**Fédération des fournisseurs d'accès à Internet associatifs**
(dite « Fédération FDN »)
FFDN — 16, rue de Cachy — 80 090 Amiens
Déclarée en préfecture de la Somme — W751210904

# Réponse à l'occasion de la réunion avec le BEREC à propos de neutralité du Net à Bruxelles

Fédération FDN & La Quadrature du Net

14 Mars 2017

Ce document développe les arguments principaux que nous avons soumis lors d'une réunion avec le BEREC et d'autres acteurs de la société civile à Bruxelles. Il est organisé en sujets, dans l'ordre dans lequel ils ont été discutés lors de la réunion.

## 1 Présentation

La « Fédération des fournisseurs d'accès à Internet associatifs », également nommée « Fédération FDN » [1], est un rassemblement de 30 fournisseurs d'accès à Internet à but non-lucratif, principalement en France.

Chacun de ces fournisseurs d'accès à Internet est géré par ses abonnés. Chacun est par ailleurs déclaré comme opérateur au régulateur compétent. Nos opérateurs sont principalement établis en France, y compris dans les territoires d'Outre-Mer, et l'un est sis en Belgique.

Le travail de la Fédération elle-même est effectué par ses utilisateurs, toutes les actions sont accomplies par des bénévoles, y compris le présent document. Bien qu'il soit rédigé par des bénévoles, ce n'est pas pour autant qu'il ne contienne pas une réelle expertise du marché des télécommunications en France ou en Europe. Nos organisations sont anciennes (à l'échelle de l'histoire de l'Internet), et nous travaillons sur ces sujets depuis des années. En France, les positions de la Fédération FDN sur les sujets tels que la neutralité du Net sont considérées comme sérieuses, bien argumentées et ont l'oreille des dirigeants. Nous n'agissons d'habitude pas au niveau européen parce qu'il est relativement difficile pour les bénévoles d'être présents à Riga, Vienne, Londres et Bruxelles sans financement significatif.

La Quadrature du Net, organisation de défense des droits et libertés fondamentales à l'ère du numérique, travaille avec nous sur ce sujet et sur le présent document. La Quadrature est active au niveau européen depuis 2008. Ses activités sont concentrées

[1] En référence à FDN, « French Data Network », un fournisseur d'accès à Internet à but non lucratif fondé en 1992, le plus ancien fournisseur d'accès à Internet encore actif en France, et à l'origine de la Fédération.

sur l'implication des citoyens dans la défense de leurs droits et libertés. L'organisation produit des analyses de textes juridiques, aide les citoyens à les comprendre, et développe des outils pour aider les citoyens à agir, par exemple, en assurant le suivi des votes exprimés par les députés européens.

## 2 Sujet 1 – Méthodes de mesure/applications individuelles

Nous avons notre lecture ainsi qu'une compréhension propre sur la question de « la surveillance rapprochée ».

En premier lieu, ceci ne peut pas signifier une surveillance permanente du réseau et sans objectif défini. Il en va de même pour la surveillance globale du réseau et, bien entendu, pour tout ce qui concerne un individu spécifique. Toute récolte systématique de données sur la qualité, le débit ou l'état opérationnel de l'accès Internet d'un utilisateur final doit être considérée comme attentatoire à la vie privée : *il s'agit bien* de données personnelles. Même avec son consentement : il est bien connu que le consentement de l'utilisateur s'obtient systématiquement et sans lecture des conditions générales d'utilisation. Certaines mesures systématiques ont une valeur en tant qu'information générale, mais aucune ne devrait, en aucun cas, être utilisée pour attenter au respect de la vie privée d'un citoyen.

Nous pensons que des mesures précises, régulièrement mises en place sont attentatoires à la société démocratique, même si la mesure repose sur le consentement.

