



Consultation publique sur l'internet ouvert et la neutralité du Net :

Réponse de la Ligue [Odebi](#) au questionnaire de la Commission Européenne.

Organisation citoyenne ayant pour objet de défendre les libertés civiles dans la société de l'information, Odebi doit répondre au [questionnaire de la Commission](#) en privilégiant deux points de vue : l'un, évident en l'état actuel des débats, est celui de la liberté d'information. L'autre, actuellement peu pris en compte, est celui du respect de la vie privée, et en particulier du secret des correspondances.

Ainsi, quand le questionnaire pose en préambule : « *This questionnaire therefore focuses principally on the behaviour of operators, and in particular how they may manage traffic flowing over their networks [...], in order to see how this behaviour might impact on the 'net freedoms' of citizens (i.e. their 'ability to access and distribute information or run applications and services of their choice').* » il n'aborde pas le problème fondamental qui est masqué par le concept de plus en plus flou ou élargi de « Neutralité du Net » : celui du respect du secret des communications. De ce fait, cette réponse ne peut suivre l'ordre des questions proposé par la Commission, et doit être considérée globalement comme une réponse à la question 15 et à la suggestion du paragraphe 4.6 du questionnaire.

Le débat sur la neutralité du Net gagne l'Europe après s'être développé aux États-Unis, dans un contexte particulièrement spécifique de dérégulation, et de questionnement quant à l'évolution du rôle de la FCC. A contrario, [Me O. Iteanu fait à juste titre remarquer une certaine clarté du droit français](#) en matière de neutralité des communications : « *C'est en 1996 que la neutralité apparaissait effectivement dans notre droit positif. La loi de réglementation des télécommunications de 1996, consacrait cette notion que l'on retrouve aujourd'hui dans des dispositions explicites du Code des postes et Communications Electroniques.*

A l'article L. 32-1-II-5 du Code :

'Dans le cadre de leurs attributions respectives, le ministre chargé des communications électroniques et l'Autorité de régulation des communications électroniques et des postes prennent, dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées aux objectifs poursuivis et veillent : (...) 5° Au respect par les opérateurs de communications électroniques du secret des correspondances et du principe de neutralité au regard du contenu des messages transmis, ainsi que de la protection des données à caractère personnel ;' »

Ainsi, il est à première vue légitime de douter de l'utilité d'un tel débat -en tous cas- en France, dès lors que les opérateurs qui y vendent de l'accès à Internet (Internet [access providers](#)) sont tenus de respecter la loi française.





Mais : on remarque que des opérateurs mobiles interdisent l'accès à certains services internet, comptant sans doute sur une éventuelle interprétation des textes par le juge qui leur serait favorable, et surtout : le problème fondamental sous-jacent n'est pas celui de la 'neutralité stricto sensu', mais celui de la mutation d'internet vers un environnement NGN, judicieusement mentionné par le questionnaire : « *Particularly as operators start to invest in Next Generation Networks and increased traffic management capabilities, clarity may be needed as to what constitutes 'reasonable traffic management' and what might be considered as unacceptable both by regulators and consumers.* »

La motivation ayant mené à cette proposition architecturale est clairement exprimée par le groupe de travail SG13 de l'ITU dans un [document de recommandation faisant suite au meeting SG13 de janvier 2009](#) :

« [...] framework of **DPI** within packet-based networks and NGN environment.

