administration électronique...

Comme il est extrêmement facile de casser les sécurités WEP d'une connexion WiFi, on peut même imaginer des actions de nuisance contre des organisations ou personnes en vue pour qu'elles soient ciblées et bannies de l'Internet. Comme on peut le voir, en supprimant toute nécessité de charge de la preuve, l'insécurité juridique des usagers est accrue.

Fermer l'accès Internet d'une famille entière si l'un de ses membres est supposé⁴ responsable de comportement « illicite » est une privation de liberté disproportionnée, alors que l'Internet est maintenant un moyen pour les citoyens de s'éduquer, d'interagir avec leurs administrations, de trouver un emploi. C'est comme si, parce que quelqu'un est suspecté d'avoir volé une pomme, toute sa famille devait rester enfermée chez elle. Est-ce ceci que les Députés européens désirent, à l'ère numérique ?

- La procédure d'appel est conçue pour ne pas être suspensive, car sinon l'effet du dispositif serait marginal, puisque tous les défendeurs feraient appel en justice sur la faiblesse de la preuve, créant les embouteillages juridiques que le dispositif vise à éviter. Par conséquent, en cas d'erreur, les usagers peuvent être empêchés d'utiliser l'Internet pour plusieurs mois et être mis sur liste noire sans aucun échappatoire, même si leur emploi en dépend.

4 C'est délibérément que ce mot est utilisé à la place de « jugé », puisque de telles actions sont réalisées en l'absence de tout jugement équitable.

- Les sanctions prévues par le dispositif de riposte graduée ne peuvent empêcher les ayant droit de lancer des procédures civiles et pénales. Comme le Conseil constitutionnel français a statué durant le vote de la loi DADVSI (qui est la transposition française de la directive EUCD), en matière de droits d'auteur, soit il y a violation, soit il n'y a rien. Le fait que certains ayant droits puisse renoncer à poursuivre les internautes lorsque ceux-ci font l'objet de mesures automatiques prises par les autorités administratives nationales est leur décision propre, qui peut être reconsidérée à tout moment, et peut ne pas être suivie par d'autres ayant droits. Le suivi massif des usagers de l'Internet n'est de ce fait pas une compensation pour l'absence de poursuites : celles-ci peuvent toujours être lancées lorsqu'assez de données ont été collectées.
- Le rôle de surveillance du trafic des usagers est dévolu à des entités privées qui, afin d'accomplir leur tâche, doivent analyser le contenu des données échangées, et de ce fait violer le droit à la correspondance privée des internautes. Ce filtrage sera de toute façon inopérant lorsque les usagers, pour faire respecter ce droit, auront recours à des canaux de communication cryptés. Ces canaux cryptés sont déjà monnaie courante, et recommandés par de nombreuses administrations pour sécuriser les échanges de données contre les interceptions électroniques par des systèmes de type Echelon. Je les utilise personnellement chaque fois que je me connecte à mes ordinateurs. Le trafic crypté sera-t-il bloqué comme étant « illicite » par nature ?

Les moyens d'actions envisagés par les dispositifs de riposte graduée sont tout simplement dépassés et inefficaces.

L'aberration juridique inhérente au dispositif de riposte graduée est décrite en détail dans le « rapport Cédras »⁵, écrit par Jean Cédras, professeur de Droit de l'Université de La Rochelle. Ce rapport, commandé par le Ministère français de la Culture, a été enterré à peine remis, parce que ses conclusions ne correspondaient pas aux vues à court terme des grands industriels de biens culturels.

Le gouvernement Suédois a lui aussi rejeté cette approche. Le Parlement européen l'adoptera-t-il parle biais de directives qui n'ont rien à voir avec le sujet ?

L'histoire complète

Durant les 15 dernières années, en parallèle de la diffusion de l'Internet, beaucoup de législations proposées ou adoptées ont ajouté de nouvelles formes de sanctions à celles punissant déjà la violation des droits d'auteur : poursuites légales contre le contournement de mesures techniques de « protection »⁶ (appelées « MTP », depuis 1994 aux États-Unis puis en Europe), obligation d'utiliser certaines MTP (SSSCAct aux États-Unis et l'amendement appelé « Vivendi » à la loi DADVSI en France), possibilité pour les fournisseurs de contenu de surveiller le trafic (loi LCEN en France en 2006), mesures civiles préventives extrêmes (directive 2004/48/CE, projet de l'accord ACTA), sanctions pénales de violations à but non commercial et d'incitation (brouillon de la directive IPRED2 et de l'accord ACTA), etc.

La plupart de ces nouvelles formes de sanctions et d'amendes sont conçues pour être appliquées sans jugement, par la création de procédures automatiques qui peuvent se dérouler avant même que toute violation ait effectivement lieu. La riposte graduée s'inscrit dans cette tendance. Comme pour toutes les

5 <http://www.odebi.org/docs/RapportCedras.pdf> .