Ces mesures globales sont déjà en place, en tout cas en France. Elles pourraient être améliorées par plusieurs ajouts : la connaissance des interconnexions entre les réseaux des grands opérateurs (les fournisseurs d'accès à Internet, les CAP et les CDN, qui exploitent tous des réseaux), des règles afin de décider si un accord d'interconnexion est autorisé, des niveaux de saturation de ces interconnexions, ou de la difficulté de les renforcer. À notre avis, la mise en œuvre est à ce jour insuffisante. Cette information fournit une vision claire des opérateurs qui abusent de leur position pour des bénéfices indus.

Par exemple, si tous les abonnés d'un FAI veulent accéder à une plateforme vidéo donnée, il semble raisonnable que la plateforme vidéo en question augmente sa capacité, investisse dans davantage de serveurs, dans de plus grandes capacités réseau, dans davantage de production de contenu, etc. De même, il apparaît légitime que les FAI investissent dans le renforcement de l'interconnexion vers le contenu que ses abonnés désirent, puisque c'est précisément ce pour quoi ils payent. S'il ne fournit pas une bonne interconnexion vers les sevices que ses clients désirent utiliser, l'opérateur ne peut pas être considéré comme un « fournisseur d'accès à Internet », mais seulement comme un « opérateur de boucle locale ». Le consommateur doit alors se connecter, par le truchement de cet accès local, à un véritable fournisseur d'accès à Internet. La façon typique de le réaliser est de passer par un Réseau Privé Virtuel (VPN) qui donne accès au contenu par une connexion encapsulée.

La surveillance globale des interconnexions permet aux autorités de régulation d'obtenir une vision claire des dynamiques du marché et d'identifier tout à la fois ceux des opérateurs qui mettent de la bonne volonté à renforcer leur interconnexion, et ceux qui y rechignent.

Pour ce qui est des services individuels, nous ne pensons pas qu'il soit raisonnable d'en établir une surveillance systématique. Ce concept repose sur l'idée que la qualité de toutes les connexions est mesurée en permanence et que si la qualité chute, c'est révélateur d'un problème. Nous pensons que la question doit se poser dans l'autre sens. Il faut en premier lieu détecter la survenance d'un incident, plutôt que de mesurer la qualité. Et lorsqu'un incident est détecté, alors la mesure de qualité peut s'utiliser pour extraire l'information utile à sa résolution.

Pour cette détection, une plateforme ouverte de récolte de rapports individuels, comme RespectMyNet (RMN, `respectmynet.eu`), est pertinente. Cela permet de récolter l'information rapidement et de réagir aux rapports d'incidents. Les campagnes de promotions de ces sites de crowd-sourcing peuvent aider à faire détecter les incidents par des individus non-spécialistes des réseaux. Des campagnes aussi simples que « Vous pouvez accéder au service pendant l'après-midi mais avec moins de fiabilité en soirée ? Signalez-le ! ». Un autre point important de la détection est que, généralement, la violation est annoncée publiquement par celui qui la commet. Les opérateurs **en assurent la publicité** ! En utilisant de gros panneaux de publicité, ils clament un peu partout qu'ils proposent une offre d'accès spécifique à une plateforme donnée ou à une autre. Dernier point, mais non des moindres, lorsque les violations ne sont pas reconnues, par exemple lorsqu'une interconnexion est en surcharge tous les soirs, le problème devient typiquement de notoriété publique et chacun en est informé. De nombreux rapports sont reçus sur des plateformes publiques telles que RMN.

La mesure réelle de la qualité peut commencer dès lors que le problème est détecté, afin d'essayer d'y trouver un remède. La nature exacte de la mesure peut varier (bande passante, latence, gigue, mise en cache DNS, perte de paquets, etc.). Mais l'idée est qu'une fois qu'il y a suspicion, des mesures intelligentes et efficaces sont possibles. Ces mesures peuvent être mises en place par des sondes installées volontairement par des utilisateurs : qu'il s'agisse de ceux qui ont remonté le problème ou simplement des utilisateurs de bonne volonté non impliqués dans cette remontée. Il est ensuite aisé de rassembler toutes les informations collectées en un tout cohérent et facile à interpréter.

Si, au même moment, un service est fluide pour les abonnés d'un opérateur A, lent pour les abonnés d'un opérateur B mais pas si ces mêmes abonnés utilisent un réseau virtuel privé pour router leur trafic sur un autre chemin, alors il y a un problème d'interconnexion.

