RAPPORT D'ACTIVITÉ

L'état d'internet en France

ÉDITION 2021

TOME 3

arcep

République française - juillet 2021

RAPPORT D'ACTIVITÉ

L'état d'internet en France

arcep

Sommaire

INTRODUCTION 06

Les faits marquants de l'Arcep 06

Les réseaux pendant la crise sanitaire 10

PARTIE 1 19

ASSURER LE BON FONCTIONNEMENT D'INTERNET

CHAPITRE 1
Améliorer la mesure de la qualité d'internet 20

CHAPITRE 2
Superviser l'interconnexion de données 38

CHAPITRE 3
Accélérer la transition vers IPv6 48

PARTIE 2 70

VEILLER À L'OUVERTURE D'INTERNET

CHAPITRE 4
Garantir la neutralité d'internet 71

CHAPITRE 5
Plateformes, maillons structurants de l'accès à internet 87

PARTIE 3 96

AGIR FACE AU DÉFI ENVIRONNEMENTAL DU NUMÉRIQUE

CHAPITRE 6
Encourager un numérique soutenable 97

LEXIQUE 104

Édito

L'ANNÉE 2020 : ENTRE DÉFIS LIÉS À LA CRISE SANITAIRE ET PERSPECTIVES EN MATIÈRE DE RÉGULATION DES PLATEFORMES



Par Laure de La Raudière,
Présidente de l'Arcep

La crise sanitaire liée à la Covid-19 nous a rappelé à quel point les réseaux d'échanges sont indispensables à la vie du pays, notamment pour la compétitivité, la croissance et l'emploi. De nombreux Français ont aussi découvert de nouveaux usages pendant les confinements : télétravail, télé-éducation, consultations de santé en ligne, visioconférences avec des proches pour maintenir le lien social. Cela illustre la nécessité pour chaque foyer, en tout point du territoire français, de disposer d'une connexion à internet de qualité.

Cette situation exceptionnelle a confirmé combien les réseaux sont et doivent rester un « bien commun » et une « infrastructure de libertés ».

Internet est en effet un espace de liberté : liberté d'expression, de communication, liberté d'accès au savoir et de partage, mais aussi liberté d'entreprendre et d'innover. Parce que le plein exercice de ces libertés est essentiel dans une société ouverte, innovante et démocratique, il est plus que jamais indispensable de garantir qu'internet réponde à des exigences fortes en termes d'accessibilité, d'universalité, de performance, de neutralité, de confiance et de loyauté.

« Les réseaux sont et doivent rester un "bien commun" »

Les principes fondateurs d'internet, et notamment le principe d'égalité de traitement et d'acheminement de tous les flux d'information, quel que soit leur émetteur ou leur destinataire, doivent ainsi perdurer. Le concept de neutralité du net, consacré en Europe au travers du règlement internet ouvert en 2016, est venu donner un cadre juridique garantissant la préservation de ces principes.

Le législateur européen fait désormais peser sur les fournisseurs d'accès à internet (FAI) des obligations que les régulateurs nationaux sont amenés à contrôler et à sanctionner le cas échéant. En France, c'est l'Arcep qui est chargée de sa mise en œuvre, et veille à son respect.

Cependant, si le règlement européen sur l'internet ouvert accorde des droits aux utilisateurs, tels que le droit d'accéder et de diffuser des informations et contenus

en ligne, il ne s'impose qu'aux seuls fournisseurs d'accès (FAI). Situés à une extrémité de la chaîne d'accès à internet, les terminaux (smartphones, assistants vocaux, voitures connectées, etc.) et les écosystèmes fermés des plateformes dites structurantes se révèlent être des maillons faibles de l'ouverture d'internet.

L'Arcep a établi ce constat pour les terminaux dès 2018 et a prolongé cette étude aux plateformes numériques structurantes en 2019. Comme pour les débats sur l'internet ouvert, l'Arcep a aussi mobilisé l'échelon européen, notamment au travers du réseau européen des régulateurs des communications électroniques.

Le travail effectué sur ces sujets a contribué à l'ouverture d'une nouvelle séquence de la régulation du numérique par la Commission européenne qui a publié deux propositions de règlements. Avec le *Digital Services Act*, la Commission propose de réviser la directive Commerce électronique de 2000, notamment le régime de responsabilité à l'égard des contenus hébergés appliqué aux intermédiaires techniques. Au travers du *Digital Markets Act*, la Commission entend mettre en place une régulation économique *ex ante* des grands acteurs du numérique appelés « *gatekeepers* »[1].

La proposition de *Digital Markets Act* est une avancée notable qui mérite cependant d'être renforcée sur plusieurs aspects. Il apparaît nécessaire de mieux considérer la dimension écosystémique de certains acteurs en vue de faciliter une plus grande concurrence, y compris entre les plateformes elles-mêmes. Cette approche permettrait de favoriser la liberté de choix des utilisateurs finaux, parfois captifs d'un écosystème donné.

Il conviendrait aussi de doter le régulateur d'outils proactifs et de renforcer les moyens qui lui sont alloués pour une mise en œuvre efficiente de son intervention *ex ante*. Il s'agirait en particulier de renforcer le dispositif de suivi de ces écosystèmes afin de réduire l'asymétrie d'information et de prévoir des remèdes individualisés plus adaptés qu'une solution « *one size fits all* ». Une plus grande coopération entre la Commission et les États membres apporterait en outre des ressources et appuis déterminants.

L'Arcep, en tant qu'architecte et gardien des réseaux d'échanges en France, continuera à veiller à l'ouverture d'internet et compte également sur la mobilisation de l'ensemble de l'écosystème pour mener à bien cette mission.

« La proposition de *Digital Markets Act* est une avancée notable »

1. Cette dénomination est largement similaire au concept d'opérateur de plateformes numériques structurantes de l'Autorité.

16 JANVIER 2020

Qualité de service d'internet

Le Gouvernement homologue par un arrêté publié au Journal Officiel la décision de l'Arcep n° 2019-1410 relative à la mise en place d'une API « carte d'identité de l'accès » par les opérateurs, marquant ainsi le début du calendrier de déploiement.



LES FAITS MARQUANTS DE L'ARCEP EN 2020

PRINTEMPS 2020

Le suivi des réseaux lors la crise sanitaire

La mobilisation exceptionnelle de l'écosystème d'internet (autorités publiques, opérateurs, fournisseurs de services, utilisateurs finaux, etc.) et les actions entreprises par le Gouvernement et le régulateur ont permis de faire face à des besoins numériques inédits, maîtriser les risques de congestion et veiller au respect de la neutralité du net.



6 AVRIL 2020

Environnement

L'Arcep ajoute des indicateurs environnementaux à sa décision de collecte annuelle (émissions la consommation électrique et les émissions de gaz à effet de serre des activités des opérateurs de communications électroniques). Au sein du BEREC, l'Arcep co-préside un nouveau groupe de travail dédié au développement durable chargé d'étudier l'impact environnemental des télécoms au sens large et d'envisager les pistes permettant de le réduire.



11 JUIN 2020

Environnement

« Pour un numérique soutenable » : L'Arcep lance une plateforme de travail et appelle les acteurs de l'écosystème numérique et de l'environnement à participer aux échanges et à contribuer à l'élaboration d'un premier rapport d'étape. Un premier échange, le 9 juillet 2020, permet de réunir 65 participants et de définir conjointement les points d'attention et le programme de travail.

16 JUIN 2020

Internet ouvert

Le groupe des régulateurs télécom européens, le BEREC, publie les lignes directrices révisées destinées à guider les régulateurs nationaux dans la mise en œuvre du règlement « Internet ouvert », adopté en novembre 2015. En France, c'est l'Arcep qui est chargée de sa mise en œuvre, et veille à son respect par les fournisseurs d'accès à internet (FAI).

7 SEPTEMBRE 2020

Régulation des plateformes

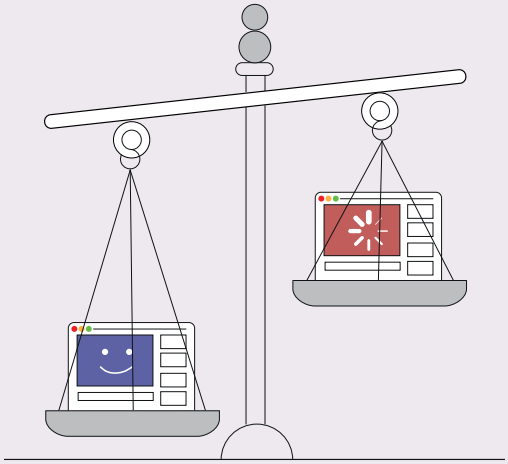
L'Arcep répond à la consultation publique de la Commission européenne sur le *Digital Services Act*. Elle appelle l'Union européenne à se doter d'une régulation *ex ante* des plateformes structurantes et à faire à nouveau d'internet un espace de libre choix et de libre innovation.

14 SEPTEMBRE 2020

Qualité de service d'internet

L'Arcep publie la version 2020 du Code de conduite de la qualité de service d'internet, visant à encourager les outils de mesure en *crowdsourcing* vers encore plus de transparence et de robustesse pour les protocoles de test et les publications des résultats.





15 SEPTEMBRE 2020

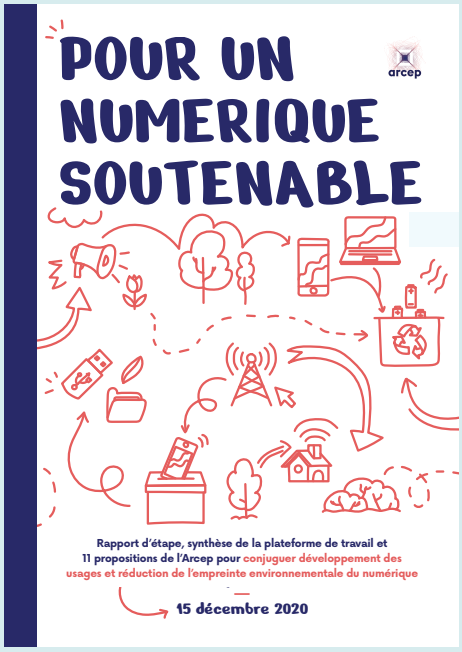
Internet ouvert

Première interprétation par la Cour de Justice de l'Union Européenne du règlement européen relatif à la neutralité du net, dans le cadre d'une question préjudicielle en lien avec une offre de *zero-rating* proposée par un opérateur hongrois.

AUTOMNE 2020

Environnement

« Pour un numérique soutenable » : Entre septembre et novembre 2020, l'Arcep mène cinq ateliers thématiques et deux grandes discussions pour faire dialoguer l'ensemble des parties prenantes sur les sujets numériques et environnementaux afin de recueillir leurs expertises, leurs visions, leurs pratiques et questionnements tant sur les réseaux de communications électroniques, que sur les terminaux, les centres de données ou les usages du numérique.





4 DÉCEMBRE 2020

Transition vers IPv6

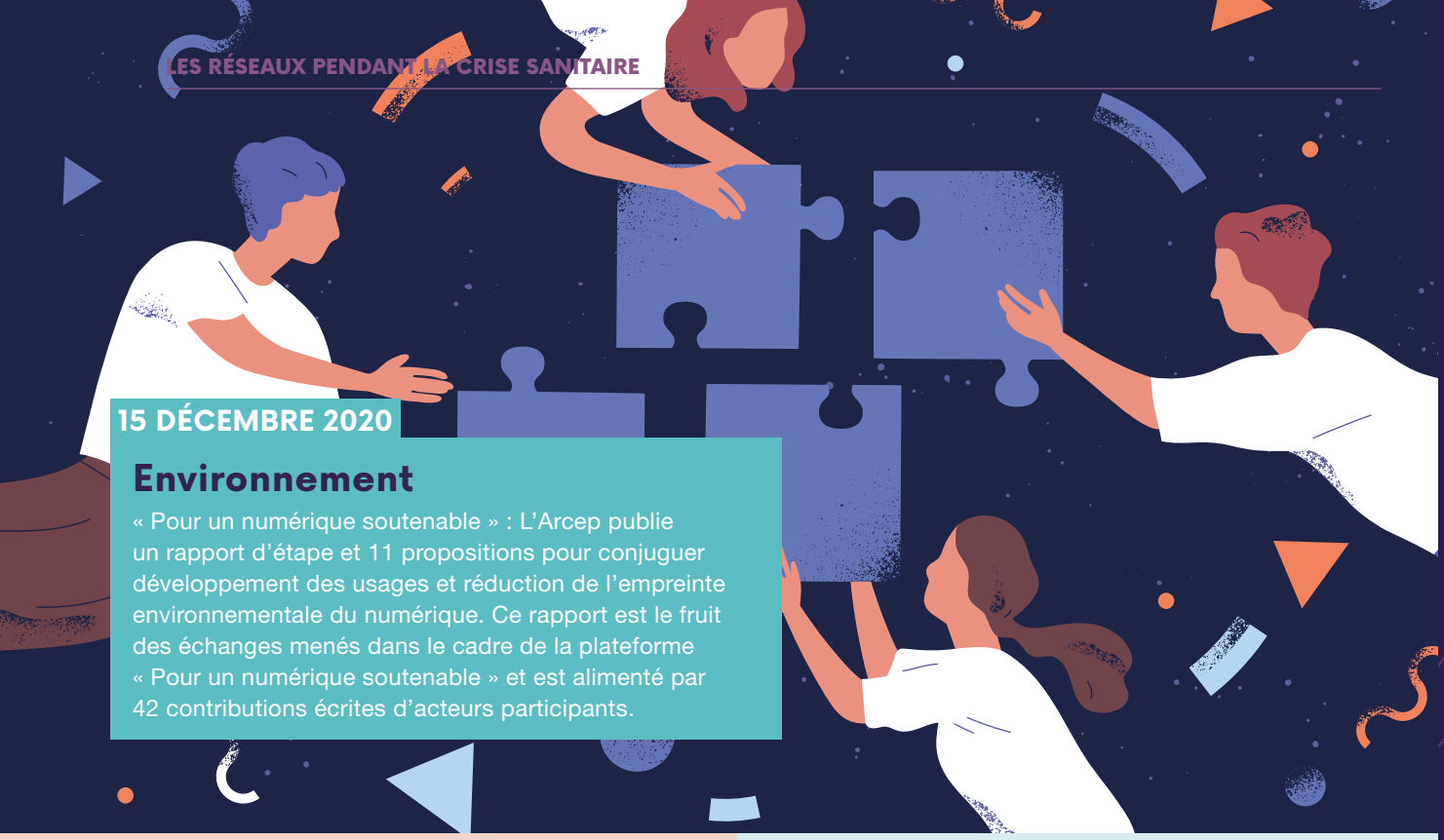
L'Arcep met en ligne l'édition 2020 de son baromètre de la transition vers IPv6, qui signale des progrès significatifs mais encore insuffisants dans la migration vers IPv6. Elle publie également le premier guide de la task-force IPv6 « Entreprises : pourquoi passer à IPv6 ».



8 DÉCEMBRE 2020

Qualité des services mobiles

L'Arcep publie les résultats de sa campagne de mesures 2020 : la qualité de service continue de s'améliorer malgré le contexte sanitaire, les débits descendants atteignent ainsi en moyenne 49 Mbit/s en 2020 contre 45 Mbit/s en 2019 et mettent en ligne les premières cartes de couverture mobile avec une fiabilité moyenne relevée de 95 % à de 98 %.



15 DÉCEMBRE 2020

Environnement

« Pour un numérique soutenable » : L'Arcep publie un rapport d'étape et 11 propositions pour conjuguer développement des usages et réduction de l'empreinte environnementale du numérique. Ce rapport est le fruit des échanges menés dans le cadre de la plateforme « Pour un numérique soutenable » et est alimenté par 42 contributions écrites d'acteurs participants.

15 DÉCEMBRE 2020

Régulation des plateformes

La Commission Européenne publie deux propositions de règlements : le *Digital Services Act* qui révise la directive commerce électronique de 2000 et le *Digital Markets Act* qui vise à mettre en place une régulation économique *ex ante* des grands acteurs du numérique.



21 DÉCEMBRE 2020

Internet ouvert



L'Arcep lance une nouvelle version de Wehe, une application mise à disposition des utilisateurs pour détecter les bridages de flux et de ports internet. L'application est disponible gratuitement en français sous Android, iOS et F-Droid.



FIN 2020

Interconnexion de données

Grâce à la collecte d'information sur l'interconnexion et l'acheminement de données qu'elle réalise, l'Arcep met à jour son baromètre de l'interconnexion de données en France avec les données de 2020.

31 DÉCEMBRE 2020

Transition vers IPv6

L'Arcep introduit une obligation de support d'IPv6 à compter du 31 décembre 2020 sur le réseau mobile des opérateurs qui se sont vus attribuer des fréquences 5G dans la bande 3,4 - 3,8 GHz en France métropolitaine.

LES RÉSEAUX **PENDANT LA CRISE SANITAIRE**

La crise sanitaire de la Covid-19 a eu de nombreux impacts sur les usages des réseaux, en particulier pendant le premier confinement du printemps 2020. Les observations et les principaux enseignements tirés de cette période sont donc principalement centrés sur cette période. L'Arcep se concentre ici sur les thématiques présentées dans le rapport, et n'abordera donc pas, pour importantes qu'elles soient, les questions liées à l'inclusion numérique soulevées dans le cadre de cette crise.

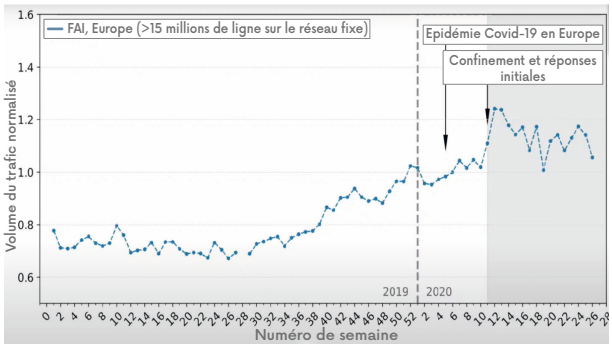
La volumétrie du trafic internet varie, en règle générale, très sensiblement au cours de la journée et en fonction du jour de la semaine. En temps normal en effet, le trafic internet connaît un pic le soir, du fait d'usages relativement consommateurs en bande passante (vidéo notamment), et durant les week-ends. Ce sont ces pics d'utilisation qui déterminent le dimensionnement des réseaux. La crise sanitaire de la Covid-19 a illustré le besoin et la nécessité pour les citoyens français de rester connectés à leur environnement professionnel, personnel et culturel depuis leur domicile. Ce basculement de nombreux usages au sein des foyers a entraîné une forte augmentation du trafic mais aussi une modification importante du profil de trafic. Cette situation a posé un certain nombre de questions sur le fonctionnement d'internet, liées à des thèmes abordés dans ce rapport : Quels ont été les impacts du confinement sur les usages et les réseaux ? Le dimensionnement des réseaux était-il suffisant pour supporter l'augmentation de trafic liée à la crise ? Quels étaient les principaux risques de congestion ? Quelles ont été les bonnes pratiques à adopter pour qu'internet continue à fonctionner ? Comment garantir le respect de la neutralité du net dans cette situation exceptionnelle ?

QUELS ONT ÉTÉ LES IMPACTS DE LA CRISE SANITAIRE ET DU CONFINEMENT SUR LES USAGES ET LES RÉSEAUX ?