6 Les guillemets sont nécessaires parce qu'aucune de ces mesures ne « protège » effectivement les œuvres, qui peuvent toujours être copiées numériquement dans leur ensemble. Elle garantissent seulement les monopoles des fournisseurs de logiciels de visionnage de contenus, liés aux éditeurs qui distribuent du contenu brouillé selon des algorithmes triviaux mais (originellement) secrets tels que l'algorithme CSS.

autres de ces mesures, elle a fait l'objet d'une action mondiale (sous le nom de « *three-strikes approach* ») par les lobbies des ayant droit, rejoints par les promoteurs de dispositifs d'« informatique de confiance » tels que le système NGSCB⁷ (auparavant connu sous le nom de « TCPA/Palladium ») développé par Intel et Microsoft (qui est un des principaux membres du lobby BSA). Ce système n'a pas rencontré de succès commercial, et toute tentative de créer un tel marché par la loi est accueillie favorablement par ces acteurs.

Les mesures obligatoires de « sécurité » menacent la sécurité de l'Europe

L'amendement de compromis 2 sur l'Article 20 contient, dans les deuxième et dernier items du paragraphe 2.b), des mentions étonnantes sur les « *restrictions imposées par le fournisseur concernant la capacité d'un abonné à accéder, à utiliser ou à distribuer du contenu licite ou à exécuter des applications ou services licites* » », et sur « *toutes restrictions sur l'usage de l'équipement terminal imposée par le fournisseur* », desquelles l'utilisateur doit être au moins informé. Comment se fait-il qu'un usager puisse-t-il être restreint dans sa capacité à utiliser l'Internet, qui plus est si de telles actions sont « licites » ?

La réponse réside dans le désir des fournisseurs de contenu de restreindre, sur l'ordinateur de l'utilisateur lui-même, sa capacité à utiliser le contenu culturel qu'il a légalement acquis. Par exemple, en 2004, SonyBMG a ajouté à certains de ses CD une « mesure technique de protection » sous la forme d'un logiciel appelé XCP⁸, qui s'installait silencieusement sur l'ordinateur de l'utilisateur sans l'en avertir, et empêchait automatiquement l'utilisateur d'entreprendre certaines actions telles que copier des fichiers audio depuis le CD vers d'autres médias. Ce logiciel représentait une menace sérieuse en terme de sécurité, en ouvrant des brèches qui favorisaient l'installation de logiciels malicieux, mais toute tentative de le supprimer était légalement impossible car étant assimilé au contournement d'une MTP.

Le but des systèmes de type NGSCB est bien plus grand: il vise à prévenir tout programme « non de confiance » (« *untrusted* » en anglais) à accéder à du « contenu de premier choix » (« *premium content* ») stocké localement sur l'ordinateur de l'utilisateur ou accessible par Internet. Sur les ordinateurs exécutant ce système, tout programme non reconnu par le fabricant du système ne peut interagir avec ces données. Ici encore, dans ce dispositif, c'est à des entités privées de décider si une nouvelle application qui offrirait un service nouveau et innovant est capable d'accéder le contenu légitime de l'utilisateur, et de fait d'être commercialement intéressant ou non pour les consommateurs. En particulier, les logiciels libres ne seront jamais considérés, puisque pour les ayant droit la mise à disposition du code source est une menace sur le secret des MTP qu'ils mettent en œuvre (et qui sont pourtant inefficaces de toute façon, étant « cassées » à peine quelque mois après avoir été commercialisées).

Être capable d'imposer, par le biais des autorités nationales ou de ceux qu'on appelle les « parties prenantes », de telles « mesures techniques », est un moyen subtil mais terriblement efficace de biaiser le marché au détriment des logiciels libres et des services nouveaux offerts par des individus ou PME innovantes. Les usagers doivent-ils posséder le logiciel d'un vendeur spécifique pour accéder à l'Internet ? Comment les agences de sécurité nationales et européennes peuvent-elles s'assurer que de tels logiciels, secrets par nature, ne contiennent pas de portes dérobées⁹ pouvant mettre en danger

7 <http://www.lebars.org/sec/tcpa-faq.fr.html>.

8 http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal.

9 <http://www.heise.de/tp/r4/artikel/2/2898/1.html>.

l'indépendance informationnelle de l'Europe ?

À ce titre, certaines dispositions du « rapport Alvaro », qui ouvrent la voie à de tels comportements, sont à prendre avec la plus grande précaution. Par exemple, l'Amendement 32 dispose : « *En mettant en œuvre les provisions de cette Directive, les États membres doivent s'assurer, en conformité avec les paragraphes 2 et 3, qu'aucune disposition obligatoire pour des fonctionnalités techniques spécifiques, incluant, sans limitation, celles ayant pour but de détecter, intercepter ou prévenir la violation de droits de propriété intellectuelle par les usagers, sont imposées sur les équipements terminaux ou de communication électronique d'une façon qui pourrait nuire au placement de ces équipements sur le marché et à la libre circulation de ces équipements à l'intérieur et entre les États membres* ». Cet amendement pourrait être compris comme empêchant les dispositions obligatoires sur les fonctionnalités techniques; une lecture attentive montre au contraire que, tant qu'ils ne « *nuisent pas au placement de ces équipements sur le marché* », de telles obligations de fonctionnalités techniques sont complètement permises, d'autant plus si elles sont fournies par le même vendeur que celui qui fournit le logiciel de l'ordinateur.