Les données brutes collectées durant les mesures, faites à partir de lignes individuelles, ne devraient **jamais** être publiées telles quelles. De telles données brutes contiennent des informations personnelles et doivent être sujettes aux règles sur la protection des données. La collecte de données, leur traitement et leur rétention, doivent être faits dans le respect du Règlement général sur la protection des données (RGPD) sous le contrôle étroit des autorités de régulation nationales et de protection des données. Seuls

les résultats agrégés des mesures doivent être publiés. Cela signifie de ne publier que les valeurs clés, sans possibilité aucune de remonter à un comportement individuel. De plus, les rapports d'enquête doivent probablement être toujours publiés : une enquête a été conduite sur une possible violation dans un cas particulier et sa divulgation est d'intérêt public, même s'il a été conclu qu'il n'y a pas eu violation.

Le type de mesures qui peuvent être utiles dans ce contexte ont déjà été exposées :

- mesures identiques réalisées depuis des emplacements différents (même opérateur ou pas, à travers un réseau virtuel privé ou pas, etc.) ;
- mesures identiques faites à des instants différents (durant la nuit, le soir, le jour, etc.) ;
- latence, vitesse, perte de paquets, afin d'en déduire la qualité perçue du réseau global ;
- qualité d'expérience (QoE) (p. ex. fluidité du streaming vidéo, fluidité d'un téléchargement d'une page HTML, etc.) ;
- etc.

# 3 Sujet 2 – Méthodes de mesure / IAS comme un tout

Le but essentiel de cette mesure est de garantir que la publicité commerciale procure une information précise sur la bande passante maximale pour un abonné donné. Les problèmes de neutralité du Net sont secondaires pour ce problème. Le but est d'éviter des publicités offrant « jusqu'à 30Mb/s » alors que votre accès à Internet ne vous permet qu'un débit de 0.5Mb/s. Pour les technologies anciennes, comme le xDSL, la bande passante est directement, physiquement, restreinte par la ligne téléphonique elle-même ; et parfois à un point de concentration plus haut dans le réseau. Pour les technologies récentes comme la fibre, la ligne n'est plus un goulot d'étranglement.

Parmi les tests actuellement disponibles, SpeedTest, le plus largement utilisé, est biaisé. Presque tous les grands fournisseurs d'accès à Internet en Europe ont passé un accord avec SpeedTest pour qu'il héberge quelques uns de leurs serveurs. En conséquence, un utilisateur final ne teste sa vitesse de connexion qu'au réseau de son fournisseur d'accès. Ce biais est acceptable dans le contexte de cette section. La vitesse mesurée n'est pas réellement en rapport avec la bande passante pour chaque accès à Internet fourni par le fournisseur d'accès. Mais il s'agit là d'une mesure correcte des caractéristiques de la ligne de l'abonné, à comparer à celles des lignes des autres abonnés.

Cela peut aussi être une mesure intéressante dans les investigations de neutralité du Net. Par exemple, l'abonné dispose de 20 Mb/s selon une mesure de type SpeedTest, mais il ne peut accéder à une plateforme vidéo dans de bonnes conditions, tandis que d'autres abonnés à d'autres fournisseurs d'accès avec des résultats de mesure du type

SpeedTest similaires, y accèdent dans de bonnes conditions. Le problème n'est alors pas en relation avec sa ligne, mais avec quelque chose dans le réseau entre son opérateur et la plateforme vidéo : probablement l'interconnexion.