La modification des usages a entraîné une très forte augmentation du trafic internet au niveau des fournisseurs d'accès à internet (FAI), avec une hausse d'environ 30 % pendant le premier confinement selon certaines estimations[1,2]. Une augmentation du trafic du même ordre de grandeur est également visible au niveau des points d'échange (IXP). Cela a notamment été observé au niveau des deux points de présence (PoP) à Paris et à Marseille[3] de France-IX, premier point d'échange internet en France.

En ce qui concerne les réseaux mobiles, aucune augmentation notable n'a été observée suite au premier confinement, même si certaines congestions ponctuelles ont pu être observées en France.

ÉVOLUTION DU TRAFIC POUR LES PRINCIPAUX FAI EN EUROPE DURANT LE PREMIER SEMESTRE DE 2020

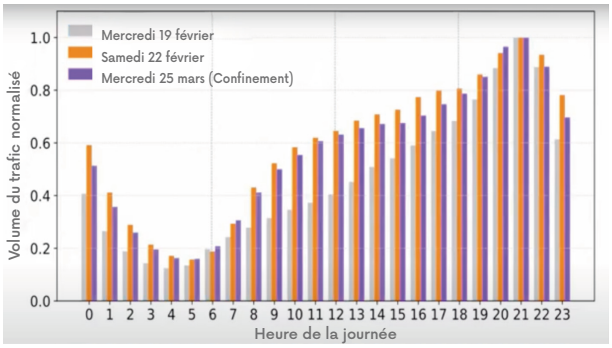


Source : *The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic*

Une modification importante du profil journalier de trafic a par ailleurs été observée : le pic de trafic habituellement constaté en soirée a été « étalé » sur toute la journée. Le profil de trafic en journée ressemblait ainsi davantage au profil de trafic observé pendant les week-ends. Cette modification de profil s'explique par la modification des usages, notamment l'augmentation des visioconférences liées au recours au télétravail, mais aussi une augmentation du *streaming* vidéo et des jeux en ligne, fortement consommateurs en bande passante.

1. Étude Netscout à partir des données des fournisseurs d'accès à internet français.
2. Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, and Georgios Smaragdakis. 2020. *The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic*. In Internet Measurement Conference (IMC '20), October 27–29, 2020, Virtual Event, USA. ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3419394.3423658
3. https://www.franceix.net/en/technical/traffic-statistics/

ÉVOLUTION DU PROFIL JOURNALIER DU TRAFIC



Source : *The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic*

D'après certains outils de *crowdsourcing*, la qualité de service internet (QoS) a connu une légère baisse lors du premier confinement, ce qui pourrait être lié à l'augmentation du trafic et aux quelques congestions ponctuelles observées. En effet, d'après l'observatoire d'Ookla sur l'impact de la pandémie de Covid-19 sur la performance d'internet[4], le débit moyen des mesures effectuées en France sur le réseau fixe est passé de 146,26 Mbit/s au 9 mars 2020 à 126,45 Mbit/s au 13 avril 2020, soit une baisse d'environ 15 %. Cette variation est également observée par nPerf[5] mais est moins visible dans le baromètre annuel 2020 de QoSi[6]. La variation de la QoS est moins visible sur le réseau mobile (environ -5 % entre mars et avril 2020[7]). Le retour à la normale des débits sur les réseaux fixe et mobile a été observé environ 2 mois après, l'impact sur la QoS ayant donc été minimisé sur le long terme.

Une augmentation du volume de tests de QoS effectués par les utilisateurs finaux pendant cette période a aussi été observée, ce qui montre l'utilisation réalisée par les utilisateurs des outils de mesure en *crowdsourcing* en particulier lors d'une baisse de QoS. Ookla a par exemple connu un pic de +77 % de mesures sur le réseau fixe au début du premier confinement en France.

Enfin, une augmentation du taux d'utilisation d'IPv6 a également été observée pendant le premier confinement, ce qui pourrait notamment s'expliquer par l'augmentation du trafic issu des accès grand public, plus fréquemment activés en IPv6 que les accès entreprise (cf. chapitre 3 sur IPv6).

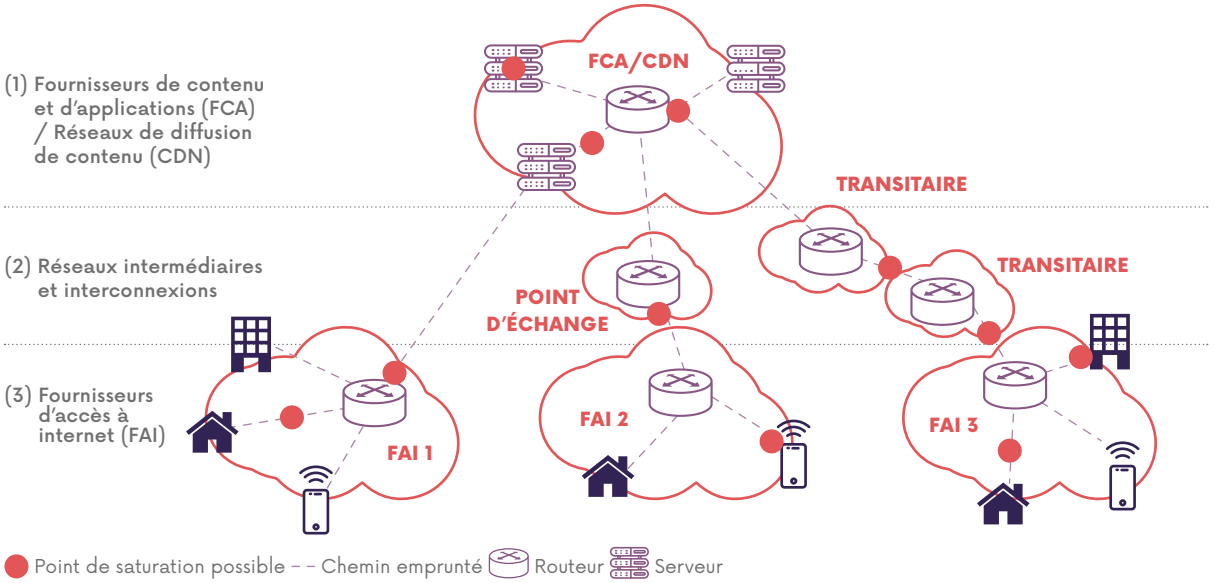
Malgré une augmentation importante des usages et du trafic internet, les réseaux internet fixe et mobile ont montré leur résilience lors du premier confinement.

LE DIMENSIONNEMENT DES RÉSEAUX ÉTAIT-IL SUFFISANT POUR SUPPORTER L'AUGMENTATION DE TRAFIC LIÉE À LA CRISE ? QUELS ÉTAIENT LES PRINCIPAUX RISQUES DE CONGESTION ?

Un utilisateur qui se connecte à internet pour accéder à un contenu ou un service particulier (par exemple navigation web, visioconférence, *streaming* vidéo, téléchargement, etc.) peut faire face à une indisponibilité de ce service ou contenu, voire de plusieurs services à la fois. Cette indisponibilité peut être due à une surcharge au niveau du réseau ou du système d'information d'un maillon de la chaîne technique qui permet d'acheminer le trafic du serveur hébergeant le contenu au terminal de l'utilisateur. Des saturations peuvent parfois survenir au niveau du réseau local (LAN) du domicile de l'utilisateur final, par exemple à cause d'une sursollicitation du Wi-Fi[8]. Au-delà de ces limitations au niveau de l'utilisateur final, cette partie se focalise sur les risques de congestion qui peuvent avoir lieu au niveau des différents acteurs de la chaîne d'internet. D'une façon plus simple, et comme indiqué dans le schéma ci-après, les problèmes de congestion peuvent ainsi survenir à 3 niveaux : au niveau du fournisseur de contenu et d'applications (FCA) ou du réseau de diffusion de contenu (CDN) (1), au niveau des réseaux intermédiaires et interconnexions (2) et au niveau du réseau du fournisseur d'accès à internet (FAI) (3).

4. https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#/France
5. Baromètre des connexions internet fixes en France métropolitaine premier semestre 2020 : https://media.nperf.com/files/publications/FR/2020-07-27_Barometre-connexions-fixes-metropole-nPerf-S1-2020.pdf
6. Étude de la qualité d'expérience des opérateurs mobiles opérateurs mobiles en France métropolitaine 2020 : https://www.5gmark.com/news/2020/Etude_Connectivite_Mobile_France_QoSi_2020_v1.pdf
7. https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#/France
8. Voir partie suivante sur l'optimisation des usages (p. 14).

SCHÉMA SIMPLIFIÉ DES POINTS POSSIBLES DE SATURATION DES RÉSEAUX



Source : Arcep

- Au niveau du FCA/CDN (1), des congestions peuvent tout d'abord se situer au niveau des serveurs, quand un service est bien plus sollicité que normalement. Cette saturation peut être liée à une limitation matérielle (processeur, mémoire, carte réseau, etc.) ou à une limitation logicielle (dépassement du nombre maximum d'utilisateurs simultanés, de fichiers ouverts, de ports TCP ouverts, etc.). De nombreux autres points de congestion sont possibles au niveau du FCA/CDN : les liens, les équipements d'agrégation, de collecte, de *firewall*[9] et de routage peuvent limiter le trafic, si on dépasse leur capacité (physique ou souscrite) en octets par seconde ou paquets par seconde.
- Au niveau des réseaux intermédiaires et des interconnexions (2), des congestions peuvent survenir au niveau des liens s'ils ne sont pas suffisamment dimensionnés par rapport au trafic qui y circule. Cette congestion peut se manifester en général au niveau d'un lien de *peering* privé, d'un lien de *peering* public (au niveau d'un IXP), entre un FCA et un transitaire, entre deux transitaires ou entre un transitaire et un FAI. Selon le point de congestion, la saturation peut impacter un ou plusieurs services et un ou plusieurs acteurs. Les acteurs d'internet prévoient en général un surdimensionnement et une redondance des interconnexions pour faire face à des événements exceptionnels comme les grandes manifestations sportives. La situation liée à la crise de Covid-19 était inédite et a provoqué une montée en charge importante pour les réseaux.
- Au niveau du réseau du FAI (3), des congestions peuvent avoir lieu à différents niveaux : au niveau de l'accès qu'il soit fixe ou mobile, au niveau du réseau de transport/collecte du FAI ou au niveau du cœur du réseau du FAI. En effet, quand un client souscrit une connexion internet fixe, le débit ne lui est pas dédié de bout en bout (hors offre spécifique) : à chaque point du réseau, une capacité plus importante est partagée entre les différents utilisateurs, en partant du principe que tous les utilisateurs n'utilisent pas leur connexion au débit maximum simultanément[10]. Le dimensionnement est aussi réalisé de façon à ne pas saturer, mais une situation inhabituelle peut potentiellement entraîner des congestions. Par ailleurs, des saturations de l'accès internet mobile peuvent survenir au niveau d'une cellule notamment quand plusieurs utilisateurs qui y sont connectés sollicitent des services qui consomment beaucoup de bande passante (*streaming* vidéo, visioconférence, téléchargement, etc.).

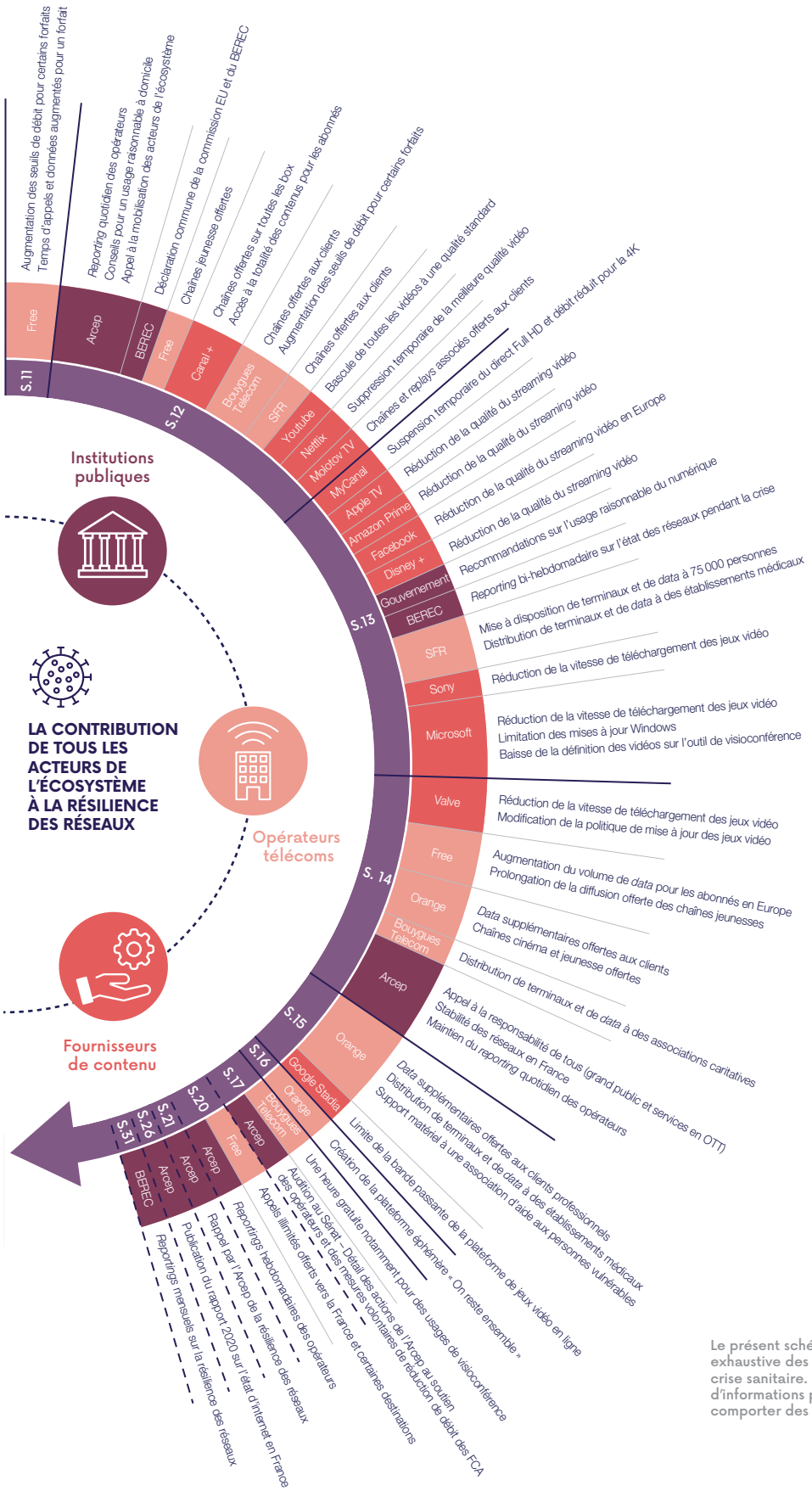
Lors de la crise, des saturations sont apparues au niveau de nombreux fournisseurs de contenu, perturbant l'accès à plusieurs services (services de visioconférences, *e-learning*, etc.). Des tensions très locales sur l'accès à internet mobile ont aussi été constatées ponctuellement.

Au-delà du réseau internet, des congestions peuvent aussi apparaître sur le réseau voix. Cela a été constaté dans les premiers jours de confinement : en effet, la forte augmentation des appels téléphoniques avait entraîné des saturations ponctuelles et temporaires sur le réseau voix. Le redimensionnement des interconnexions concernées par les opérateurs a permis d'améliorer rapidement la situation.

Grâce, d'une part, aux capacités et performances des réseaux de télécommunications, et d'autre part à la mobilisation des différents acteurs de l'écosystème, les réseaux en France n'ont pas connu de congestion majeure durant la période de confinement liée à la Covid-19 entre mars et mai 2020. Pour autant, au-delà de cette crise, l'augmentation des usages se poursuit sur le long terme et nécessite une montée en débit des infrastructures au travers du déploiement de la fibre et de la 5G.

9. Voir lexique.
10. La norme GPON permet par exemple de mettre un maximum de 128 clients sur un arbre proposant 2488 Mbit/s descendants et 1244 Mbit/s montants. Plusieurs dizaines d'arbres GPON sont ensuite concentrés et souvent connectés au réseau par un lien 10 Gbit/s.

L'ÉCOSYSTÈME MOBILISÉ POUR TOUS PENDANT LA CRISE SANITAIRE



Le présent schéma n'est pas une liste exhaustive des actions prises durant la crise sanitaire. Il a été élaboré à partir d'informations publiques et pourrait comporter des erreurs ou imprécisions.

Source : Arcep

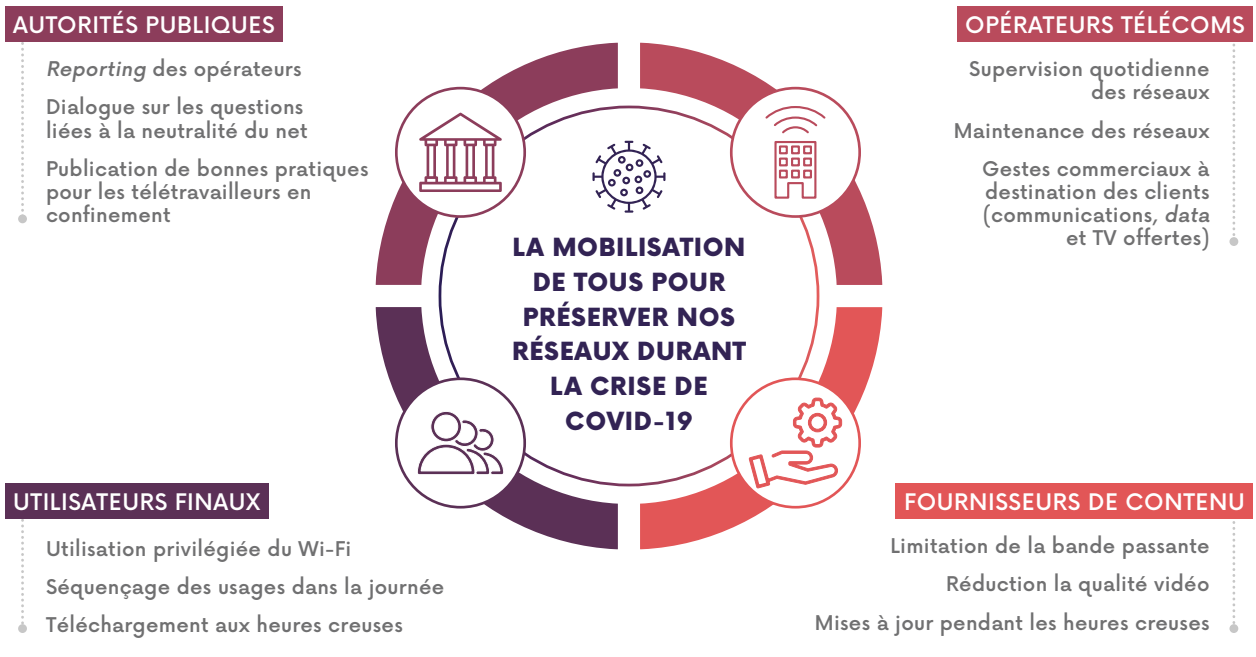
QUELLES ONT ÉTÉ LES BONNES PRATIQUES POUR QU'INTERNET CONTINUE À FONCTIONNER ?