*The IPv4/v6/NGN access and metro networks are primarily built with the packet switching and routing technologies, which are opaque for the details of the upper layers of the protocol stack and devoid of service control capabilities. While these technologies can determine source and destination IP addresses and TCP ports of each packet, they could hardly determine the behaviour of the application, the user, the content, or other aspects of the upper layer protocols and applications. As a result, a NGN and Ipv4/v6 service provider hires an opaque or black broadband pipe at a cheaper price, it is likely that subscribers will change to rent upper value-added services with content awareness from other Internet content providers. **This is an insufferable problem for network service providers that the more investments in their broadband infrastructure, the less return from the service income.***

The better method to address this issue is to change an opaque and black broadband pipe into a transparent broadband pipe, which provides service providers visibility using the networks, traffics and applications, visibility implementing service management and control. This offers network operators complete visibility of network applications, flexible traffic control through the real-time comparison and string matching between the particular overhead or contents octets of the packet flows and a set of the octets predefined rules. »

Outre le fait que cette déclaration de l'ITU pose clairement le problème de sa gouvernance, elle démontre sans ambiguïté que l'objectif des opérateurs est bien d'essayer de s'extirper de leur statut de 'dumb piper' en centralisant des 'services d'intelligence' au cœur même de leurs infrastructures de routage, et ce afin d'augmenter leurs gains, par le biais de la facturation de services différenciés -ou discriminés-.

La gestion du trafic, basée sur une classification des contenus échangés, leur permettrait ainsi de vendre de la 'qualité de services' (QoS) aux utilisateurs, alors qu'aujourd'hui le trafic est acheminé au mieux, en 'best effort'.

Le problème est donc de vendre cette QoS, et pour cela, il faut qu'elle soit perceptible par les utilisateurs. Or , [comme le fait remarquer XiPeng Xiao](#) : « *In the developed regions where the selling of QoS is intended, CoS may not be able to create much user-perceivable differentiation under normal networks conditions- Best Effort itself is already good enough. This is somewhat intuitive because if there is no congestion in a network, the DiffServ CoS won't be that useful. While CoS may be useful in developing regions where capacity is in shortage, selling of QoS in those regions may not be a profitable undertaking.*»

D'où sans doute la menace d'une congestion des réseaux -en raison des contenus vidéos- constamment exposée au législateur par les fabricants de routeurs : Dès lors que la congestion menacerait, la QoS deviendrait indispensable, et le best effort ne serait plus un modèle viable.





Pour autant, face à de tels arguments techniques, le bon sens permet de remarquer que :

1 : Depuis les débuts de l'internet, le besoin total de débit des utilisateurs ne fait qu'augmenter, et les opérateurs ont toujours augmenté le débit disponible pour y faire face : et aujourd'hui, soudainement, cette adaptation de la bande passante de l'infrastructure à la demande ne serait plus possible? Pour quelle raison? Si ce n'est de justifier la QoS vis à vis du public et du législateur par un argument technique ad verecundiam...

2 : A supposer que les opérateurs investissent dans une infrastructure de routage capable de gérer la QoS, et que cela permette à cet instant d'éviter la saturation des réseaux : la demande de débit continuant à augmenter (pour quelle raison cesserait-elle soudainement de le faire?), si les opérateurs ne font pas d'efforts pour augmenter leur capacité (le 'diamètre de leurs tuyaux') alors la saturation arrivera de toutes façons. La QoS ne peut pas faire de miracles : Les lois de la physique étant ce qu'elles sont, QoS ou pas, il est impossible de faire rentrer 2Tb/s de débit utilisateurs dans le tuyau 1Tb/s d'un opérateur... En bref : la QoS ne permet que de retarder l'investissement inéluctable dans une augmentation de capacité des réseaux.

Dès lors, quel est l'intérêt de la QoS? Pour les fabricants de routeurs, il est évident : vendre des machines complexes et coûteuses. Pour les opérateurs, c'est moins évident : ils investissent à la fois dans des routeurs 'intelligents', et puis, inéluctablement, dans les tuyaux. Cela étant, ce faisant, ils peuvent augmenter leurs gains via la vente de QoS. Quant aux utilisateurs, ils paieront in fine leur accès plus cher -et ce, de façon pérenne-, puisque tel est bien le modèle que les opérateurs veulent instaurer via une mutation NGN. De fait, la gestion de trafic n'est pas une solution à un problème technique : elle permet juste de la facturation. Face à cette évidence, certains avancent des arguments extrêmes, en citant par exemple le cas de la téléchirurgie : est-il bien raisonnable d'envisager d'utiliser le réseau IP pour de telles applications vitales? Les patients potentiels en jugeraient certainement par eux-mêmes si d'aventure ils se retrouvaient un jour face à une telle proposition.