Une mesure plus technique qui évite les divers facteurs environnementaux peut servir d'outil de diagnostic pour l'opérateur mais pas pour les objectifs poursuivis par le BEREC. Du point de vue de la réglementation, une mesure unique mauvaise peut être due à un WiFi de mauvaise qualité et ne suffit pas à mettre en évidence un problème systémique de neutralité ou de capacité du réseau. Bien sûr, les fournisseurs d'accès peuvent utiliser de tels outils diagnostiquer des problèmes rencontrés par leurs abonnés, mais le BEREC ne doit prendre en considération que les valeurs relatives entre des abonnés moyens sur des lignes moyennes. Pour ce sujet, les facteurs environnementaux sont dissous dans la moyenne : chaque fournisseur a sa part d'abonnés avec un WIFI de mauvaise qualité. Si un facteur environnemental crée une réelle différence sur une mesure moyenne, le facteur est alors probablement créé par le fournisseur (p. ex. en fournissant un WIFI de très mauvaise qualité dans le routeur qu'il loue ou vend à ses abonnés).

Nous aimerions insister sur le fait que tout ne peut être mesuré. Certaines violations de la neutralité du Net sont tout simplement décidées dans les contrats passés avec les utilisateurs finals. Certaines dispositions de tels contrats ne respectent pas la régulation pour un Internet ouvert. Il ne semble pas que rendre les termes de leur contrat, ainsi que la loi, *intelligibles* aux utilisateurs finals soit un objectif réalisable. Mis à part ceux qui connaissent la loi, ils n'auront *pas* une attitude proactive pour rapporter les violations de neutralité liées à leur contrat.

Quelques fournisseurs d'accès au sein de l'UE violent déjà la neutralité du Net, non seulement par des mesures techniques qu'ils ont adoptées, mais aussi par des contrats qui ne respectent pas la régulation et ils continueront à le faire tant qu'ils seront en position de force.

# 4 Sujet 3 – Considérations pratiques concernant la mise en œuvre des systèmes de mesure de qualité de service

Nous considérons ici que le point clé est de protéger la vie privée. Ces instruments de mesure collecteront des données sur le comportement d'individus dans certaines circonstances. D'autres aspects sont également importants, mais celui-ci doit être considéré comme étant le plus important.

Techniquement, ces mesures sont sans valeur si la méthode de mesure n'est pas correctement documentée d'un point de vue scientifique. Par conséquent, selon nous, il est nécessaire que ces outils soient des logiciels libres (et pas seulement open source). Le logiciel libre garantit trois avantages majeurs : l'outil sera utilisable sur tous les équipements terminaux, il sera pertinent, et il aura la confiance des utilisateurs finals.

Se contenter d'ouvrir le code source aura pour effet que certaines personnes y jetteront peut-être un coup d'œil, mais ils ne pourront rien faire en pratique, ce qui conduira à de mauvais résultats. Permettre aux gens de voir le code et de le modifier garantit que l'ouverture du code soit utile. Encourager une communauté en autorisant le retour d'expérience et la contribution au code de l'outil signifie qu'il reste pertinent et à jour : si une nouvelle violation est découverte, les gens peuvent proposer aux autorités de régulation un outil de mesure qui teste cette violation.

C'est aussi la seule manière de garantir que l'outil restera disponible sur tout type d'équipement terminal. La régulation déclare que l'utilisateur peut utiliser l'équipement terminal de son choix. En conséquence, les outils utilisés par les autorités de régulation et par le BEREC ne peuvent pas créer de discrimination entre ces équipements. Pour ces raisons, l'outil de mesure doit être un logiciel libre : open source de sorte que la description exacte de la mécanique de mesure soit publique ; librement adaptable à tout équipement terminal ; librement distribuable pour qu'il soit disponible pour l'utilisateur final dans n'importe quel dépôt logiciel. Un logiciel qui serait seulement open source ne serait pas disponible partout (la plupart des distributions de Linux, les téléphones mobiles Replicant.us, les téléphones CyanogenMod, etc.).

Un autre aspect à considérer est la confiance. Un outil de mesure qui est installé sur l'ordinateur d'un utilisateur final doit être un logiciel en lequel l'utilisateur a confiance. Si ce n'est pas le cas, il ne l'installera pas. Le logiciel libre permet que : chacun puisse voir le code source, les utilisateurs capables de comprendre ce code puissent expliquer ce que fait l'outil et s'attaquer aux problèmes de sécurité ou aux comportements indésirables. Être en mesure de vérifier que le code de l'outil n'exerce pas de surveillance ou n'envoie pas de données à un organisme non réputé de confiance est important et contribue à établir la confiance. Si l'utilisateur n'est pas capable de faire cela, il sera réticent à installer et à l'utiliser un outil qui effectue des mesures qu'il ne comprend pas.