La mobilisation exceptionnelle de tous les acteurs de l'écosystème (opérateurs, fournisseurs de contenu et d'applications, utilisateurs finaux et institutions publiques) a permis de faire face à l'intensité inédite des besoins numériques durant la crise. Tout d'abord, les entreprises télécoms et le tissu de PME, d'acteurs locaux et d'associations qui les entourent ont travaillé de concert pour maintenir et assurer le fonctionnement continu des réseaux. En plus de la mobilisation de leurs équipes sur le terrain, les opérateurs ont également multiplié les gestes commerciaux à destination de leurs clients confinés : données mobiles supplémentaires offertes, communications téléphoniques gratuites, accès libre aux chaînes de télévision payantes, augmentation du débit sur certaines offres, etc. Enfin, les opérateurs ont également mis à disposition des terminaux et ont offert de la *data* au profit d'établissements hospitaliers ou d'associations en aide aux plus vulnérables et aux plus démunis dans le but de permettre de rester connectés les uns aux autres.

Suite à un dialogue proactif initié par le Gouvernement ou de leur propre initiative, les fournisseurs de contenu et d'applications (FCA) ont aussi contribué à l'effort collectif. Les « grands » utilisateurs des réseaux, telles les plateformes de *streaming* vidéo ou encore les plateformes de jeux en ligne, ont réduit la charge de leurs contenus en circulation en limitant la bande passante requise par leurs services, en diminuant la qualité de leurs vidéos ou encore en programmant les téléchargements et les mises à jour de leurs services en période de faible affluence. Le dialogue mis en place entre Disney et les opérateurs a aussi permis d'anticiper le lancement de la plateforme de *streaming* vidéo Disney+. En effet, à la différence d'autres FCA, l'architecture retenue par Disney ne reposait pas sur son propre CDN[11] mais sur le recours à des CDN tiers, pouvant ainsi saturer un lien d'interconnexion partagé avec de multiples autres contenus en cas de pic d'utilisation lié au lancement de la plateforme. Le redimensionnement de certaines interconnexions a donc pu être nécessaire pour prévenir d'éventuels risques de congestion des réseaux.

La mise en place d'un dialogue proactif entre les opérateurs et les principaux fournisseurs de contenu et d'applications s'est avéré plus que jamais nécessaire pour favoriser l'anticipation des événements pouvant avoir un impact sur la charge des réseaux.

MOBILISATION DES ACTEURS DE L'ÉCOSYSTÈME DURANT LA CRISE SANITAIRE



Source : Arcep

11. Voir lexique.

De même, les utilisateurs finaux ont également pu contribuer à l'effort collectif pour les réseaux, en adaptant leurs usages notamment guidés par les recommandations du Gouvernement et de l'Arcep sur les bonnes pratiques à suivre par exemple en matière de télétravail[12] ou encore les recommandations de l'Arcep pour améliorer la qualité de son Wi-Fi[13]. Ainsi, les utilisateurs finaux qui ont suivi ces recommandations ont basculé certains de leurs usages de la 4G au Wi-Fi, optimisé l'utilisation de leur Wi-Fi (par exemple en utilisant des répéteurs Wi-Fi), séquencé leurs usages numériques dans la journée et reporté aux heures creuses les usages lourdement consommateurs en bande passante.

Durant toute la crise, le Gouvernement et l'Arcep ont opéré un suivi quotidien de l'évolution des réseaux télécoms. En complément des dispositifs directement dédiés à la gestion opérationnelle de la crise, les opérateurs ont alors transmis quotidiennement au Gouvernement et à l'Arcep puis de façon plus espacée les données relatives à l'état de leurs réseaux. De plus, la résilience des réseaux télécoms étant aussi une question transnationale, les régulateurs européens dont l'Arcep ont activement contribué au suivi de l'état des réseaux européens au sein du BEREC. Ce dernier a d'ailleurs publié de manière bi-hebdomadaire, puis mensuellement, un rapport détaillant l'état des réseaux en Europe pendant la crise sanitaire, qui a conclu constamment à l'absence de congestion majeure des réseaux en Europe.

COMMENT GARANTIR LE RESPECT DE LA NEUTRALITÉ DU NET DANS CETTE SITUATION EXCEPTIONNELLE ?

Pour répondre à cette demande exceptionnelle et démultipliée de connectivité, les fournisseurs d'accès à internet ont rapidement émis l'hypothèse de devoir prioriser l'acheminement dans leurs réseaux de certains contenus jugés essentiels (notamment le télétravail, l'enseignement à distance ou encore la télémédecine) afin d'assurer leur fonctionnement continu. Parfois présentée comme la solution pour contenir l'augmentation des flux en circulation en période de crise, cette dernière n'est pas si simple en pratique, notamment lorsqu'il est question de distinguer des flux similaires (exemple : la visioconférence du *streaming* vidéo) ou encore lorsque des services sont détournés de leurs usages premiers (exemple : le recours à des plateformes de jeux vidéo à des fins d'enseignement pédagogique). Si à situation exceptionnelle, mesures exceptionnelles, qu'en est-il de la validité de cette pratique au regard du règlement internet ouvert ?

Selon l'article 3 du règlement internet ouvert, les FAI sont tenus de traiter tout le trafic de façon égale et non discriminatoire quelles que soient la nature et l'origine des données en circulation dans leurs réseaux. Le traitement différencié de certains contenus est donc strictement encadré par le règlement internet ouvert, mais peut toutefois s'inscrire dans l'une des trois exceptions explicitement prévues par ce dernier : l'obligation de respecter une autre disposition légale, la nécessité pour un FAI de préserver la sécurité de son réseau et enfin le risque d'une congestion imminente. C'est dans le cadre légal de cette dernière exception que l'Arcep a ouvert un dialogue proactif avec les opérateurs sur les éventuelles mesures de gestion de trafic envisagées par ces deniers en lien avec la crise sanitaire. Au regard du règlement internet ouvert, les fournisseurs d'accès à internet pouvaient, si besoin, prendre des mesures exceptionnelles de gestion de trafic afin de réduire les effets d'une congestion imminente survenant dans leurs réseaux. Toutefois, bien qu'exceptionnelles, ces mesures doivent aussi respecter certaines conditions : permettre de résorber le phénomène de congestion, être les moins contraignantes possible à l'égard du trafic en circulation, traiter de manière égale les catégories de trafic équivalentes et ne pas être appliquées plus longtemps que nécessaire. Ces critères permettent d'assurer la pérennité d'un traitement non discriminatoire entre fournisseurs de contenus similaires, y compris lors de la mise en œuvre de mesures exceptionnelles de gestion de congestion par les FAI.

Dès les premiers jours de la crise, l'Arcep et le Gouvernement ont ouvert un dialogue proactif avec les opérateurs pour s'assurer du respect du principe de neutralité du net, y compris en cette période de crise sanitaire exceptionnelle. L'attention constante des opérateurs quant au maintien de leurs réseaux, ainsi que la mobilisation de l'ensemble des acteurs de l'écosystème, ont permis aux réseaux de fonctionner de manière continue et neutre pendant toute la durée de la crise sanitaire.

De même, la question de la résilience des réseaux de télécommunication s'est posée au niveau européen. Dans une déclaration conjointe[14], la Commission européenne et le BEREC ont aussi rappelé la possibilité pour les opérateurs de recourir à de telles mesures exceptionnelles de gestion de trafic en cas de congestion imminente. Les différents rapports, édités par le BEREC, ne font d'ailleurs état d'aucune décision formelle prise par un État membre sur le fondement de l'article 3 du règlement internet ouvert en lien avec la crise sanitaire.

In fine, malgré la gravité et la dureté de la crise sanitaire en France et en Europe, le règlement internet ouvert a montré sa capacité à s'appliquer en toutes circonstances.

12. Bonnes pratiques sur l'utilisation d'internet en télétravail publiées par l'Arcep : https://www.arcep.fr/demarches-et-services/utilisateurs/teletravail-et-connexion-internet.html
13. Cinq astuces pour améliorer la qualité de son signal Wi-Fi : https://www.arcep.fr/demarches-et-services/utilisateurs/comment-ameliorer-la-qualite-de-son-wifi.html
14. Déclaration conjointe de la Commission européenne et du BEREC sur la manière de faire face à la demande accrue de connectivité des réseaux due à la pandémie de Covid-19 : https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9236-joint-statement-from-the-commission-and-the-body-of-european-regulatorsfor-electronic-communications-berec-on-coping-with-the-increased-demand-for-network-connectivity-due-to-the-covid-19-pandemic

La parole à



LUCA BELLI

PhD, Professeur à l'École de droit de la Fundação Getulio Vargas (FGV - Rio de Janeiro), Coordinateur du Centre Technologie et Société et Responsable des coalitions sur la neutralité du net et sur la connectivité communautaire du Forum de l'ONU sur la gouvernance de l'internet (IGF)

LA VALEUR DE L'OUVERTURE D'INTERNET EN TEMPS DE CRISE : NEUTRALITÉ DU NET, RÉSEAUX COMMUNAUTAIRES ET AUTODÉTERMINATION NUMÉRIQUE

La pandémie de la Covid-19 a mis en évidence l'importance fondamentale de l'accès à internet, et de l'exclusion totale que les non-connectés affrontent en temps de crise. Notre nouvelle routine repose sur les réunions et l'apprentissage en ligne, la télémédecine et les applications de e-commerce. Cependant, pour presque 4 milliards de personnes qui ne bénéficient pas d'une connexion à internet ou ne peuvent pas se la permettre, l'arrivée de la Covid-19 équivaut à être assigné à résidence. De plus, une partie indéfinie de la population est officiellement considérée comme « connectée » bien qu'elle ne soit *de facto* que partiellement connectée.

Les statistiques officielles considèrent un « individu connecté » lorsqu'il accède à internet au moins une fois au cours des trois derniers mois.[1] Une telle définition est critiquable et ne tient pas compte du nombre incroyable de restrictions abusives, qu'elles soient de nature politique ou économique, qui affectent comment un individu est connecté.

Si votre accès est bloqué ou dégradé, mais que vous avez accédé à un site gouvernemental approuvé au moins une fois au cours des trois derniers mois, vous êtes officiellement considéré comme un « individu connecté », malgré le fait que votre connectivité soit remarquablement limitée. De même, l'expérience numérique des personnes défavorisées qui ne peuvent pas se permettre de payer un abonnement pour accéder à Internet (c'est-à-dire, la plupart de la population mondiale) se limite principalement à des applications sponsorisées (généralement des réseaux sociaux dominants inclus dans les offres dites de « *zero-rating* »[2]). Ces usagers sont loin d'être des individus « connectés », mais sont officiellement considérés comme tels.

Les usagers d'internet sont des « *prosumers* », à la fois consommateurs et producteurs, car ils peuvent non seulement avoir accès, mais aussi créer et partager les contenus ou les applications de leur choix. Ils peuvent contribuer activement à l'évolution du net par leur créativité et leur innovation. Cette idée de garder l'usager au centre d'internet est l'essence même de son architecture originale, qui considère que l'« intelligence » du Net « est de bout-en-bout »[3]. Cette même philosophie est au cœur des régulations sur la neutralité du net qui exigent des fournisseurs d'accès à internet de traiter le trafic sans discrimination fondée sur leurs intérêts commerciaux.

L'importance de préserver et de promouvoir l'ouverture d'internet est essentielle dans le contexte pandémique actuel. En effet, la Covid-19 nous oblige à faire face à des questions difficiles. Comment presque la moitié du monde peut-elle encore être exclue de toute connectivité ? Comment pouvons-nous penser que ceux qui n'accèdent qu'à un petit nombre d'applications prédéfinies une fois en trois mois puissent être considérés comme des personnes connectées ? Comment peut-on penser que les applications de *zero-rating*, qui sont faussement présentées comme « gratuites » [4] et qui sont rémunérées avec des données personnelles – et tout type d'usage que l'on peut en avoir d'elles – représentent un modèle durable, alors que cela exacerbe les problèmes évidents de concentration et de manque de concurrence et que cela affaiblit la souveraineté (numérique) ? Que pouvons-nous faire différemment ?

Pour traiter ces questions et y apporter des réponses concrètes, les coalitions sur la neutralité du net et sur la connectivité communautaire du Forum des Nations unies sur la gouvernance de l'internet (IGF, en anglais) ont rédigé un rapport conjoint consacré à **The Value of Internet Openness in Times of Crisis.**[5] Ici ont été retranscrits quelques éléments-clés, abordés par ce rapport de l'IGF.

Tout d'abord, l'accès à internet est devenu essentiel pour que nos économies, nos sociétés et nos démocraties fonctionnent. Les fractures numériques ont un impact économique, social et démocratique énorme. Ces fractures n'existent

1. ITU (2014). *Manual for Measuring ICT Access and Use by Households and Individuals*, p.81.
2. http://www.zerorating.info/
3. Carpenter (1996). *Architectural Principles of the Internet*. Request for Comments : 1958.
4. Belli & Zingales (16.02.21). *WhatsApp's New Rules : Time to Recognize the Real Cost of "Free" Apps*. Medianama.
5. Belli, Pahwa & Manzar (Eds.) (2020). *The Value of Internet Openness in Times of Crisis.* Official Outcome of the UN IGF Coalitions on Net Neutrality and on Community Connectivity.

pas seulement entre ceux qui ont accès au numérique et ceux qui n'y ont pas accès, mais aussi entre ceux qui sont officiellement considérés comme « connectés ». L'expérience numérique de ceux qui sont « effectivement connectés »[6], qui jouissent d'un internet de haute qualité et de tous ses avantages, est radicalement différente de celle que font ceux qui sont mal connectés, obligés de troquer leur vie privée pour accéder à des applications sponsorisées et laissés avec une connectivité limitée ou de faible qualité.

Lorsque la pandémie a explosé, la Commission européenne et le BEREC ont commencé à surveiller régulièrement le trafic internet afin d'identifier les phénomènes de congestion. En effet, le règlement internet ouvert (UE) 2015/2120 prévoit que des mesures de gestion du trafic allant au-delà des mesures raisonnables peuvent être appliquées pour prévenir ou atténuer les effets d'une congestion temporaire ou exceptionnelle. Bien que l'augmentation du trafic ait été observée dans les réseaux fixes et mobiles, aucune congestion exceptionnelle n'a été signalée. Même sous pression, les réseaux, les normes et les institutions européennes se sont avérés résilients. Malheureusement, cette image idyllique s'applique seulement à ceux qui ont accès à internet.

Les défis en matière de connectivité sont encore très répandus, même dans les pays les plus développés. Par conséquent, il est temps d'envisager des solutions alternatives pour étendre la connectivité, car les solutions que nous utilisons traditionnellement ont des limites évidentes.

Beaucoup d'individus à travers le monde ne se sont pas résignés à un faux choix entre une mauvaise connectivité, des offres de « *zero-rating* » payées avec leurs données personnelles ou le fait de ne pas avoir du tout d'accès à internet. Ils ont décidé de devenir les acteurs de leur avenir numérique et ont créé leurs propres infrastructures, connues sous le nom de réseaux communautaires (Community Networks).[7]

Des communautés locales, des ONG, des petites entreprises et des administrations construisent leurs propres réseaux pour surmonter le manque de couverture internet, en développant des services qui répondent aux besoins des populations locales. Ces initiatives libèrent de nouvelles opportunités de manière ouverte et décentralisée pour l'éducation, le commerce et l'emploi des habitants locaux[8].

Ces réseaux communautaires sont conçus, possédés, et gérés par des communautés locales et pour les communautés locales. Ils représentent un nouveau paradigme, où la connectivité est considérée et gérée comme un bien commun. Ils démontrent que, lorsque les gens ont des informations sur la façon de construire un réseau et sont libres de choisir cette option, ils le font. Dans un tel cadre, les individus agissent comme de véritables « *prosumers* », qui n'ont pas besoin de troquer leur vie privée pour des applications, et sont libres d'accéder, de créer et de partager tout contenu et toute innovation qui correspondent à leur besoins. Ainsi, les individus redeviennent le moteur essentiel de l'ouverture numérique et la force motrice de l'autodétermination numérique.[9]

6. https://a4ai.org/meaningful-connectivity/
7. https://comconnectivity.org/
8. Belli (2017). « Network Self-Determination and the Positive Externalities of Community Networks ». In Belli (Ed). *Community Networks: the Internet by the People, for the People*. FGV Direito Rio.
9. Belli (2018). *Network self-determination : When building the Internet becomes a right*. IETF Journal.

La parole à



MARIE-LAURE DENIS

*Présidente - **CNIL***

LA PROTECTION DES DONNÉES PERSONNELLES AU DÉFI DE LA CRISE SANITAIRE ET DES NOUVEAUX USAGES NUMÉRIQUES

2020 a été l'année la plus importante pour l'internet depuis le smartphone en 2007. S'il est difficile d'en mesurer encore tous les effets, la pandémie a sans aucun doute conduit à la plus grande évolution des usages numériques des dernières années en développant de nouveaux usages comme le click & collect ou la télémédecine et en consolidant d'autres de manière irrémédiable comme le *streaming* ou le télétravail, qui vont profondément bouleverser nos organisations professionnelles.

En recalibrant brutalement l'ordre des priorités de nos sociétés modernes, cette année a également été celle d'évolutions notables dans l'écosystème numérique : l'apparition du mot « souveraineté numérique » dans les éléments de langage français et européens ; la possibilité de confier aux fabricants d'ordiphones, dans certains pays, le protocole de « *contact tracing* » qui éviterait les contaminations ou encore la recrudescence des attaques cyber sur des entreprises, des administrations ou des hôpitaux passés parfois un peu vite au « tout numérique ». Plus largement, ce qui a marqué cette année, c'est la conviction renforcée que les pratiques des acteurs de ce secteur doivent, plus encore qu'auparavant, être conformes aux attentes de nos concitoyens.

La CNIL y a contribué, d'abord en consacrant des moyens importants à la gestion de la pandémie, au contrôle de nouveaux systèmes d'information et d'une application, TousAntiCovid. Celle-ci a fait l'objet d'une attention particulière à la protection de la vie privée par défaut, dans son protocole comme dans son développement. La CNIL a également rendu plusieurs avis concernant la plateforme des données de santé, le *Health Data Hub*, dont l'objectif est de proposer une infrastructure pour développer la recherche en santé. À cette occasion, la question des transferts de données hors de l'Union européenne pour les services d'informatique en nuage a été posée et l'arrêt « Schrems 2 » de la Cour de justice de l'Union européenne en juillet 2020 a confirmé l'exigence d'une protection des données qui s'applique également quand les données quittent notre continent. Cet arrêt, qui remet en cause de nombreuses pratiques numériques des entreprises, fait déjà sentir ses effets. Les annonces se succèdent ces derniers mois pour proposer de nouveaux schémas de gestion des données personnelles qui, *a minima*, préservent ces données d'accès illégitimes à l'étranger, voire, dans certains cas, garantissent le stockage, le traitement et le support de ces données et services au sein de l'UE.

S'il n'appartient pas à la CNIL de juger de l'intérêt économique et industriel de telles évolutions, ces efforts marquent le rôle accru pris par la protection des données depuis l'entrée en application du RGPD[1] en 2018. On pourrait ainsi également citer la polémique sur les modifications des conditions d'utilisation de Whatsapp, qui a incité Facebook à repousser l'entrée en vigueur de ces modifications de plusieurs mois, ou l'adoption de deux sanctions de la CNIL de 100 M€ et 35 M€ contre Google et Amazon respectivement, dans le cadre des vérifications d'un recueil du consentement libre et éclairé préalable au dépôt de cookies publicitaires.