Une première discrimination est donc celle découlant de l'augmentation du coût de l'abonnement qui ne peut qu'accroître des inégalités d'accès à la société de l'information : Or cet accès est devenu tellement important socialement que la question de l'inscrire en tant que droit dans les constitutions est désormais légitimement posée.

La gestion de trafic, permettant de vendre de la QoS, grâce à une classification des services fait craindre -légitimement- de possibles discriminations, et, partant, de possibles atteintes à la liberté d'information : ce problème est au centre des débats sur la neutralité, le questionnaire de la Commission s'inscrivant dans cette perspective.

Pour autant, c'est l'arbre qui cache la forêt. La question -certes technique- qu'il faut poser est : Comment les opérateurs envisagent-ils la classification des contenus échangés par les utilisateurs ou des services qu'ils utilisent?

Techniquement : en utilisant des procédés de Deep Packet Inspection (DPI), c'est à dire en ouvrant les paquets IP pour en lire le contenu. Cette inspection est très exactement analogue à l'ouverture d'une lettre par la poste : c'est un viol du secret des correspondances. Que ce dernier soit effectué par une machine ou par un humain n'y change rien : dans une démocratie, le contenu des communications échangées entre une source et un destinataire n'a pas à être lu par un postier ou un opérateur, dont le seul rôle est l'acheminement.

Le secret des correspondances doit être respecté et clairement garanti par la loi, et si un doute persiste sur l'interprétation des textes existants quant à leur application à Internet, alors le législateur doit y remédier.





Qui plus est, cela devrait être fait rapidement : un certain nombre d'études ont été publiées, conseillant au législateur de prendre son temps pour réguler, et de procéder par étapes, sur plusieurs années. La manœuvre qui se cache derrière ces conseils aux régulateurs est limpide : il s'agit pour les opérateurs et les fabricants de routeurs de gagner le plus de temps possible afin de permettre le déploiement généralisé d'une infrastructure NGN utilisant ces techniques de DPI, et de placer le public et le législateur devant le fait accompli, sans pratiquement aucune possibilité de retour arrière.

Par ailleurs, le niveau d'intrusion dans les contenus échangés n'a pratiquement aucune limite : même dans le cas où les échanges sont cryptés, il est possible d'identifier les activités des utilisateurs par la mise en évidence statistique de patterns comportementaux.

Certains minimisent la menace en avançant le fait que les routeurs DPI n'ont à l'heure actuelle pas assez de puissance de calcul pour effectuer ces opérations de DPI sur des lignes à 1Tb/s : il est simplement évident que leur puissance de calcul va augmenter.

Une fois comprise -et actée dans la loi- l'impossibilité de faire de la classification de services par DPI dans une démocratie, le problème de la neutralité du Net est grandement simplifié : n'ayant plus accès qu'aux headers des paquets IP, la seule discrimination qui pourrait se faire serait sur les adresses IP. Une telle discrimination semble à peu près impensable tant elle serait flagrante et arbitraire, en sus d'être sans doute illégale. Mais là encore, si le moindre doute d'interprétation subsiste, alors le législateur doit intervenir pour lever toute ambiguïté.