Pour chaque programme installé par l'utilisateur final, la sécurité est un point clé. Elle n'est actuellement pas mise en application par les « grosses entreprises du numérique » qui collectent des données avec de mauvaises mesures de sécurité du côté de l'utilisateur final (voir les divers botnets – réseaux de robots déloyaux – construits sur l'loT), ni sur le cœur de la collecte des données (voir les divers rapports de « hacking » dans l'actualité, avec des tas de fuites de données personnelles). Ce projet n'est en aucune manière différent. Mais comme il est géré par une autorité publique, et une autorité impliquée dans le monde du numérique, nous considérons qu'il est nécessaire de faire respecter ces questions de sécurité, avec une prise en considération stricte de la sécurité de l'équipement terminal, de la sécurité de l'utilisateur et du respect de sa vie privée.

Nous pensons qu'une approche modulaire peut être intéressante avec un « outil central » pour rapporter les mesures et divers outils de mesure qui peuvent y être incorporés. Cela rend possible l'ajout régulier de nouveaux modules et que chaque module puisse effectuer les mesures appropriées désirées par les autorités de régulation lorsqu'elles investiguent sur une violation présumée de la neutralité du Net. Cela permet également à l'utilisateur final de désactiver quelques modules lorsqu'il pense que le respect de sa vie privée est menacé. Cela favorise aussi une collaboration productive entre les autorités de réglementation et le reste du monde : les outils globaux étant des

logiciels libres, toute organisation de passionnés d'informatique, ou d'activistes, peut fournir de nouveaux outils et les intégrer au noyau. Cela nécessite que les données soient collectées dans un format ouvert et documenté, associé à une structure documentée (p. ex. une structure JSON documentée), de manière à ce qu'il soit facile d'articuler les nouveaux outils et les nouvelles analyses de données.

Comme ces nouveaux outils doivent être des logiciels libres, chacun sera capable de contribuer et de développer un nouveau module. Cela peut être très utile : dès lors qu'apparaît une nouvelle violation, toute la communauté peut faire équipe et proposer un nouvel outil de détection. De telles contributions peuvent être faites par des initiés : des gens travaillant pour un fournisseur d'accès qui viole la neutralité du Net, et qui, désapprouvant ce qui est fait, peuvent rapporter de façon anonyme la violation ou la technique de violation, procurant ainsi les bases du développement d'un nouvel outil. Le logiciel libre permet ce genre d'actions.

Nous encourageons le BEREC à utiliser ses alliés et à les protéger : le fait de contribuer aux outils et de rapporter les violations doit se faire en toute sécurité pour eux, car ils agissent comme des lanceurs d'alertes.

Nous considérons que toutes les données doivent être publiées. Mais rien ne doit permettre de remonter à l'utilisateur final. Il doit y avoir une documentation claire sur la façon dont les données sont rendues anonymes par le système, et cette documentation doit être sérieusement mise en question. Elle peut devenir une référence sur la manière de collecter des données publiques sur les gens sans mettre en péril le respect de leur vie privée. Il y a probablement sur ce sujet un espace pour un partenariat avec des chercheurs spécialisés et des travaux scientifiques : les données sont-elles réellement anonymes ?

Les mesures globales et structurelles (liens d'interconnexion, sur-capacité du réseau, etc.) sont structurellement anonymes (le respect de la vie privée concerne les humains, pas les entreprises), et doivent être totalement publiques. Les mesures centrées sur l'utilisateur, faites à partir de lignes privées, sont sujettes à l'anonymisation et doivent être publiées sous une forme agrégée.

Au risque d'enfoncer une porte ouverte : les données publiées doivent être structurées et utilisables, disponibles publiquement sans restriction ou enregistrement. Par sous forme de fichier PDF dans un rapport annuel.