En se projetant vers l'avenir, il est probable que les usages numériques, soutenus par les confinements de l'année passée, continuent de se développer, soulevant de nouveaux défis pour les régulateurs. Pour accompagner ces évolutions, les réseaux doivent également évoluer, sur le mobile avec la 5G mais également sur les réseaux fixes, sur le point de basculer massivement vers la fibre optique. Les travaux de l'Arcep pour consolider la mesure de la qualité de service des réseaux fixes sont particulièrement utiles dans cette période et la méthode proposée, reposant sur la mise en place d'interfaces (API) dans les équipements des opérateurs, montre que le régulateur peut également adopter de nouvelles approches. Cette pratique n'est pas sans soulever des questions sur le traitement des données des abonnés mais la CNIL est pleinement engagée aux côtés de l'Arcep, dans une démarche exemplaire d'inter-régulation visant à définir des modalités opérationnelles respectueuses de la vie privée des individus.

1. Voir lexique.

PARTIE 1

Assurer le bon fonctionnement d'internet

CHAPITRE 1
Améliorer la mesure de la qualité d'internet

CHAPITRE 2
Superviser l'interconnexion de données

CHAPITRE 3
Accélérer la transition vers IPv6

CHAPITRE 1

AMÉLIORER LA MESURE DE LA QUALITÉ D'INTERNET

À retenir

À l'été 2021,
les opérateurs devront effectuer auprès de l'Arcep la démonstration d'une box de développement avec l'API « carte d'identité de l'accès ». L'API sera ensuite déployée progressivement dans les box des utilisateurs.

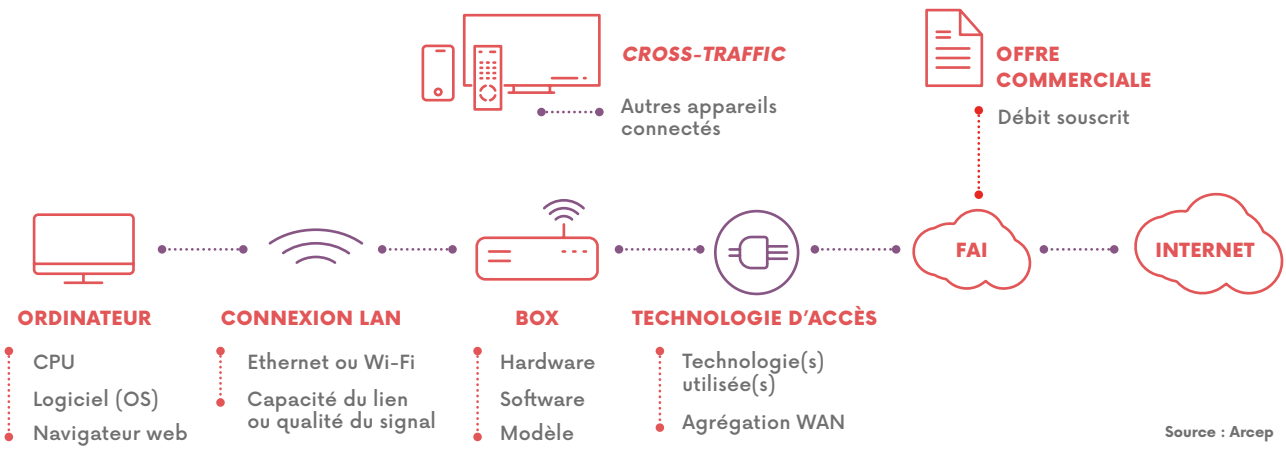
10 acteurs de la mesure
se sont déclarés conformes à la version 2020 du Code de conduite de la qualité de service d'internet.

La qualité du service de données mobiles continue de progresser : le débit moyen en France métropolitaine atteint
49 Mbit/s
en 2020.

La qualité de service internet dépend d'abord de la montée en débit des infrastructures, notamment au travers du déploiement de la fibre sur le fixe et des technologies 4G et 5G sur le mobile. Afin de permettre aux utilisateurs de faire des choix plus éclairés quand il s'agit d'opter pour un opérateur, l'Arcep met ainsi à disposition des utilisateurs l'outil « Ma connexion internet » qui permet de connaître les technologies et les débits disponibles pour une adresse donnée.

Si les déploiements permettent aux opérateurs de proposer toujours plus de débit dans leurs offres internet, les usages évoluent également et pour certains sont sensibles au débit disponible. De nombreux clients souhaitent donc mesurer la qualité de service dont ils disposent à domicile, mais aussi en mobilité.

CARACTÉRISTIQUES DE L'ENVIRONNEMENT UTILISATEUR



Source : Arcep

1 Les biais potentiels de la mesure de la qualité de service

Aujourd'hui, les utilisateurs peuvent facilement faire remonter leurs mesures de la qualité de service (QoS) de leur accès internet *via* des outils de test dits « en *crowdsourcing* ».

Néanmoins, un grand nombre de caractéristiques techniques ou d'usages ont une influence sur la mesure et il est très difficile de savoir si une mauvaise qualité mesurée est due au réseau d'accès du fournisseur d'accès à internet (FAI), à la qualité du Wi-Fi et/ou à l'utilisation parallèle d'autres appareils connectés au réseau local lors du test.

« L'environnement utilisateur » est le premier facteur qui peut affecter le résultat d'une mesure lors d'un test. Le schéma de la page précédente récapitule les caractéristiques principales de l'environnement utilisateur pouvant avoir une influence sur le résultat.

D'autres caractéristiques (emplacement et capacité de la mire de test, méthodologie de mesure de l'outil de test) peuvent également être facteurs de biais lors de la mesure de la qualité de service. Les biais potentiels sont développés dans les sections suivantes.

2 La mise en place de l'API pour caractériser l'environnement utilisateur

2.1 Présentation de l'API carte d'identité de l'accès

Alors que sur les réseaux mobiles les applications de test de débit sont à même d'identifier l'environnement utilisateur (technologie radio, intensité du signal, etc.), sur les réseaux fixes, la mesure de la qualité de service est particulièrement complexe : il est à ce jour quasi impossible techniquement pour un outil de mesure (souvent appelé « *speed test* ») de connaître avec certitude la technologie d'accès (cuivre, câble, fibre, etc.) sur laquelle a été réalisé un test. Ce manque de caractérisation de la mesure, qui ne permet pas d'isoler des facteurs susceptibles de modifier fortement les résultats, rend les données difficilement exploitables, voire, dans certains cas, induit en erreur le consommateur. Dans ce contexte, l'Arcep a lancé en début d'année 2018 un vaste chantier sollicitant toutes les parties prenantes afin de résoudre les difficultés de mesure de la qualité de service des réseaux fixes. Cette démarche de co-construction[1] initiée par l'Arcep implique une vingtaine d'acteurs dont des outils de mesure en *crowdsourcing*, des opérateurs, des organismes de protection des consommateurs et des acteurs académiques. Pour permettre aux acteurs de la mesure de mieux caractériser l'environnement utilisateur, l'écosystème a convergé vers la mise en place d'une *Application Programming Interface* (API) implémentée dans les box des opérateurs et accessible aux outils de mesure qui respectent le Code de conduite publié par l'Arcep[2]. Cette interface logicielle permettra de transmettre les informations qui constituent la « carte d'identité de l'accès ».

Une consultation publique a été menée au printemps 2019 sur ce projet ; les dix-sept contributions reçues et publiées[3] par l'Arcep ont permis d'ajuster, en concertation avec les acteurs de l'écosystème, les modalités de mise en œuvre de l'API. L'Arcep a adopté la décision correspondante fin octobre 2019[4] et le Gouvernement a homologué cette décision par un arrêté publié au *Journal Officiel* le 16 janvier 2020[5].

L'API « carte d'identité de l'accès » a pour objectif de caractériser l'environnement de la mesure. Cette API sera accessible à des outils de mesure en *crowdsourcing* utilisés par les usagers pour évaluer le débit ou plus généralement la qualité de service de leurs accès internet. Sollicitée uniquement lorsque l'utilisateur initie un test de débit, et sous son contrôle, l'API renseignera l'outil de mesure sur une série d'indicateurs techniques, tels que le type de box, la technologie d'accès à internet, les débits montants ou descendants contractuels.

Opérateurs et box concernés, paramètres techniques remontés, calendrier de mise en place, spécifications techniques d'implémentation sont précisés dans la décision de l'Arcep.

Les modalités de fonctionnement de l'API prennent pleinement en compte les questions de respect et de protection de la vie privée des utilisateurs. D'abord, les données recueillies par l'API ne sont évidemment pas transmises à l'Arcep. Ensuite, aucune donnée liée à l'identification de l'utilisateur (identifiant, nom, localisation, etc.) n'est transmise par l'API aux outils de mesure. Enfin, l'API n'est sollicitée que lors d'un test de débit initié par l'utilisateur lui-même et ne répond pas aux sollicitations depuis internet. Questionnée dans le cadre de cette démarche, la CNIL a pu s'assurer que le dispositif répondait dans son principe aux exigences en matière de protection des données personnelles tout en insistant sur l'importance du rôle de conseil de l'Arcep, notamment au travers du « Code de conduite de la qualité de service internet », vis-à-vis des outils de mesure exploitant l'API.

Les résultats obtenus, désormais enrichis grâce à l'API, seront un nouveau pas dans l'amélioration de la mesure de la qualité de service des réseaux fixes.

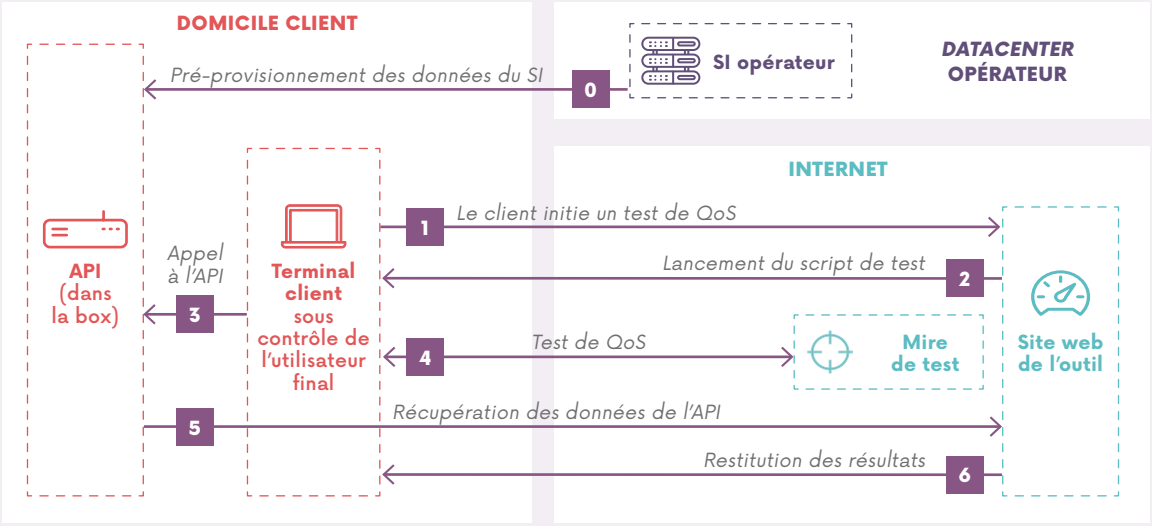
1. La démarche de co-construction de l'API est décrite dans le rapport 2018 sur l'état d'internet en France : https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf#page=11
2. Édition 2018 du Code de conduite de la qualité de service internet : https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf
3. Réponses reçues à la consultation publique : https://www.arcep.fr/uploads/tx_gspublication/reponses_consultation_publique_api_box-oct2019.zip
4. Décision n° 2019-1410 de l'Arcep en date du 10 octobre 2019 : https://www.arcep.fr/uploads/tx_gsavis/19-1410.pdf
5. Arrêté du 8 janvier 2020 homologuant la décision n° 2019-1410 de l'Arcep : https://www.arcep.fr/fileadmin/cru-1624346775/reprise/textes/arretes/2020/arr-08012020-homolog-2019-1410-api-box.pdf

PLUS D'INFORMATIONS SUR L'API « CARTE D'IDENTITÉ DE L'ACCÈS »

Comment fonctionne l'API ?

Le schéma suivant décrit de façon simplifiée le fonctionnement de l'API lorsqu'un client initie un test de QoS avec un outil de test ayant accès à l'API.

FONCTIONNEMENT DE L'API « CARTE D'IDENTITÉ DE L'ACCÈS »



Ce schéma est simplifié : pour une meilleure lisibilité, les flux vers internet (flèches 1, 2, 4 et 6) passent par la box mais ne sont pas représentés ici.

Source : Arcep

Quels sont les outils de mesure qui ont accès à l'API ?

L'API sera accessible aux outils de mesure qui se sont déclarés conformes au « Code de conduite de la qualité de service internet » publié par l'Arcep. Les travaux sur le Code de conduite sont abordés dans la section suivante.

Quelles sont les box concernées par l'API ?

Les opérateurs qui ont plus d'un million de clients et qui remplissent les conditions décrites dans la décision de l'Arcep (Bouygues Telecom, Free, Orange et SFR) auront l'obligation d'implémenter l'API dans la majorité des modèles de box xDSL, câble, FttH et 5G fixe proposées aux clients à partir du 17 juillet 2021.

L'Arcep encourage également à implémenter l'API dans les autres modèles de box et dans les box des opérateurs non soumis à la décision.

L'API est-elle accessible depuis internet ?

Non, l'API est accessible uniquement depuis le réseau local de l'utilisateur final et ne répond pas aux requêtes provenant d'internet. De plus, un système de restriction d'accès est mis en place, afin que seuls les outils autorisés puissent accéder à l'API.

Quand l'API sera-t-elle disponible ?

En juillet 2022, l'API « carte d'identité de l'accès » sera implémentée et activée dans la quasi-totalité des box du parc concerné par la décision de l'Arcep après plusieurs phases de démonstrations et d'implémentations.

CALENDRIER DE DÉPLOIEMENT DE L'API



2.2 La poursuite des travaux de co-construction dans le cadre du comité de suivi API

Depuis la publication de la décision, l'Arcep a réuni régulièrement opérateurs et outils de mesure en *crowdsourcing* dans un comité de suivi du développement de l'API afin d'en préciser les spécifications. Cinq groupes de travail ont été mis en place :

- Modalités d'implémentation de l'API (architecture, mécanismes d'autorisation, etc.) ;
- Définition du processus d'accès à l'API pour les outils de mesure ;
- Design API ;
- Qualité des données remontées par l'API ;
- Mise en œuvre des règlements RGPD et *ePrivacy*.

L'ensemble des spécifications de l'API qui seront discutées et définies au sein du comité de suivi API seront publiées prochainement.

3 Vers des méthodologies de mesure plus transparentes et robustes

3.1 Présentation du Code de conduite 2020 de l'Arcep

À l'instar des caractéristiques de l'environnement utilisateur, les méthodologies de mesure sont également des facteurs ayant une forte influence sur le résultat des mesures de qualité de service. En effet, la bonne compréhension de la nature des tests réalisés par ces outils, de leurs limites, mais aussi la façon dont sont présentés les résultats sont essentielles pour que les utilisateurs puissent réaliser leurs tests dans les meilleures conditions et en interpréter correctement les résultats.

L'Arcep avait identifié en 2017 le besoin d'une plus grande transparence des méthodologies de mesure. Elle a publié en décembre 2018 une première version du Code de conduite de la qualité de service internet à destination des acteurs de la mesure[6].

Ce Code de conduite porte sur deux aspects : d'une part, inviter les outils à accompagner la publication des résultats par une explication claire des choix méthodologiques réalisés afin que toute personne tierce soit en mesure d'analyser les résultats présentés ; d'autre part, indiquer les bonnes pratiques permettant l'obtention de mesures plus robustes.

Cette approche permet d'inciter les acteurs à un niveau adéquat de transparence et de robustesse, à la fois pour les protocoles de test, mais aussi pour la présentation des résultats.

La démarche de co-construction, retenue pour l'élaboration de l'édition 2018 du Code de conduite, a été poursuivie pour alimenter cette nouvelle version. L'Arcep a ainsi relancé un cycle de travail avec plus d'une vingtaine d'acteurs dont des éditeurs d'outils de mesure en *crowdsourcing*, des organismes de protection des consommateurs, des opérateurs et des acteurs académiques, dont la version 2020 du Code de conduite est le résultat[7]. Cette mise à jour du Code de conduite garde la même structure en deux grandes parties de la version 2018 :

- la première concerne le protocole de test de l'outil de mesure, c'est-à-dire à la fois les méthodologies de mesure des différents indicateurs (débit, latence, temps de chargement des pages web et qualité du *streaming* vidéo), les mires de test ainsi que les autres tests que l'outil propose ou les informations qu'il communique à l'utilisateur final ;
- la seconde concerne les publications agrégées, dont un engagement général sur la mise en place d'algorithmes visant à exclure les mesures erronées, manipulées ou non pertinentes. Par ailleurs, pour garantir la représentativité statistique, les outils respectant le Code de conduite s'engagent à publier la période couverte, le nombre de mesures et les facteurs susceptibles d'introduire un biais significatif dans l'analyse des catégories comparées.

Afin d'accompagner progressivement la montée en compétence de l'écosystème de mesure de la qualité de service, plusieurs axes ont été renforcés dans la nouvelle version du Code de conduite. Il est notamment demandé aux outils de mesure de la qualité de service de :

- préciser aux utilisateurs les différents facteurs qui peuvent impacter la mesure, par exemple l'utilisation et les caractéristiques du Wi-Fi, ou encore le modèle et la version du système d'exploitation et du navigateur web, qui peuvent avoir une forte influence sur la mesure de qualité de service ;
- afficher une valeur médiane pour certains paramètres, notamment pour la latence. Cette information est en effet plus pertinente que la moyenne pour refléter l'expérience utilisateur, notamment dans le cas où il existe des valeurs extrêmes dans les résultats mesurés ;
- introduire une capacité minimale pour les serveurs (mires) de test, afin d'éviter que le test soit limité par ces mires ;
- préciser la capacité pour les mires de test de réaliser des tests en IPv6, le protocole utilisé pouvant impacter la mesure de débit.

Ce Code de conduite met aussi l'accent sur un certain nombre de biais de mesure à expliciter dans les publications agrégées des outils de mesure. Il prend enfin davantage en compte les spécificités de la mesure de la qualité de service d'internet sur les réseaux mobiles.

6. Édition 2018 du Code de conduite de la qualité de service internet : https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf
7. Édition 2020 du Code de conduite de la qualité de service internet : https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-QoS-internet-2020_sept2020.pdf

Enfin, le Code de conduite évoluera à nouveau avec la mise en place de l'API « carte d'identité d'accès ». En effet, les travaux pour améliorer encore les pratiques et renforcer le Code de conduite se poursuivront lors de la mise en place effective de l'API. La prise en compte des fonctionnalités proposées par cette API aux outils de mesure permettra en effet de fiabiliser non seulement les tests de QoS mais aussi les publications agrégées. Ces évolutions se feront bien évidemment en concertation avec les acteurs impliqués.