Cela étant, la QoS pourrait présenter un intérêt pour l'utilisateur, qui resterait d'ailleurs à quantifier précisément pour en estimer la pertinence. (D'où l'expression QoE : quality of 'experience', et, en toute logique, l'intérêt pour les opérateurs de maintenir constamment la juste quantité de saturation nécessaire pour pouvoir faire 'sentir' le gain de la QoS à leurs abonnés, et ainsi justifier sa facturation.) Quoi qu'il en soit, la seule solution QoS respectueuse du secret des correspondances est que ce soit l'utilisateur lui-même -ou l'application qu'il utilise- qui indique le type de service qu'il utilise, ou plus précisément quelle combinaison de préférences (packet loss/latency/jitter) est la plus adaptée à son usage à un instant donné. Dans cette configuration, les fournisseurs d'accès n'ont pas à ouvrir le contenu des paquets pour ensuite les taguer, puisque l'utilisateur tague lui-même ses paquets, qui plus est avec le strict minimum nécessaire à une prise en compte de ses besoins réels.

Alors les fournisseurs d'accès pourraient être tentés, même dans cette configuration, de proposer des offres segmentées, par options. D'une part cela n'aurait sans doute pas trop d'intérêt au vu de la diversité des usages familiaux, qui plus est si l'on tient compte du coût du système de gestion et de facturation, et d'autre part, cela aurait sans doute le même effet que celui constaté avec la « jungle » des offres de téléphonie mobile : au total, des prix élevés cachés dans des offres inextricables ne permettant pas au consommateur de visualiser la moindre concurrence. Ce type de segmentation avait été envisagé en France, avant d'être abandonné face au rejet des abonnés.

Que l'accès soit en best effort, ou managé -dans la configuration décrite ci-dessus-, le plus raisonnable est sans doute de rester sur des forfaits illimités tarifés au débit. Quant à l'idée d'imposer des quotas de volumes de données, elle a déjà été rejetée par les consommateurs français il y a plusieurs années.

Concernant les problèmes de convergence sur un cœur de réseau IP : d'une façon générale, tout ce qui précède vaut tant pour les accès fixes, que pour les accès mobiles. D'autre part, il est aussi évident que de plus en plus les opérateurs utiliseront le même réseau pour offrir de l'accès internet et d'autres services. Il est à craindre que ces opérateurs affectent de plus en plus la bande passante de leur réseau à ces autres services, au détriment de l'accès internet : la Loi devra donc imposer à ces fournisseurs d'accès de garantir par contrat un débit internet minimum clairement indiqué, pour





prévenir toute dérive dans l'allocation de leur bande passante globale.

Enfin, le questionnaire de la Commission mentionne un autre éventuel objectif de la gestion de trafic : « *In future, traffic may also be managed to ensure that legal obligations are met in some Member States, particularly for example with regard to illegal content.* » Comme nous l'avons rappelé dans [notre réponse](#) au [questionnaire](#) relatif à la Neutralité du Net proposé par la Secrétaire d'Etat française chargée de la Prospective et du Développement de l'économie numérique, cette référence au 'legal content' provient directement du [premier des quatre principes](#) proposés par Michael Powell début 2004 et censés palier la dérégulation spécifique aux Etats-Unis en guidant la politique de la FCC : « *Freedom to Access Content. First, consumers should have access to their choice of legal content.* » Cette restriction de ce principe de liberté d'accès a généré en France un débat sur la 'Quasi-neutralité':

En effet, c'est au juge qu'il revient d'apprécier la licéité d'un contenu, et pas à un intermédiaire technique. Ce principe fondamental a été au centre des débats lors de la transposition en droit français de la directive 2000/31CE concernant la responsabilité des hébergeurs, à qui l'on demandait de juger de la licéité d'un contenu, et, le cas échéant, de le supprimer. Cette obligation de jugement imposée aux hébergeurs français est mise en évidence par la rédaction même de [l'article 6 de la Loi n°2004-575](#) du 21 juin 2004 pour la confiance dans l'économie numérique :

« 5. La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants [...]»