# 5 Sujet 4 – Méthodes et outils de surveillance de la neutralité de Net

Nous considérons qu'il existe différentes sortes de violation de la neutralité du Net.

Les violations les plus faciles à détecter sont celles faites sur des bases commerciales. Elles sont écrites dans les contrats, sont généralement affichées sur de grands panneaux publicitaires un peu partout. Les autorités de régulation doivent lire ces contrats, et faire appliquer les règles de la neutralité du Net. Par exemple, le « zero rating » (mais

il y a d'autres exemples), qui devrait être clairement interdit, est, au moins en partie, contrôlé par les règles édictées par le BEREC. Il est de la responsabilité des autorités de régulation de lire les contrats des utilisateurs finals, de vérifier qu'ils sont en accord avec les lignes directrices sur la neutralité du Net et de faire appliquer ces recommandations. Nous considérerons comme un échec de se contenter de stopper la violation sans qu'il n'y ait de sanction, car cela ne constitue pas une incitation pour le fournisseur à mieux se comporter. Le fait que les autorités de régulation puissent avoir des interprétations différentes de la régulation et des lignes directrices du BEREC est un problème. Cela ne permet pas une mise en œuvre harmonisée de la régulation dans tous les pays et laisse place à l'incertitude pour les utilisateurs finals.

La partie complexe est relative aux violations basées sur la technique. La Quadrature et quelques autres ONG développent depuis longtemps un outil que facilite la détection des problèmes concernant l'accès à Internet : Respect My Net (`respectmynet.eu`, RMN). Il a été conçu dès l'origine pour aider les autorités de régulation à identifier les problèmes, au moins tels qu'ils sont perçus pars les utilisateurs finals à travers l'Europe. De tels rapports peuvent être « 200 personnes affirment que leur connexion Internet est mauvaise le soir sur ce service vidéo », « 150 personnes affirment qu'elles ne peuvent pas envoyer des courriels » ou autres.

Le projet permet aux utilisateurs finals de signaler différents types de problèmes rencontrés avec leur connexion, et de « confirmer » des problèmes similaires si quelqu'un a déjà signalé ce qu'ils constatent. Selon nous, ce type de plateforme, disponible à travers toute l'Europe, peut aider les législateurs à pister les rumeurs sur quelque chose qui ne va pas. Si RMN fait apparaître que de nombreuses personnes rencontrent le même problème, il est intéressant de déclencher une mesure ciblée et de publier le résultat de ces enquêtes.

Nous considérons qu'un outil de production participative de rapports pour détecter une violation, couplé à un outil d'usage général de mesures multiples tel que décrit plus haut, peut être un excellent moyen de détection de violations de la neutralité du Net. RMN est un tel outil de production participative. Il est actuellement développé par de petites ONG, presque sans ressources dédiées et évolue lentement. Un partenariat cohérent entre les ONG impliquées, le BEREC ou les autorités de réglementation, peut être une manière d'intégrer cet outil dans un processus plus formel. Comme cet outil est géré en coopération par de nombreuses ONG à travers toute l'Europe, chaque autorité de réglementation a de bonnes chances d'obtenir des rapports des ses utilisateurs locaux dans la bonne langue et par conséquent de créer une meilleure interaction.

Le même outil, développé selon une approche du haut vers le bas, de la Commission, au BEREC, aux autorités de réglementation, etc., serait probablement mois efficace, utiliseraient plus de ressources pour aboutir à un résultat mal adapté aux différences entre les diverses cultures européennes. il semble plus efficace d'avoir une bonne interaction entre les organisations de la société civile qui ont créé l'outil et les autorités de réglementation qui l'utilisent. Les autorités de régulation pourraient, par exemple, fournir les informations sur les types de violations qu'elles aimeraient détecter, ou fournir quelques évolutions de l'outil (en participant à l'effort de localisation par exemple).

Le fait d'avoir une plateforme commune en Europe aidera aussi les différentes autorités de régulation à se coordonner et à comparer leurs situations, au niveau du BEREC.