3.2 Les outils conformes à la version 2020 du Code de conduite

L'Arcep a publié le 14 septembre dernier l'édition 2020 du Code de conduite de la qualité de service internet. Dès début 2021, plusieurs outils s'y déclaraient conformes. Les outils qui étaient déjà conformes à la version 2018 ont renouvelé leur déclaration de conformité et de nouveaux outils ont manifesté leur intérêt pour rejoindre la démarche de co-construction de l'Arcep.

Outils qui se sont déclarés conformes au Code de conduite 2020

En ce qui concerne la qualité de service fixe, les outils de test qui se sont déclarés conformes à la version 2020 du Code de conduite de la qualité de service internet sont :

- **nPerf,** développé par nPerf ;
- **DébiTest 60 :** le testeur de connexion de 60 Millions de consommateurs, développé par QoSi ;
- **5GMark,** développé par QoSi ;
- **Speedtest UFC-Que Choisir,** développé par UFC-Que Choisir ;
- **IPv6-test :** le test de qualité de service IPv4 et IPv6, développé par IPv6-test ;
- **Speedtest,** développé par Ookla* ;
- **TestADSL,** développé par SpeedChecker*.

En ce qui concerne la qualité de service mobile, les outils de test qui se sont déclarés conformes à la version 2020 du Code de conduite de la qualité de service internet sont :

- **nPerf,** développé par nPerf ;
- **DébiTest 60 :** le testeur de connexion de 60 Millions de consommateurs, développé par QoSi ;
- **5GMark,** développé par QoSi ;
- **Speedtest,** développé par Ookla* ;
- La solution de *crowdsourcing* **Tutela,** développée par Tutela*.

Bien qu'ils ne proposent pas solutions de mesure à destination des utilisateurs finaux, les outils suivants se sont également déclarés conformes au Code de conduite :

- Sondes **Whitebox,** développées par SamKnows* ;
- La solution **Eyes'ON,** développée par SoftAtHome*.

D'autres outils de test de débit existent, mais ils ne se sont pas encore déclarés conformes au Code de conduite 2020.

* Outils non déclarés conformes à l'édition 2018 et qui se sont déclarés conformes à l'édition 2020 du Code de conduite de la qualité de service d'internet.

La parole à



JAMES CARROLL

*Directeur des initiatives stratégiques - **Ookla***

LA MESURE DE QoS AU SERVICE DES CONSOMMATEURS

Notre mission à Ookla est de contribuer à rendre internet meilleur, plus rapide et plus accessible pour tous. Depuis plus de 15 ans, notre solution Speedtest aide les consommateurs à s'assurer qu'ils obtiennent ce pour quoi ils paient auprès de leur fournisseur d'accès à internet (FAI) et de leur opérateur de réseau mobile. À leur tour, les régulateurs, les fournisseurs et les opérateurs utilisent les données *Speedtest Intelligence*® pour surveiller les concurrents et optimiser leurs propres réseaux en termes de fiabilité et de performance.

Travailler avec l'Arcep pour nous assurer que nous sommes conformes à leur Code de conduite a été stimulant pour nous à Ookla. Lorsque notre projet a commencé il y a 15 ans, nous nous sommes concentrés sur le fait d'aider les consommateurs et les utilisateurs finaux à comprendre leur connexion internet et sa qualité. Le cœur du Code de conduite de l'Arcep vise à mieux les informer pour leur permettre de prendre des décisions claires. Nous sommes heureux de travailler avec un régulateur qui partage notre passion pour les consommateurs et nous sommes également ravis de voir comment cette relation peut améliorer l'éducation des consommateurs autour de la connectivité internet.

Étant donné que les particuliers et les entreprises dépendent de plus en plus d'internet pour l'éducation, la santé et le divertissement, l'accès aux services internet fixe et mobile n'est pas seulement le moteur de la croissance économique, il a également un impact sur la sécurité publique et la qualité de vie. C'est pourquoi la fourniture d'un accès universel à internet rapide et fiable est une priorité essentielle pour la plupart des régulateurs et des gouvernements du monde entier. Ookla® s'engage farouchement à mesurer les performances et la disponibilité d'internet dans le monde et à en rendre compte de manière transparente.



JANUSZ JEZOWICZ

*PDG - **SpeedChecker***

L'INTÉRÊT DE CARACTÉRISER L'ENVIRONNEMENT UTILISATEUR POUR FIABILISER LES MESURES QoS

Nous suivons le Code de conduite QoS de l'Arcep depuis quelques années et soutenons pleinement l'orientation du régulateur français. Si le Code de conduite de l'Arcep n'est pas obligatoire pour les outils de mesure de QoS, le respect du Code présente des avantages non négligeables pour les éditeurs, notamment la possibilité de se connecter à l'API « carte d'identité de l'accès » qui sera proposée par les opérateurs en France dans les années à venir.

Le projet API « carte d'identité de l'accès » est un nouveau développement passionnant pour la QoS, qui offrira la prochaine génération d'outils pour les consommateurs en rendant compte du débit d'internet mais aussi en aidant au dépannage. Actuellement, les clients qui testent le débit et obtiennent de faibles résultats ne comprennent pas pourquoi. La plupart des clients se connectant *via* le Wi-Fi, il n'est pas surprenant qu'un nombre important de résultats à faible débit soit associé à une mauvaise qualité du Wi-Fi. Cela a un impact sur les utilisateurs et les opérateurs en termes d'augmentation des appels d'assistance et de problèmes de réputation.

Chez SpeedChecker, nous nous attaquons à ce problème depuis un certain temps en introduisant un test Wi-Fi intégré à nos applications mobiles. Notre test Wi-Fi peut identifier les goulots d'étranglement du Wi-Fi et conseiller à l'utilisateur de se concentrer sur les améliorations du Wi-Fi au lieu de se plaindre auprès du FAI. En raison des limitations technologiques, notre test Wi-Fi ne peut pas fonctionner dans le navigateur web où la plupart des utilisateurs testent internet. L'approche API « carte d'identité de l'accès » sera utilisable sur n'importe quelle plateforme, y compris les navigateurs web, et offrira d'autres améliorations sur la précision.

Nous considérons cette API comme une étape importante vers des méthodes de *crowdsourcing* plus précises sur les réseaux fixes. Le *crowdsourcing* QoS sur les réseaux mobiles est déjà populaire depuis un certain temps et nous espérons que l'API « carte d'identité de l'accès » encouragera également l'industrie à utiliser ce concept puissant pour les réseaux fixes.

La parole à



ROXANNE ROBINSON

*Directrice des affaires publiques - **SamKnows***

LES ENJEUX DE LA MESURE DE LA QUALITÉ D'EXPÉRIENCE INTERNET

SamKnows mesure, analyse et visualise la qualité de l'expérience (QoE) et la qualité de service (QoS) d'internet en temps réel. Nos données de mesure sont utilisées dans le monde entier afin d'aider les FAI à améliorer les performances du réseau, les régulateurs à évaluer les FAI et de garantir que les consommateurs peuvent prendre des décisions éclairées concernant leurs connexions internet.

Les données QoS ont toujours été cruciales pour les FAI et les régulateurs afin d'analyser les performances d'internet, mais à mesure que les débits ont augmenté au fil des ans, un changement dans la façon dont les consommateurs utilisent leur connexion internet est clairement visible. Les mesures au-delà du débit, qui examinent les performances d'applications réelles, donnent une vue plus holistique des performances et peuvent mettre en évidence des problèmes que le débit peut masquer. SamKnows propose une vaste gamme de tests QoE qui mesurent les services les plus populaires disponibles aujourd'hui pour les consommateurs.

La pandémie a renforcé cet intérêt pour les données de QoE. La maison est devenue un lieu où les gens utilisent leur connexion internet pour travailler, éduquer leurs enfants, accéder aux soins de santé, rester en contact avec leurs amis et leur famille et se divertir en regardant des films ou en jouant à des jeux en ligne. La mesure des services de visioconférence ou des plateformes de jeu populaires fournit des données en temps réel aux consommateurs qui peuvent voir les performances de leur connexion internet.

L'analyse des données QoS et QoE est considérablement facilitée par la présence d'informations contextuelles « environnementales ». C'est exactement ce que propose l'API de carte d'identité d'accès de l'Arcep. SamKnows a utilisé des solutions similaires avec d'autres FAI aux États-Unis et elles sont efficaces pour fournir des informations précises. Fournir ces données avec les tests QoS permet de donner un sens aux résultats de mesure en les remettant dans leur contexte. L'ajout de métriques QoE importantes est la prochaine étape pour donner une vue véritablement holistique de l'expérience utilisateur.



JOHN DAVIES

*Analyste stratégie - **Tutela Technologies Ltd.***

AIDER LES OPÉRATEURS À COMPRENDRE ET À RÉPONDRE AUX DEMANDES ET ATTENTES CROISSANTES DE LEURS ABONNÉS

L'utilisation des réseaux mobiles continue de croître et d'évoluer, tout comme les attentes des abonnés vis-à-vis de leurs opérateurs mobiles. Bien que la possibilité de passer un appel téléphonique reste importante aujourd'hui, de nombreux abonnés sont plus conscients des limites des réseaux lorsqu'ils tentent de rejoindre un appel vidéo familial ou lorsqu'ils jouent en ligne dans le bus. Dans un futur proche, cela évoluera vers des cas d'utilisation telle que la réalité augmentée mobile et l'IoT[1] grand public.

L'objectif de Tutela est de mesurer les réseaux dans des conditions réelles, en fournissant des données et des analyses permettant aux opérateurs de comprendre l'expérience réelle des abonnés. Cela recouvre aussi bien les mesures de débit traditionnelles que la fréquence de connexion réseau d'un utilisateur qui est adaptée à différentes applications.

Le fondement de cette approche est une méthodologie de test construite autour de la transparence, de la qualité et du respect de la vie privée. C'est pourquoi Tutela travaille en étroite collaboration avec l'Arcep sur son Code de conduite pour atteindre nos objectifs communs de tests réseau équitables, parlants et robustes. De même, les opérateurs qui s'appuient sur les données QoS pour diriger leurs investissements ont besoin de données et d'analyses qui fournissent des informations de haute qualité sur l'expérience de l'abonné, tout en étant conformes aux réglementations en matière de confidentialité.

Pour donner une vision réelle des performances, Tutela collecte des données en arrière-plan pendant qu'un abonné utilise son appareil dans des circonstances typiques. Ces données permettent aux opérateurs d'aligner leurs investissements sur les résultats des abonnés. Alors que la 5G accueille une nouvelle génération de besoins d'abonnés, nous sommes impatients de travailler avec des organisations comme l'Arcep pour continuer à offrir aux opérateurs des informations exploitables sur les performances réelles du réseau.

1. Voir lexique.

Travaux du BEREC : accompagnement des ARN dans la mise en œuvre d'outils de mesure et mise à jour de la méthodologie QoS

L'outil développé par le BEREC est un outil *open source* de mesure de qualité de service internet (mesure de débit, latence, etc.), qui intègre également des indicateurs d'usage (navigation web, *streaming* vidéo, etc.) et des indicateurs liés à la neutralité du net (blocage de ports, détection de *proxy*, manipulation DNS, etc.). Au début de l'année 2020, le BEREC a apporté les dernières modifications au code de cet outil, qui est disponible sur Git Hub : https://github.com/net-neutrality-tools/nntool.

Cet outil est mis à disposition des autorités de régulation nationales (ARN) des différents États membres qui peuvent l'adopter, sur base volontaire. Le BEREC a ainsi mis en place un groupe de travail pour coordonner les différents projets nationaux de mise en place d'outil de mesure de qualité de service. Au-delà d'être un cadre d'échange et de partage d'expériences et de bonnes pratiques entre experts, le BEREC se propose de répertorier toutes les initiatives nationales et de suivre les différents projets de développement de nouveaux outils par les différentes autorités européennes.

Par ailleurs, les travaux sur l'outil de mesure BEREC ont souligné l'importance de mettre à jour la méthodologie de mesure de la qualité de service préconisée par le BEREC en 2017 – BoR (17) 178 – pour prendre en compte notamment les évolutions technologiques, plus spécifiquement dans la mesure d'indicateurs de qualité de service et en particulier de débit. Cette mise à jour s'appuiera aussi sur la publication des lignes directives du BEREC détaillant les paramètres de qualité de service publiées en 2020 – BoR (20) 53 –. Un rapport sur la méthodologie sera publié début 2022 et pourrait permettre d'alimenter la prochaine édition du Code de conduite de la qualité de service d'internet de l'Arcep.

Plus généralement, les travaux au sein du BEREC devraient faciliter l'adoption d'un outil de mesure qui pourrait devenir à terme un nouveau dispositif de diagnostic de l'Arcep sur les volets de qualité de service et de neutralité du net.

4 L'impact du choix de la mire de test

Le choix de la « mire de test », c'est-à-dire le serveur avec lequel le test de qualité de service réalise les mesures de débit descendant, de débit montant et de latence est important. C'est un facteur qui conditionne le résultat de la mesure.

4.1 Impact de la bande passante entre une mire et internet

Une mire doit avoir suffisamment de bande passante disponible pour ne pas être un facteur limitant. En particulier, c'est le cas quand la capacité de la mire est inférieure ou égale à celle de la ligne testée.

Pour donner un exemple concret : un test sur une ligne FttH qui permettrait un débit de 1 Gbit/s sera limité à 500 Mbit/s, si deux clients FttH effectuent simultanément ce même test sur une mire qui serait connectée à internet avec seulement 1 Gbit/s.

L'Arcep a ainsi travaillé avec l'ensemble de l'écosystème pour ajouter dans le Code de conduite 2020 un ensemble de nouveaux critères de transparence minimum sur les mires utilisées par les outils de mesure, afin que l'utilisateur soit informé de la bande passante de chaque mire proposée en France par l'outil de test de la qualité de service utilisé.

Le Code de conduite 2020 recommande une capacité minimale de 1 Gbit/s pour la mire de test afin de réduire le nombre de mesures où celle-ci est l'élément limitant.

4.2 Impact de la localisation des mires de test

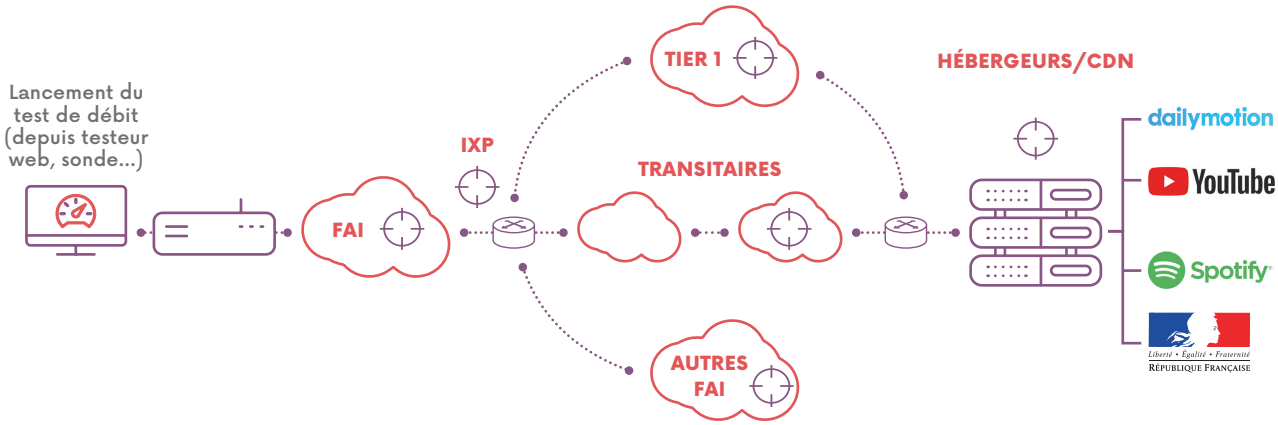
La localisation de la mire est primordiale pour le calcul de la latence car celle-ci dépend principalement du trajet parcouru par l'information entre le client et la mire. La localisation influe également sur la montée en débit et donc sur le débit moyen. La localisation est moins importante pour les outils qui affichent le débit en régime établi.

Comme explicité sur le schéma ci-dessous, les mires de test peuvent être localisées à différents endroits :

- dans le réseau du FAI de l'utilisateur : le résultat du test ne dépend que du FAI mais il est très peu représentatif d'un usage réel des services internet, souvent hébergés au-delà de ce simple réseau ;
- dans le réseau d'un autre FAI directement interconnecté (par *peering*) avec le FAI de l'utilisateur : le test prend non seulement en compte le réseau du FAI de l'utilisateur mais également la qualité du réseau et de l'interconnexion avec un autre FAI ; ce test est le plus souvent très peu représentatif d'un usage réel des services internet ;
- à un point d'échange internet (IXP, pour *Internet Exchange Point*) : le réseau testé ne dépend pratiquement que du FAI et se rapproche d'un usage réel, une partie du trafic internet passant par les IXP ;
- dans le réseau d'un transitaire : le test n'est pertinent que si le transitaire échange beaucoup de trafic avec le FAI de l'utilisateur ; il est à noter que les observatoires réalisés par des transitaires (comme l'observatoire d'Akamai) représentent uniquement la qualité de service vers un point précis de l'internet ; - dans le réseau d'un Tier 1 : le réseau testé va au-delà des seules performances du réseau du FAI ; les mesures sont encore plus représentatives d'un usage réel que lorsque les mires sont placées à un IXP ;
- au plus proche des serveurs des fournisseurs de contenu et d'applications : le réseau testé est celui emprunté de bout en bout jusqu'à un hébergeur donné ; les tests sont donc très représentatifs d'un usage en particulier (l'observatoire de Netflix, par exemple, donne uniquement une mesure de la qualité vers son service).

L'emplacement géographique est trompeur. Prendre le serveur géographiquement le plus proche de son domicile ne signifie pas que le serveur est proche d'un point de vue réseau. Par exemple, un habitant de Nice peut penser pertinent d'utiliser un serveur hébergé dans sa ville. Toutefois, il est tout à fait possible qu'il soit nécessaire de passer par Paris pour joindre ce serveur si ce dernier n'est pas hébergé sur le réseau de son fournisseur d'accès à internet.

IMPACT DE LA LOCALISATION DES MIRES DE TEST



Source : Arcep

QUELQUES EXEMPLES DE BIAIS LORS DES MESURES DE QUALITÉ DE SERVICE INTERNET

Les éléments et résultats présentés ci-dessous ont vocation à illustrer le potentiel impact du navigateur choisi par l'utilisateur pour effectuer les mesures de débit dans une configuration de test donnée. Ils ne doivent être considérés que dans le cadre de la configuration de test retenu et en tout état de cause :

- **ne permettent pas de comparer les performances des navigateurs testés, mais visent à souligner les biais potentiellement induits par les navigateurs lors d'une mesure de débit ;**
- **ne sont pas représentatifs de la qualité de service perçue par l'utilisateur final ni du débit réel que le navigateur permet d'atteindre grâce à sa connexion internet.**

Les mêmes réserves s'appliquent aux autres paramètres étudiés (outils de tests de débit, systèmes d'exploitation, bloqueurs de publicité, etc.).

Sur de nombreux tests de débit de connexion à 1 Gbit/s, la limitation de débit n'est pas liée au réseau de l'opérateur ou à la mire utilisée, mais au PC de test. Ce phénomène est encore plus présent sur des connexions à 10 Gbit/s, où les équipements utilisés par le client sont généralement limitants.