« 2. Les personnes physiques ou morales qui [...]le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère[...] »

« 3. Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible. »

Le glissement sémantique de 'litigieux' à 'illicite' démontre que ce sont des faits 'litigieux' qui sont signalés à l'hébergeur, et en revanche sa responsabilité peut-être engagée pour des faits 'illicites', qu'il lui revient donc de juger. Cette rédaction a été recadrée par le conseil constitutionnel par le considérant 9 de la [décision n° 2004-496 DC du 10 juin 2004](#) , limitant sa portée aux contenus 'manifestement' illicites, à savoir : uniquement les contenus à caractère pédopornographique, révisionniste, ou xénophobe.

S'agissant de gestion de trafic, il est évident que le terme 'legal content' concerne les fournisseurs d'accès : or, on ne peut pas plus demander aux fournisseurs d'accès de se substituer au juge, et de juger la licéité des contenus qu'ils acheminent. Si le volume de données stockées par les hébergeurs est énorme, celui des données acheminées par les fournisseurs d'accès l'est encore plus : Il est simplement irréaliste d'envisager d'exiger d'eux qu'ils surveillent les flux de contenus, et encore plus de penser que la justice pourrait caractériser leur licéité.

Et c'est bien ce qu'affirme l'article 15 de la [directive 2000/31](#) : « [...] Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12[FAI/mere conduit], 13[キャッシング] et 14[hébergeurs], une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. »

L'article 15 restreint ainsi la portée éventuelle du principe d'un accès libre aux contenus légaux : Que reste-t-il donc de la restriction de ce premier principe de Powell? La prise en compte des contenus





déjà jugés illicites par l'autorité judiciaire. En pratique cela mène à la possibilité de demander aux fournisseurs d'accès de filtrer ces contenus déjà jugés.

Concrètement si un contenu hébergé dans un pays est jugé illicite, il suffit au juge d'en demander le retrait à son hébergeur. Nul besoin donc d'impliquer un fournisseur d'accès exerçant son activité sur son territoire. Le seul cas où il serait envisageable de l'impliquer serait celui d'un contenu hébergé à l'étranger.

Ironiquement, cette interprétation du premier principe de Powell se retourne contre le premier amendement de la constitution de son propre pays. Si la France demande à ses fournisseurs d'accès de filtrer des contenus publiés en toute légalité aux Etats-Unis par un citoyen américain, alors cela porte atteinte à la liberté d'expression de ce citoyen qui se retrouve en quelque sorte bâillonné sélectivement vis à vis de l'ensemble des citoyens français. Et par ailleurs cela porte atteinte à la liberté d'information (pas d'expression) des internautes français.

Demander aux fournisseurs d'accès de filtrer repose sur une erreur d'analyse, sur la confusion entre le droit de dire dans un pays donné, et le droit de lire ce qui est dit -légalement- dans ce pays depuis tous les autres pays.

Cependant, le premier principe de Powell peut aussi être interprété à l'inverse : si un contenu est hébergé légalement aux Etats-Unis, alors tous les internautes peuvent y accéder librement, y compris les français.

Cette approche par les quatre principes, initialement proposés pour tenter de contourner un problème de régulation interne aux Etats-Unis, s'avère donc au moins partiellement inadaptée.

Il semble plus efficace d'aborder le problème séquentiellement par sa base réelle et concrète :

La mutation NGN proposée est basée sur une classification par DPI.

Ce procédé de classification ne respecte pas le secret des correspondances.

Si un doute d'interprétation subsiste, alors la loi doit clairement et spécifiquement l'interdire.

Partant de là seule une discrimination sur les adresses IP reste techniquement possible.

Au besoin les lois prohibant cette non-neutralité flagrante devraient être explicitées.

Comme le remarque le [récent rapport de l'ARCEP](#) dans sa 4ème proposition, un risque menace le débit effectif des accès internet : Le développement de services autres que (et en sus de) l'accès internet par des opérateurs sur leurs réseaux nécessite donc de protéger par la loi le débit minimum garanti des offres d'accès, puisque le débit maximum des offres commerciales aura de moins en moins de sens.

Paris, France,
le 30 septembre 2010.
La Ligue ODEBI
<http://www.odebi.org>