Le P2P est un outil, pas un crime

On désigne par cet acronyme (abréviation du terme Anglais « *Peer-to-Peer* », traduit en Français par « Pair-à-Pair ») une technologie d'échange de fichiers, les logiciels mettant en œuvre cette technologie, ainsi que les usages qui sont fait de cette technologie.

À la différence des systèmes de diffusion classiques, dans lesquels une source unique, appelée « serveur », transmet une information définie à l'ensemble des postes des utilisateurs, appelés postes « clients », la technologie P2P est basée sur la symétrie : tous les ordinateurs utilisant le même logiciel de P2P peuvent à la fois se comporter comme clients, lorsque l'utilisateur souhaite obtenir sur son disque dur local une copie complète d'un fichier donné, mais aussi comme serveurs capables de fournir à d'autres utilisateurs tout ou partie des fichiers que ceux-ci demandent, et dont on possède déjà une copie.

Cette spécificité fait que les logiciels P2P constituent un outil révolutionnaire pour la création et la diffusion culturelles, ainsi que pour la réduction de la fracture numérique.

En effet, avec un système de diffusion classique, un auteur désireux de mettre à la disposition du public les œuvres sonores ou audio-visuelles qu'il crée devrait disposer d'un débit de communication « montant » (c'est-à-dire allant dans le sens de son ordinateur vers l'Internet) capable d'absorber la demande des internautes voulant télécharger ses œuvres à partir de son site. Or, les technologies de type ADSL ne sont pas conçues pour cela : partant du principe que les utilisateurs consomment plus d'informations qu'ils n'en produisent et diffusent, la capacité de communication du lien ADSL reliant un ordinateur à l'Internet est près de dix fois plus importante dans le sens « descendant » (c'est-à-dire dans le sens allant de l'Internet vers l'ordinateur) que dans le sens montant (le « A » de « ADSL » veut d'ailleurs dire « asymétrique », pour indiquer cette asymétrie dans les capacités de communication). De fait, pour diffuser ses œuvres, un créateur devrait louer une ligne de plus grande capacité, à un prix beaucoup plus élevé, ou louer un espace sur un serveur professionnel offrant ce type de débit.

Le P2P est la réponse à ce problème : dès le moment où plusieurs copies d'un fichier ont déjà été téléchargées par des internautes, lorsqu'un nouvel utilisateur souhaite récupérer ce fichier, des portions de celui-ci lui sont envoyées par chacun des utilisateurs le possédant. Ainsi, les capacités montantes de ces utilisateurs sont employées conjointement pour alimenter le nouvel arrivant avec une quantité d'informations équivalente à son débit descendant. Cet utilisateur bénéficie d'un accès à l'œuvre à haut débit, même si son créateur ne dispose que d'une communication montante à faible débit, mais peu

onéreuse.

Parmi les exemples de ce nouveau moyen d'échange, on peut citer :

- la mise à disposition des internautes des fichiers représentant le contenu des CD et DVD des distributions logicielles Linux ;
- le projet P2PTelevision, destiné à permettre la diffusion sur Internet de programmes audiovisuels créés par et à destination de communautés n'ayant habituellement pas accès aux média conventionnels (programmes en langues régionales, contenus locaux, etc) ;
- la diffusion aux internautes, par ses créateurs, du film *Starwreck*, le film Finlandais le plus vu de l'histoire ;
- et de bien d'autres exemples.

Le P2P est donc une technologie, révolutionnaire et excessivement peu onéreuse, pour la création d'une société de l'information inclusive. Comme toute technologie, elle est neutre, et ce sont les usages qui en sont faits qui peuvent être licites ou non. Ce n'est pas parce que certains l'utilisent pour diffuser illégalement certains contenus que cette technologie doit être bannie.

On peut cependant se demander qui seraient les principaux bénéficiaires d'une interdiction de facto des technologies P2P. Ne seraient-ce les fournisseurs de contenu dominants, qui ont les moyens de posséder des serveurs de fichiers disposant de débits montants importants, et qui pourraient voir dans des réseaux de diffusion alternatifs une menace pour leurs rentes ?

Conclusion

Le « paquet télécom » est un ensemble de directives destinées à créer un marché unique dans le secteur des télécommunications, et à préserver l'intérêt des consommateurs. Il traite des canaux de communication, mais absolument pas des contenus et services qui sont offerts et seront offerts dans le futur.

Par conséquent, les amendements traitant du contenu, qui proposent un modèle de rente spécifique favorable à quelques acteurs dominants, et auront tendance à freiner le développement de nouveaux services et acteurs tout en mettant à mal l'indépendance informationnelle européenne, n'ont rien à y faire, d'autant plus qu'ils seraient très difficiles à reconsidérer ultérieurement.

Tous ces amendements de contenu, qui discriminent sur une base impossible entre contenu « licite » et « illicite », doivent être rejetés en bloc. Cependant, comme la mutation des services de contenu à l'ère de l'Internet est un sujet d'extrême importance, un débat parlementaire sur ce sujet est absolument nécessaire, dans un cadre qui reste encore à définir.