Les versions sorties fin mai 2021 des navigateurs web ont apporté des changements importants, notamment en termes de performance et de design.

Les éléments présentés ci-dessous visent à fournir des éléments concernant l'impact du navigateur sur les mesures de débit en testant les performances des nouvelles versions des navigateurs populaires avec les deux outils de test de débit multi-hébergeurs les plus utilisés en France pour tester sa connexion internet (« outil n° 1 » et « outil n° 2 » ci-après) et de les comparer à la version installable sous Windows 10 et Ubuntu de ces mêmes outils (respectivement « outil installable n° 1 » et « outil installable n° 2 » ci-après).

L'environnement de test mis en place

Le PC qui réalise les tests présentés ci-dessous est un Nuc (mini PC) Intel de 2015[1], équipé d'un processeur Celeron N2820, processeur limité en performance, mais représentatif de la puissance de millions de PC portables d'entrée de gamme (notamment sur le segment populaire « ultraportable »). Le PC est équipé de 4 Go de ram et d'un disque de type SSD, ce qui est représentatif de ce type d'ordinateur dédié à un usage bureautique. Un dual Boot Windows 10 + Ubuntu 18.04 LTS est installé, ce sont les deux systèmes d'exploitation habituellement préinstallés sur ce type de PC.

Afin de se concentrer sur les limites introduites par le client, ces tests sont réalisés en connectant directement le client au serveur, dédié au test, *via* un câble Ethernet. Une latence fixe de 10 ms est ajoutée *via* NetEm[2].

Une telle configuration permet de s'affranchir dans une très large mesure des éventuels biais de mesure qui pourraient être liés au réseau.

Avant de réaliser les tests, toutes les mises à jour disponibles sont installées et les « maintenances » et « recherches de mises à jour » qui peuvent se déroulent en arrière-plan sont forcées, afin d'éviter qu'elles ne se produisent pendant le test, ces process en arrière-plan pouvant impacter les résultats. Le PC est redémarré et laissé au repos (navigateur ouvert) 10 minutes entre chaque série de test. Les données publiées sont une moyenne des données relevées sur 20 tests de débit.

1. Un Nuc Intel DN2820FYKH est utilisé, avec les derniers drivers proposés par Intel et le dernier BIOS disponible.
2. La commande «sudo tc qdisc add dev eth0 root netem delay 10ms » est utilisée sur le serveur (Ubuntu server 20.04 LTS) pour retarder de 10ms chaque paquet envoyé sur la carte réseau 10 Gbit/s du serveur.

Outil de test n° 1[3]

L'outil n° 1 affiche 5 publicités pendant le test de débit, dans sa version web. Les tests ont été réalisés sur chaque navigateur avec et sans un bloqueur de publicité populaire[4], afin de mettre en évidence les impacts de ce type d'extension sur la mesure de débit.

Le trafic est systématiquement chiffré dans un navigateur web (il n'est pas possible de faire un test de débit HTTP dans une page web HTTPS), tandis qu'il est en clair avec l'outil installable n° 1.

Voici les résultats des différentes séries de test, classées par débit descendant croissant :

OUTIL DE TEST DE DÉBIT N° 1



Source : Arcep

Les conclusions que nous pouvons tirer de ces tests sont les suivantes :

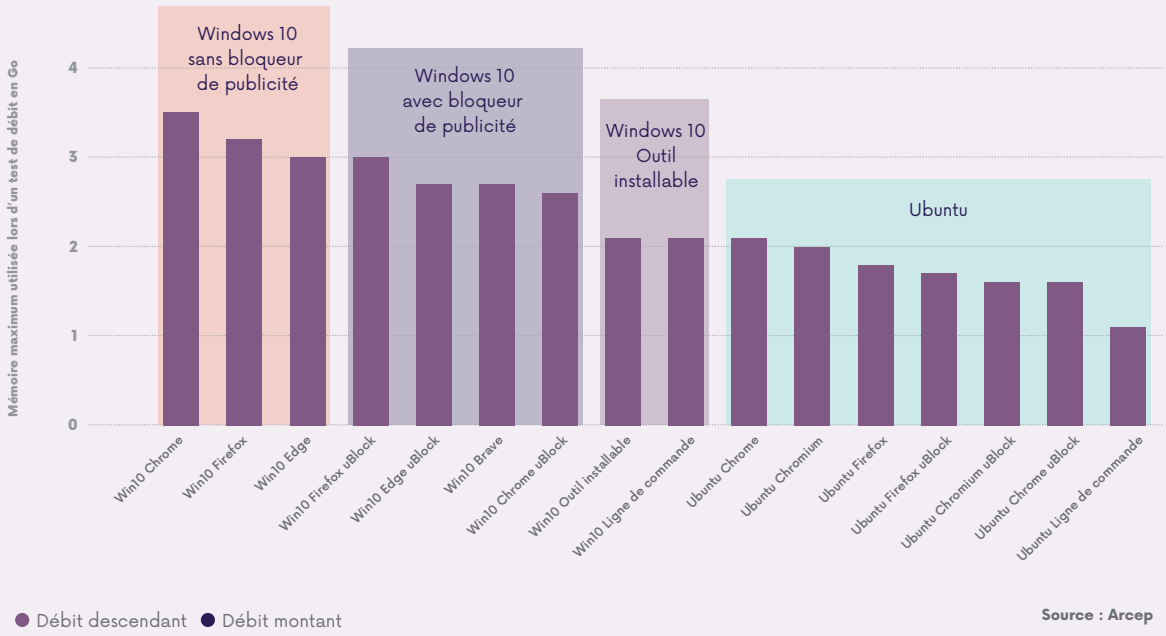
- Le choix d'un test mono-connexion ou multi-connexions (16 connexions TCP en parallèle) a peu d'impact sur les performances sur notre connexion réseau. La différence entre les deux pourrait être plus importante si la connexion internet avait des pertes de paquets.
- Firefox est peu impacté par les publicités, c'est le navigateur qui affiche le meilleur débit descendant sans bloqueur de publicité : entre 106 et 127 Mbit/s. Cela reste toutefois très éloigné du débit réel de 1 Gbit/s.
- Les navigateurs basés sur Chromium (Chorme, Edge, Brave[5], Chromium) sont fortement impactés par la publicité avec des débits descendants entre 12 et 71 Mbit/s. Ces mêmes débits sont entre 161 et 208 Mbit/s avec un bloqueur de publicité.
- L'outil installable n° 1, que ce soit dans la version avec interface graphique ou la version ligne de commande permet d'obtenir un débit fiable de plus de 940 Mbit/s symétrique. Ce débit, bien plus important que dans un navigateur est lié au fait qu'un navigateur est un logiciel complexe, reposant sur un ensemble de composants tels, par exemple, qu'une *sandbox* (mécanisme de sécurité informatique se basant sur l'isolation de composants logiciels) qui n'a pas pour objectif de réaliser un test de débit. Un autre facteur de gain de performances est l'absence d'obligation de chiffrement (HTTPS) des données quand on est dans un outil installable (le chiffrement n'est pas activé dans l'outil installable n° 1).

3. Le nom des outils n'est pas précisé ici, l'objectif étant de comparer les navigateurs web et la version installable et non les outils n°1 et n°2 entre eux.
4. uBlock Origin est le bloqueur de publicité utilisé sur Firefox, Chrome, Chromium et Edge. C'est le bloqueur de publicité le plus utilisé sous Firefox, selon addons.mozilla.org.
5. Le navigateur Brave intègre nativement un bloqueur de publicité, activé par défaut, et a été testé uniquement avec le bloqueur de publicité activé.

L'utilisation de la mémoire vive (*RAM*) lors d'un test est un élément qui peut avoir son importance. En cas de manque de mémoire vive, les performances vont être dégradées car le système fait appel à un espace d'échange situé sur disque, bien plus lent que la mémoire vive.

On relève ici la consommation mémoire maximum pendant un test de débit. La consommation varie de 1,1 Go à 3,5 Go selon le navigateur utilisé. Cela inclut la consommation de mémoire par le système d'exploitation[6]. Il est donc important pour un utilisateur d'un PC de 4 Go de RAM de fermer tous les logiciels et onglets du navigateur avant de démarrer un test de débit. À noter que la consommation de mémoire peut, pour certains outils, varier en fonction du débit. 4 Go de RAM peut donc se révéler insuffisant pour mesurer un débit de 1 Gbit/s dans un navigateur web sous Windows 10.

MÉMOIRE UTILISÉE LORS D'UN TEST MULTI-CONNEXIONS



Source : Arcep

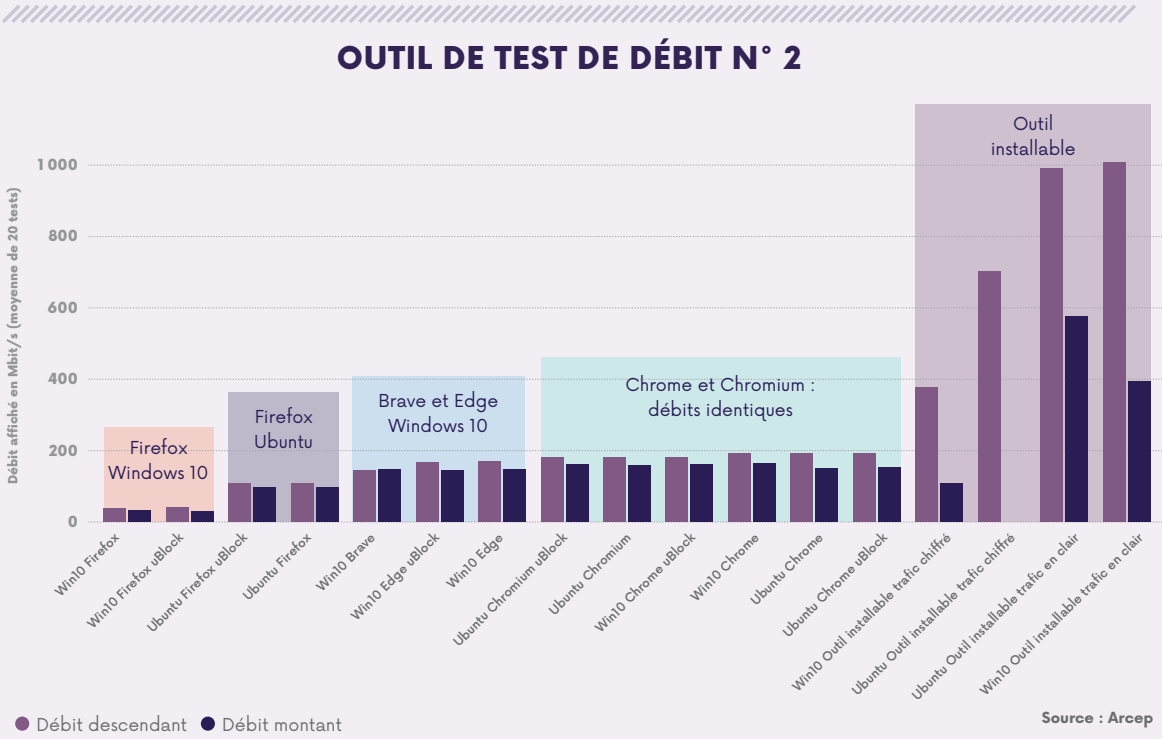
Outil de test n° 2

L'outil n° 2 n'affiche pas de publicité pendant le test de débit. Les tests ont été réalisés avec et sans un bloqueur de publicité, afin de mettre en évidence l'impact potentiel de l'extension bloqueur de publicité qui doit inspecter les connexions entrantes pour supprimer les éléments interdits par sa liste. Les tests montrent que son impact est négligeable : en absence de publicité, les débits ne sont pas significativement dégradés par uBlock.

Contrairement à l'outil n° 1, l'outil n° 2 ne permet pas de faire des tests mono-connexion. Tous les tests sont réalisés avec 16 connexions TCP en parallèle. Par contre l'outil installable n° 2[7] propose de réaliser les tests en HTTP et en HTTPS, ce qui est testé (le trafic est systématiquement chiffré dans un navigateur web).

6. À vide, sans aucune application lancée, Windows 10 affiche une consommation mémoire de 1,9 Go et Ubuntu 1,0 Go.
7. L'outil installable n°2 est une version beta, la version finale n'étant pas disponible en juin 2021. L'éditeur nous a prévenu que la partie de test du débit montant n'était pas finalisée, les performances du débit montant devraient être améliorée dans la version finale.

Voici les résultats des différentes séries de test, classées par débit descendant croissant :



Source : Arcep

Les conclusions que nous pouvons tirer de ces tests sont les suivantes :

- Firefox sous Windows 10 a des débits très limités dans les conditions de test, inférieurs à 40 Mbit/s dans le sens descendant. Sous Ubuntu, les débits sont légèrement supérieurs, mais restent inférieurs à 108 Mbit/s. Cette limitation peut entraîner un fort biais de mesure.
- Brave[8] et Edge permettent d'avoir un débit descendant entre 143 et 170 Mbit/s.
- Chrome et Chromium affichent le meilleur débit descendant : entre 181 et 192 Mbit/s. Cela reste toutefois très éloigné du débit réel de 1 Gbit/s.
- L'outil installable n° 2 permet d'atteindre le débit maximum quand le trafic est en clair (HTTP) avec plus de 992 Mbit/s[9]. Quand le trafic est chiffré (HTTPS), les débits baissent : 376 Mbit/s sous Windows 10 et 703 Mbit/s sous Ubuntu. Cela reste bien supérieur au trafic chiffré dans un navigateur web (192 Mbit/s dans le meilleur des cas).

Conclusion

Pour réaliser un test sur un PC limité en performance ou pour réaliser un test de débit à plus de 1 Gbit/s, l'outil installable est le meilleur choix pour fiabiliser la mesure. Attention, même si le test est plus fiable que dans un navigateur, d'autre biais qui ne sont pas la responsabilité de votre fournisseur d'accès à internet peuvent influencer la mesure de débit :

- **des biais liés à des logiciels installés. Par exemple des anti-virus, *firewalls* ou des VPN qui peuvent fortement dégrader un test de débit. Il est possible de s'affranchir de ces biais en démarrant sur une clef USB bootable un environnement propre[10] ;**
- **des bais liés au système d'exploitation ;**
- **des biais provenant du choix de la mire de test (voir paragraphe dédié dans ce rapport) ;**
- **des biais provenant du réseau local ou de la carte réseau (Wi-Fi ou filaire) du PC utilisé. Par exemple, une carte réseau 10 Gbit/s peut être limitée par le lien qui relie la carte réseau au processeur.**

8. Le navigateur Brave intègre nativement un bloqueur de publicité, activé par défaut, qui empêche la réalisation du test nPerf. Les tests ont donc été réalisés avec ce bloqueur de publicité désactivé.
9. Ce débit est au-dessus du débit maximum théorique possible sur une carte réseau 1 Gbit/s, toutefois la version installable est une version beta, la version finale n'étant pas disponible en juin 2021.
10. Voir tutoriel Arcep « Création d'une clef USB bootable pour réaliser un test de débit fiable ».

5 Le suivi par l'Arcep de la qualité de l'internet mobile

Si les cartes de couverture mobile, réalisées à partir de simulations numériques des opérateurs et vérifiées par l'Arcep, donnent une information nécessaire sur l'ensemble du territoire, elles présentent des visions simplifiées de disponibilité des services mobiles ; l'Arcep travaille en permanence à leur enrichissement et à leur amélioration – notamment en augmentant le seuil de fiabilité des cartes de couverture, passé ainsi de 95 % à 98 % en 2020 – mais elles ne représenteront jamais parfaitement la réalité. Ces cartes doivent ainsi être complétées par les données relatives à la qualité de service. Réalisées en conditions réelles, les mesures de qualité de service n'offrent pas une vision exhaustive du territoire, mais permettent de connaître de façon précise le niveau de service proposé par chaque opérateur dans tous les lieux mesurés. Depuis 1997, l'Arcep mène, chaque année, une campagne d'évaluation de la qualité des services mobiles des opérateurs métropolitains. Les mesures réalisées visent à évaluer la performance des réseaux des opérateurs de manière strictement comparable, et ce dans différentes situations d'usage (en ville, en zone rurale, dans les transports, etc.) et pour les principaux services utilisés (appels, SMS, chargement de page web, *streaming* vidéo, téléchargement de fichiers, etc.). Cette enquête s'inscrit dans la stratégie de régulation par la donnée de l'Arcep et permet d'éclairer les utilisateurs. Pour l'année 2020, plus d'un million de mesures en 2G, 3G et 4G ont été réalisées sur l'ensemble du territoire, dans tous les départements (à l'intérieur et à l'extérieur des bâtiments) et dans les transports (métros, TGV, routes). En 2017, l'Arcep a lancé son outil cartographique et interactif monreseaumobile.fr, qui permet de visualiser les cartes de couverture mobile des opérateurs ainsi que l'ensemble des données de cette enquête de qualité de service. Depuis juillet 2018, les territoires d'outre-mer y figurent également.

Ces mesures permettent d'évaluer la progression de la qualité de service des différents réseaux alors que le smartphone est devenu le principal moyen d'accès à internet, rendant ainsi compte des efforts d'investissement des opérateurs sur leur réseau.

5.1 En Métropole, la qualité de service continue de progresser pour l'ensemble des opérateurs, mais le rythme s'est légèrement ralenti

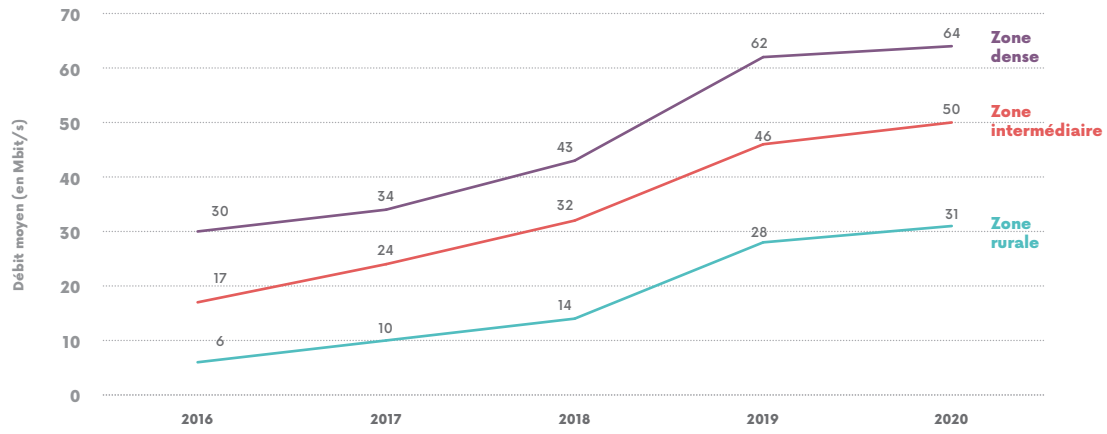
La qualité des services de l'internet mobile continue de s'améliorer globalement pour tous les opérateurs, et ce dans toutes les zones : rurales, intermédiaires et denses, mais à un rythme moindre que les années précédentes. Cela peut s'expliquer notamment par le contexte sanitaire et un durcissement de certains protocoles de mesure pour être au plus proche de l'expérience utilisateur (en particulier, de nouvelles configurations des serveurs à partir desquels les tests de débit ont été effectués). Les débits descendants atteignent ainsi en moyenne 49 Mbit/s, contre 45 Mbit/s en 2019.

À noter également cette année : la qualité de service internet a progressé dans les métros. En 2020, Paris et Lyon ont rejoint Toulouse et Rennes parmi les « métros 4G » avec l'achèvement de leurs programmes de couverture 4G du métro respectivement fin 2019 pour Lyon et en juin 2020 pour Paris.

5.2 Outre-mer, la progression de la qualité de service internet est contrastée

Certains indicateurs comme le débit moyen continuent de progresser, mais la navigation web ou le *streaming* semblent stagner, voire sont parfois moins bons qu'en 2019. Cela peut s'expliquer par la période de mesures (septembre-décembre en 2020, contre juillet-août en 2019) et aux effets de la crise sanitaire, qui a augmenté la pression sur les réseaux.

PROGRESSION DES DÉBITS MOYENS EN TÉLÉCHARGEMENT PAR ZONE



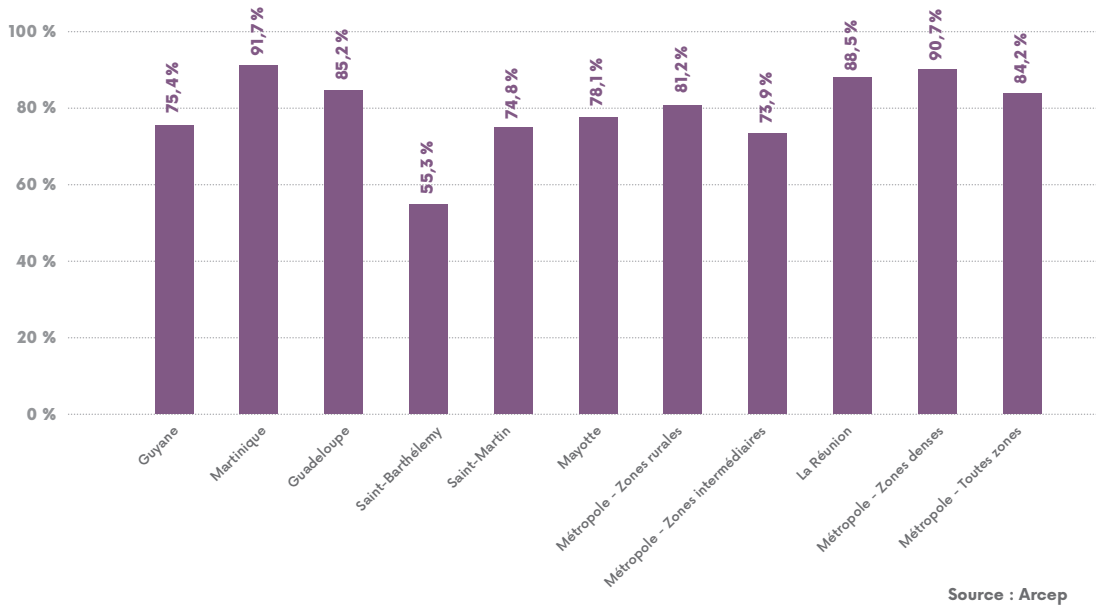
Source : Arcep

Un nouvel indicateur pour la campagne Arcep, en métropole et en outre-mer : le taux de tests dépassant les 3 Mbit/s

L'indicateur présentant le *débit moyen* est une information intéressante mais qui n'illustre qu'un volet de la qualité de service. Par exemple, un opérateur qui couvre peu mais offre des débits très élevés dès lors que l'utilisateur est couvert, peut présenter un débit moyen similaire à un opérateur avec une couverture large mais avec des débits plus faibles. L'expérience utilisateur sera cependant différente entre ces deux opérateurs.

Pour compléter l'information apportée par le débit moyen, l'Arcep a introduit en 2020 un nouvel indicateur : le *taux de débits dépassant un seuil minimal*. Ce seuil est considéré, dans les résultats de cette enquête, à 3 Mbit/s car un débit supérieur à 3 Mbit/s permet dans la plupart des cas d'assurer les usages internet mobile « standards » comme naviguer sur le web, lire ses mails, et de regarder la majorité des vidéos en 720p sans ralentissement majeur.

TAUX DE TESTS DE DÉBIT DESCENDANT ≥ 3 MBIT/S



Source : Arcep

5.3 L'enrichissement de « Mon réseau mobile »

Depuis fin 2018, l'Arcep a engagé des travaux pour faire évoluer « Mon réseau mobile ». En premier lieu, l'Arcep a publié un « Kit du régulateur » pour répondre aux attentes des territoires qui souhaitent effectuer leurs propres mesures, notamment pour identifier leurs besoins de couverture dans le cadre du *New Deal* mobile. Ce Kit comprend des modèles de cahiers des charges techniques, pouvant être réutilisés simplement dans le cadre de marchés relatifs à la sélection d'un prestataire pour réaliser une campagne de mesures sur le terrain. De premiers acteurs, tels que la SNCF et certaines collectivités territoriales, se sont saisis de ce document pour faire réaliser leurs propres mesures de connectivité. L'Arcep a engagé des discussions avec ces acteurs et depuis avril 2020, « Mon réseau mobile » s'est enrichi des données de mesure de plusieurs territoires : le Cher, les Hauts-de-France, les Pays de la Loire et l'Auvergne-Rhône-Alpes. Sont également accessibles des données de mesures sur le réseau SNCF. Ces données ont été actualisées en mars 2021, avec également l'ajout sur « Mon réseau mobile » des données de l'acteur privé QoSi – Mozark Group, qui a partagé avec l'Arcep les résultats de campagnes de terrain qu'il réalise pour son propre compte. « Mon réseau mobile » continuera à s'enrichir en intégrant les mesures de qualité de service mobile réalisées conformément au « Kit du régulateur ».

L'Arcep a également publié un Code de conduite à destination des acteurs qui proposent des applications de mesure de l'expérience mobile, comme des tests de débit en *crowdsourcing* que chacun peut réaliser sur son téléphone. Ce document a pour objectif d'assurer un niveau minimal d'exigence en matière de pertinence, de présentation et de transparence des mesures. À l'heure actuelle, cinq acteurs ont déclaré leurs outils conformes au Code de conduite 5GMark (QoSi, nPerf, 60 Millions de consommateurs, Speedtest by Ookla et Tutela). Les solutions proposées par ces acteurs ont été adoptées par certains territoires tels que les Hauts-de-France ou l'Ille-et-Vilaine.

J'alerte l'Arcep

Lancée en octobre 2017, la plateforme « J'alerte l'Arcep » est à disposition de chaque citoyen, de chaque entreprise ou de chaque collectivité qui souhaite remonter du terrain tout problème lié à l'internet mobile, à l'internet fixe ou aux services postaux. L'Arcep a dressé le bilan 2020 de son action au profit des consommateurs et de sa plateforme de signalement « J'alerte l'Arcep »*. En 2020, plus de 33 000 signalements ont été transmis à l'Arcep. De ces signalements, 40 % concernent un problème lié à qualité et la disponibilité des services fixes ou mobiles.

Ces remontées constituent un élément important dans la capacité de diagnostic de l'Arcep. En effet, elles permettent de quantifier et identifier les difficultés rencontrées par les utilisateurs afin d'orienter ses actions vers les solutions les plus appropriées possible. Les signalements sont notamment une source utile aux services de l'Autorité pour identifier les infractions potentielles au règlement internet ouvert et son principe de neutralité du net (cf. chapitre 4 de ce rapport). La plateforme a aussi été mobilisée pendant la crise sanitaire, notamment en transmettant aux opérateurs les alertes identifiées comme prioritaires (professions médicales ou paramédicales, collectivités territoriales, services de l'État). Une cinquantaine d'alertes concernant ces profils ont été transmises. Les opérateurs ont assuré un suivi individuel de ces alertes.

L'Arcep a lancé en novembre 2020 une nouvelle version de « J'alerte l'Arcep », en tirant profit des trois années d'expérience et de recul pour améliorer et enrichir le fonctionnement de cette plateforme de signalement. La plateforme est désormais ouverte à de nouveaux publics qui pourraient alerter le régulateur (marché de la distribution de la presse, profils développeurs, opérateurs, associations de consommateurs). Le parcours utilisateur a aussi été fluidifié et rendu accessible aux publics porteurs de handicaps. Une intégration aux autres outils de régulation par la donnée développés par l'Arcep est également prévue (Mon réseau mobile, Carte fibre, Ma connexion internet et Wehe). Enfin, le traitement des données par l'Arcep a été repensé pour gagner en efficacité.

* Bilan 2020 des actions de l'Arcep vis-à-vis des consommateurs et de la plateforme « J'alerte l'Arcep » : https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/regulation-par-la-data-290421.html

Tutoriel

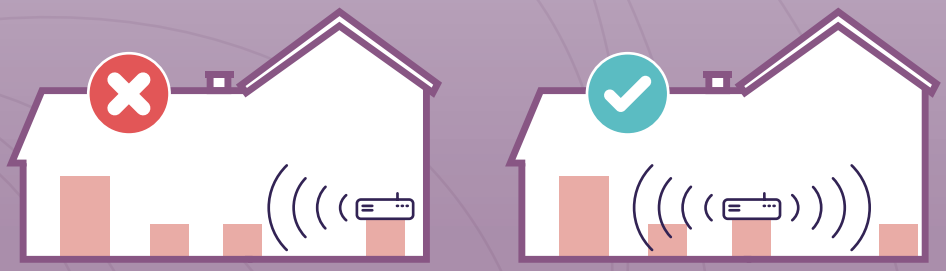
POUR AMÉLIORER LA QUALITÉ DE SON WI-FI

Les deux solutions les plus courantes pour connecter un ordinateur à une box sont le Wi-Fi et la connexion directe *via* un câble Ethernet. Le câble Ethernet, connecté à la box, *via* éventuellement le précâblage Ethernet réalisé dans les logements neufs ou rénovés, est la solution à privilégier dans la mesure du possible. L'accès direct par Ethernet permet généralement d'avoir un accès plus stable, un débit plus important et laisse le spectre Wi-Fi libre pour les terminaux qui en ont besoin. Les ordinateurs portables sont de moins en moins souvent pourvus d'un port Ethernet, toutefois des adaptateurs USB sont disponibles à petit prix pour connecter un PC qui en est dépourvu. L'Ethernet 1 Gbit/s est aujourd'hui la norme, mais l'Ethernet à 2,5 Gbit/s commence à arriver sur les nouveaux produits et certaines box sont aujourd'hui compatibles.

CINQ ASTUCES POUR OPTIMISER LA QUALITÉ DE SON SIGNAL WI-FI

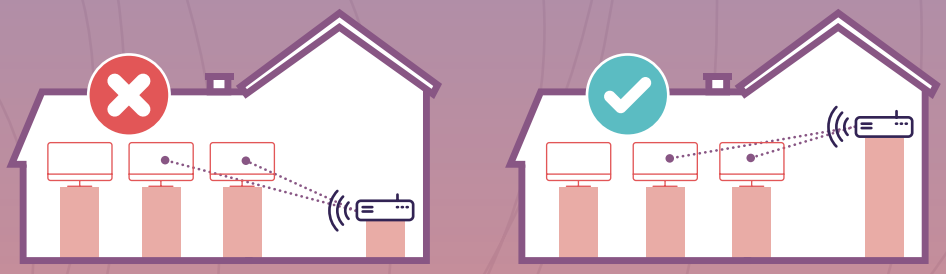
01. Placer la box dans une pièce centrale du logement

Il est recommandé de placer la box dans une pièce centrale du logement afin de limiter les obstacles que le Wi-Fi rencontre pour se connecter aux terminaux. En effet, les murs atténuent le signal radio et diminuent sensiblement le débit internet reçu par les équipements situés dans les pièces les plus éloignées. Ainsi, placer la box à l'extrémité du logement ou dans un local fermé ne permet pas de tirer le meilleur parti du réseau Wi-Fi.



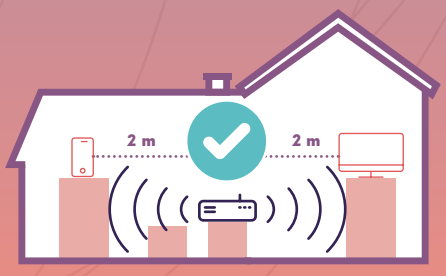
02. Mettre la box dans un endroit aussi dégagé que possible

Pour les mêmes raisons, il est recommandé de mettre la box dans un endroit aussi dégagé que possible, idéalement en hauteur. À l'inverse, mettre la box au sol, entre des livres, dans un meuble TV ou près de meubles hauts dégrade le signal Wi-Fi et l'expérience utilisateur.



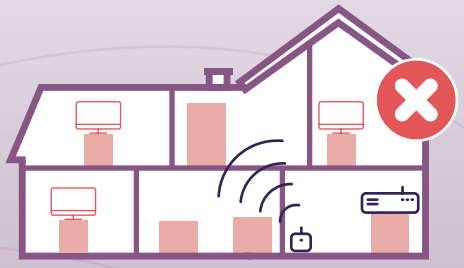
03. Éloigner la box d'autres équipements sans fil

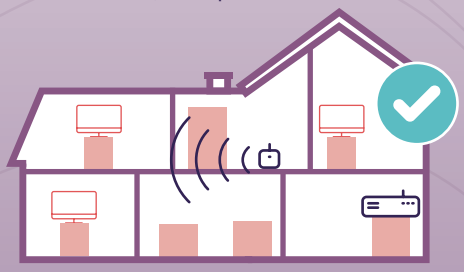
Afin de bénéficier des capacités maximales de son accès, il est également souhaitable de laisser un espace d'environ 2 mètres entre la box et d'autres équipements radio comme la base d'un téléphone sans fil, un babyphone, un micro-onde, etc. Ainsi, les interférences entre les différentes ondes radio seront limitées et le signal Wi-Fi optimisé.

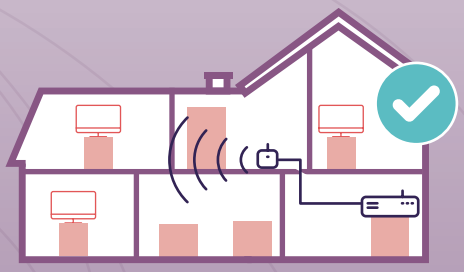


04. Utiliser un répéteur Wi-Fi

Si le débit internet est faible dans certaines pièces éloignées de la box, il est recommandé d'utiliser un répéteur Wi-Fi servant à étendre la couverture du Wi-Fi.
Afin que votre répéteur Wi-Fi puisse fonctionner, il doit être placé environ à mi-distance entre votre box et la zone à couvrir. S'il est trop près de votre box, il ne va pas étendre votre Wi-Fi. S'il est trop loin, il captera mal le Wi-Fi de votre box et le débit répété sera faible.
Pour plus de débit, il est préférable de connecter le répéteur Wi-Fi avec un câble Ethernet longue distance à la box : le câble Ethernet transporte le signal sur un maximum de 100 mètres, sans perte de débit.







05. En cas de renouvellement de votre PC, vérifiez qu'il est compatible avec le Wi-Fi 6 (802.11ax) ou le tout dernier Wi-Fi 6E

Il est recommandé de privilégier les ordinateurs compatibles avec la norme Wi-Fi 6 (802.11ax) ou la norme Wi-Fi 6E. Cette norme est plus performante que les normes précédentes, en augmentant le débit et réduisant la latence. Par ailleurs, elle est rétro-compatible avec toutes les anciennes normes, comme le Wi-Fi 5 (802.11ac) ou le Wi-Fi 4 (802.11n). Le Wi-Fi 6E est un Wi-Fi 6 qui rajoute la compatibilité avec la bande de fréquence à 6 GHz découpée en 3 canaux super-larges de 160 Mhz permettant plus de débit et de libérer les fréquences plus basses pour les équipements non compatibles.

À SON DOMICILE, FAUT-IL DE PRÉFÉRENCE UTILISER LE WI-FI OU LE RÉSEAU 4G/5G DE SON OPÉRATEUR MOBILE ?

Le Wi-Fi offre de nombreux avantages pour l'utilisateur et fait partie des bonnes pratiques pour limiter l'impact environnemental du numérique :

- Un débit généralement significativement plus important et plus stable que la 4G, à condition d'avoir une box qui propose du très haut débit et un Wi-Fi performant (Wi-Fi 5 ou Wi-Fi 6). La latence, le temps que met le signal pour aller jusqu'au serveur, est également plus faible en FttH qu'en 4G ou même 5G.
- Il n'y a généralement pas de limitation en volume de donnée sur une box fixe, là où la quasi-totalité des offres mobiles ont un « *fair use* » exprimé en nombre de Go par mois au-delà duquel le trafic est soit facturé, soit avec un débit réduit.
- Une moindre consommation de la batterie du terminal utilisé : le Wi-Fi consomme moins d'énergie que l'utilisation du réseau mobile. En sollicitant moins la batterie, sa durée de vie est allongée.
- Une consommation d'énergie plus faible du côté du réseau de l'opérateur :
  - Sur un réseau filaire, la consommation d'énergie est principalement fixe et dépend peu des usages qui en sont faits : 1,8 W par ligne par an pour l'ADSL et 0,5 W par ligne FttH par an, du côté du réseau de l'opérateur[1].
  - Sur un réseau cellulaire, la consommation d'énergie est davantage dépendante des usages, soit environ 600 Wh par Go utilisé[1].
- C'est aussi un acte citoyen de passer en Wi-Fi pour diminuer la saturation de certaines cellules mobiles, en permettant de ne pas dégrader la connexion des utilisateurs sur la même cellule qui n'ont pas d'autres possibilités de connexion.

1. Source : note Arcep « L'empreinte carbone du numérique » du 21 octobre 2019.

CHAPITRE 2

SUPERVISER L'INTERCONNEXION DE DONNÉES

À retenir

Le trafic entrant vers les principaux FAI en France à l'interconnexion a augmenté de plus de **50 %** en un an pour atteindre **27,7 Tbit/s** à fin 2020.

Le trafic provenant des CDN internes au réseau des principaux FAI en France a augmenté de **82 %** en un an pour atteindre **7,1 Tbit/s** à fin 2020.

50 % du trafic vers les clients des principaux FAI en France provient de quatre fournisseurs : Netflix, Google, Akamai et Facebook.

L'interconnexion[1] constitue le fondement d'internet. Elle désigne la relation technico-économique qui s'établit entre différents acteurs pour se connecter et échanger mutuellement du trafic. Elle garantit le maillage global du réseau et permet aux utilisateurs finaux de communiquer entre eux[2].

1 Le rôle des *datacenters* dans l'interconnexion de données

Un *datacenter* (ou centre de données) est une installation hébergeant de nombreux ordinateurs connectés qui travaillent de façon collaborative afin de traiter, stocker et partager des données. Les fournisseurs d'accès à internet (FAI), réseaux de diffusion de contenu (CDN), points d'échange internet (IXP), transitaires, hébergeurs, fournisseurs de contenu et d'applications (FCA) ainsi que les entreprises s'appuient fortement sur les *datacenter*s qui constituent des éléments centraux de la fourniture de services en ligne. Les *datacenters* se sont ainsi imposés comme des acteurs essentiels dans le numérique en général et dans l'écosystème internet en particulier.

De plus, et depuis plusieurs années, le nombre de *datacenters* en France n'a cessé de croître, essentiellement autour des grandes métropoles telles que Paris ou Marseille. Aujourd'hui, on observe une décentralisation en France, notamment dans le cadre de la numérisation des PME et collectivités locales et les perspectives d'usages d'internet qu'ouvre la 5G[3].

Les principaux enjeux dans la conception et le fonctionnement d'un *datacenter* sont notamment :

- la sécurité : garantir la sécurité physique, un contrôle d'accès, une redondance/*backup* de l'infrastructure, et une protection contre les phénomènes naturels (foudre ou inondations) ;
- l'énergie : garantir une alimentation en énergie sans aucune coupure ;
- le contrôle des facteurs environnementaux : proposer un équilibre approprié entre la climatisation, le contrôle de l'humidité et la régulation du débit d'air ;
- l'interconnexion : offrir une possibilité de se connecter à des réseaux de manière sécurisée et avec une capacité de réseau suffisante.

1. Les termes techniques liés à l'interconnexion employés ci-après sont définis dans le baromètre de l'interconnexion de données en France : https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html
2. L'Arcep tient à préciser que le présent rapport concerne uniquement l'interconnexion de données dans le réseau internet et ne s'applique pas à l'interconnexion des réseaux de deux opérateurs pour la terminaison d'appel vocal.
3. Carte des *datacenters* de colocation en France : https://www.datacentermap.com/france/map.html

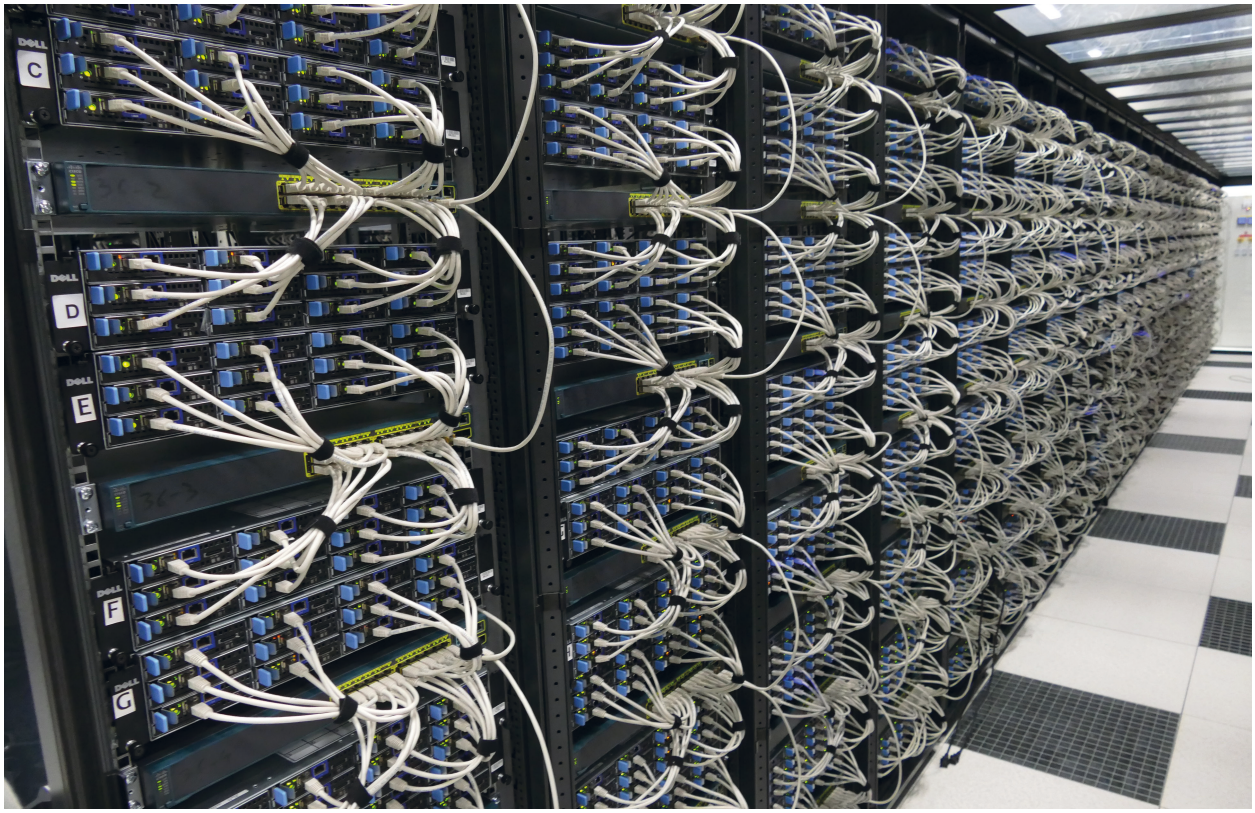
Il existe plusieurs catégories de *datacenters* avec des tailles, des localisations et des modèles économiques différents.

Un *datacenter* est dit neutre s'il permet au client de faire appel directement aux fournisseurs de son choix pour les connexions à internet. Au contraire, certains *datacenters* incluent dans leurs offres un accès à internet (par exemple certains *datacenters* de transitaires).

On distingue deux rôles principaux pour les *datacenters*, le rôle d'hébergement et le rôle d'interconnexion. Les *datacenters* d'interconnexion (ou *datacenters* centraux), tels que Telehouse TH2, Equinix PA2/PA3, Interxion Marseille, le Netcenter SFR de Lyon, le Netcenter SFR de Courbevoie et Interxion PAR2 par exemple, jouent un rôle essentiel dans l'interconnexion des différents acteurs. Véritables carrefours entre les différents acteurs internet et du numérique, ils concentrent de nombreux membres et permettent aux fournisseurs de services et aux utilisateurs de s'interconnecter, que ce soit en *peering* public au niveau d'un IXP, *peering* privé ou transit en fonction des choix métier des acteurs[4]. Offrant plusieurs services (colocation[5], *cross-connect*[6], point d'échange internet, etc.), ces *datacenters* mettent en valeur auprès de leurs clients la fourniture d'une interconnexion directe, en permettant d'acheminer le trafic entre ces acteurs sans passer par internet ou d'autres réseaux.

Ainsi, avec l'évolution des usages, la transformation numérique des entreprises et l'émergence de nouvelles technologies, le rôle des *datacenters* est de plus en plus important pour optimiser l'interconnexion et améliorer la qualité de service pour le client final.

En raison de l'importance croissante de ces acteurs pour les réseaux et services de communication électronique, l'Arcep mènera en 2021 une étude des prestations proposées par les *datacenters* aux opérateurs, afin d'identifier les éventuelles bonnes pratiques ou au contraire, les points d'attention.



4. Cf. « L'interconnexion pour les nuls », Stéphane Bortzmeyer : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/2018-06_Interco_Pour_Les_Nuls_Bortzmeyer.pdf
5. Location d'une salle privée ou partagée au sein d'un *datacenter* pour mettre des équipements informatiques.
6. Options de connectivité directe (fibre optique, câble coaxial ou UTP/STP) entre les membres.

La parole à



SAMI SLIM

*Directeur adjoint - **Telehouse***

L'INTERCONNEXION AU SERVICE DE L'AFFIRMATION DE LA FRANCE ET DE SES TERRITOIRES

Si certains *datacenters* sont appelés cœur de réseau, c'est pour une bonne raison. Ils sont les organes vitaux à la bonne santé numérique d'un pays. Ils sont les garants de son indépendance, de la diversité et de la vivacité de ses acteurs, ainsi que de son poids à l'international. L'histoire de Telehouse le prouve.

Telehouse a été la première entreprise au monde à créer un *datacenter* neutre, un « *carrier hotel* », lors de la vague de dégroupage des télécoms des années 80. Celui-ci a pu offrir une égalité de traitement aux nouveaux entrants. Opérateurs régionaux, nationaux et internationaux ont ainsi pu s'interconnecter dans les mêmes conditions, avec la même qualité de service.

Le *datacenter* s'est alors naturellement transformé en une place de marché. Il a permis la densification et la sécurisation de la connectivité entre les acteurs. À tel point que TH2 est devenu le *datacenter* le plus interconnecté en France et le 4e au niveau mondial.

Au-delà de cette fierté, les enjeux sont vitaux pour la France : il s'agit de renforcer sa souveraineté numérique. Un *datacenter* d'envergure mondiale permet en effet de capter le trafic international et de relocaliser dans l'Hexagone les interconnexions qui font transiter nos données.

En outre, l'architecture historique de fibres optiques irriguant la France depuis Paris, notamment par les voies ferrées et les autoroutes, fait mécaniquement bénéficier les territoires ruraux de la connectivité de la Capitale, et contribue à réduire la fracture numérique entre Paris et le reste de l'Hexagone.

Les régions, à l'inverse, servent aussi la capitale : plusieurs villes de France permettent à Paris de disposer de fenêtres vers l'international. Marseille vers l'Afrique et le Moyen-Orient, Bordeaux vers les Amériques, Lyon vers l'est de l'Europe et Lille vers les pays nordiques. Ces métropoles sont de formidables atouts géographiques qui vont faire de la France un carrefour mondial du numérique.

CLASSEMENT DES VILLES & DES *DATACENTERS* LES PLUS CONNECTÉS AU MONDE EN 2020

VILLE

Capacité d'interconnexion internationale (Gbps)*

1. **Francfort,** Allemagne — **110 608**
2. **Londres,** Royaume-Uni — **74 834**
3. **Amsterdam,** Pays-Bas — **71 188**
4. **Paris,** France — **67 865**
5. **Singapour,** Singapour — **56 350**

* Hors capacité domestique

DATACENTER

Nombre de *peers***

1. **Telehouse Londres** (Dockland) — **821**
2. **Interxion Francfort** (FRA1-14) — **446**
3. **Equinix FR5** (Frankfurt, KleyerStrasse) — **335**
4. **Telehouse Paris 2** (Voltaire) — **282**
5. **Equinix Slough** — **224**

** Source : *Peering* DB

2 État de l'interconnexion en France

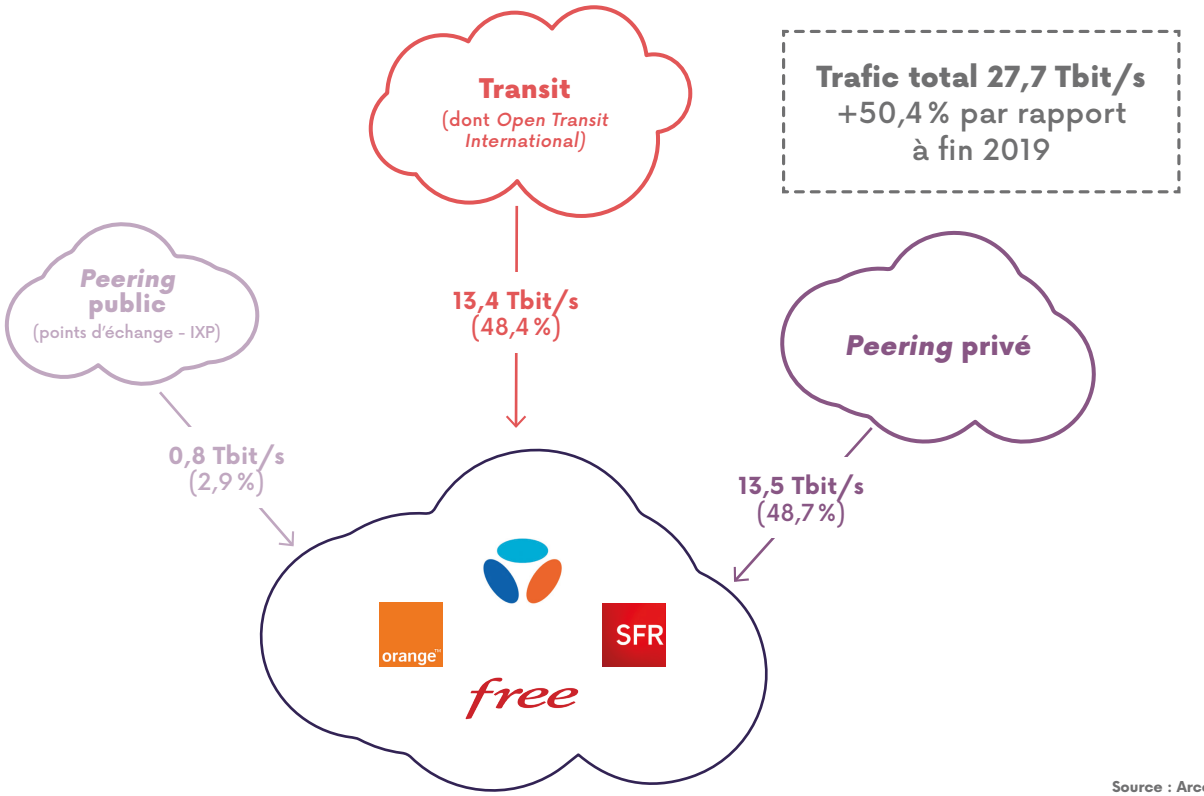
Grâce à la collecte d'information sur l'interconnexion et l'acheminement de données qu'elle réalise, l'Arcep dispose de données techniques et tarifaires sur l'interconnexion du premier semestre de 2012 au second semestre de 2020. Par souci de confidentialité, la publication des résultats[7] ne porte que sur des données agrégées des quatre principaux FAI en France (Bouygues Telecom, Free, Orange et SFR).

2.1 Trafic entrant

Le trafic entrant vers les quatre principaux FAI en France à l'interconnexion est passé de plus 18,4 Tbit/s à fin 2019 à 27,7 Tbit/s à fin 2020, marquant ainsi une augmentation de plus de 50 % en un an (l'augmentation était de 29 % entre 2018 et 2019). Le trafic provient environ pour la moitié des liens de transit. Ce taux de transit assez élevé est dû en grande partie au trafic de transit entre Open Transit International (OTI), Tier 1 appartenant à Orange, et le Réseau de Backbone et de Collecte Internet d'Orange (RBCI), qui permet d'acheminer le trafic vers les clients finaux de ce FAI. Ce taux de transit est beaucoup moins élevé chez les autres FAI qui, n'ayant pas en parallèle une activité de transitaire, font davantage appel au *peering*.

On observe une augmentation importante du trafic (+26 %) au premier semestre 2020, qui pourrait en partie refléter l'augmentation des usages lors du premier confinement en France.

RÉPARTITION DU TRAFIC ENTRANT À L'INTERCONNEXION (AU 95E CENTILE) SUR LE RÉSEAU DES PRINCIPAUX FAI EN FRANCE (FIN 2020)



Source : Arcep

7. Résultats issus des réponses des différents opérateurs à la collecte d'informations sur les conditions techniques et tarifaires de l'interconnexion et de l'acheminement de données, dont le périmètre est explicité dans la décision 2017-1492-RDPI (https://www.arcep.fr/uploads/tx_gsavis/17-1492-RDPI.pdf).

ÉVOLUTION DU TRAFIC ENTRANT À L'INTERCONNEXION VERS LES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2020

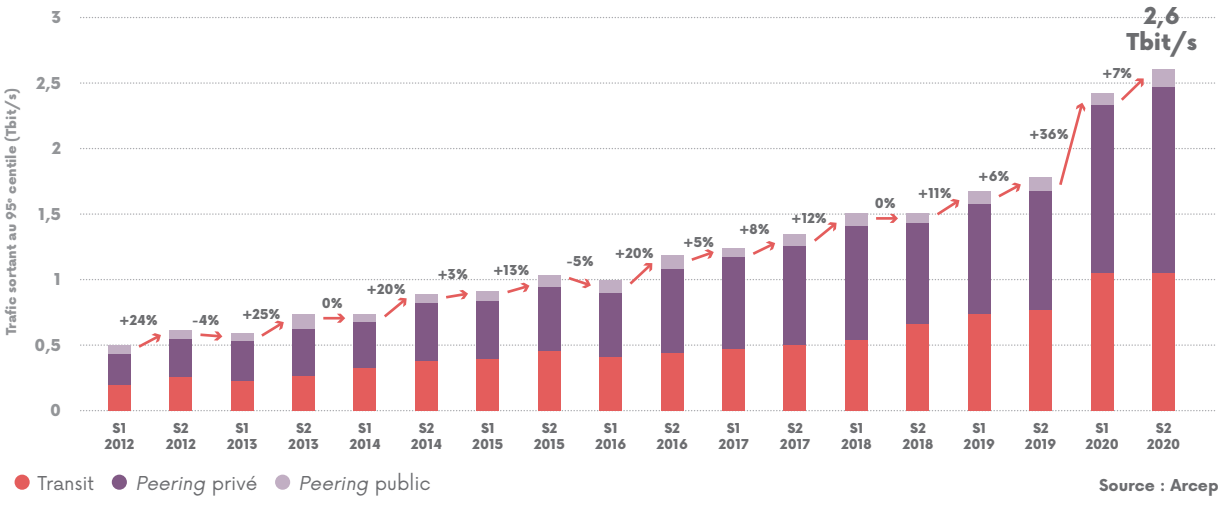


Source : Arcep

2.2 Trafic sortant

À fin 2020, le trafic sortant du réseau des quatre principaux FAI en France à l'interconnexion atteint environ 2,6 Tbit/s, soit une augmentation de 46 % par rapport à fin 2019. Entre 2012 et 2020, ce trafic a été multiplié par 5. On observe une augmentation particulièrement marquée entre le deuxième semestre 2019 et le premier semestre 2020, qui pourrait notamment être liée au début de la crise sanitaire et du confinement du printemps 2020.

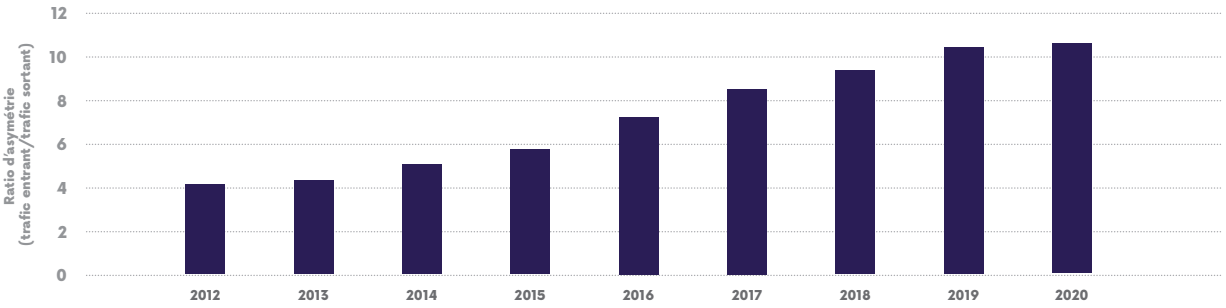
ÉVOLUTION DU TRAFIC SORTANT À L'INTERCONNEXION VERS LES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2020



Source : Arcep

Le trafic sortant est bien inférieur au trafic entrant. Par ailleurs, le taux d'asymétrie entre ces deux trafics est passé de 1/4 en 2012 à plus de 1/10 en 2020. Cette augmentation est due notamment à l'augmentation du contenu multimédia consulté par les clients (*streaming* vidéo et audio, téléchargement de contenu de grande taille, etc.).

ÉVOLUTION DU TAUX D'ASYMÉTRIE ENTRE TRAFIC ENTRANT ET TRAFIC SORTANT À L'INTERCONNEXION POUR LES PRINCIPAUX FAI EN FRANCE ENTRE 2012 ET 2020

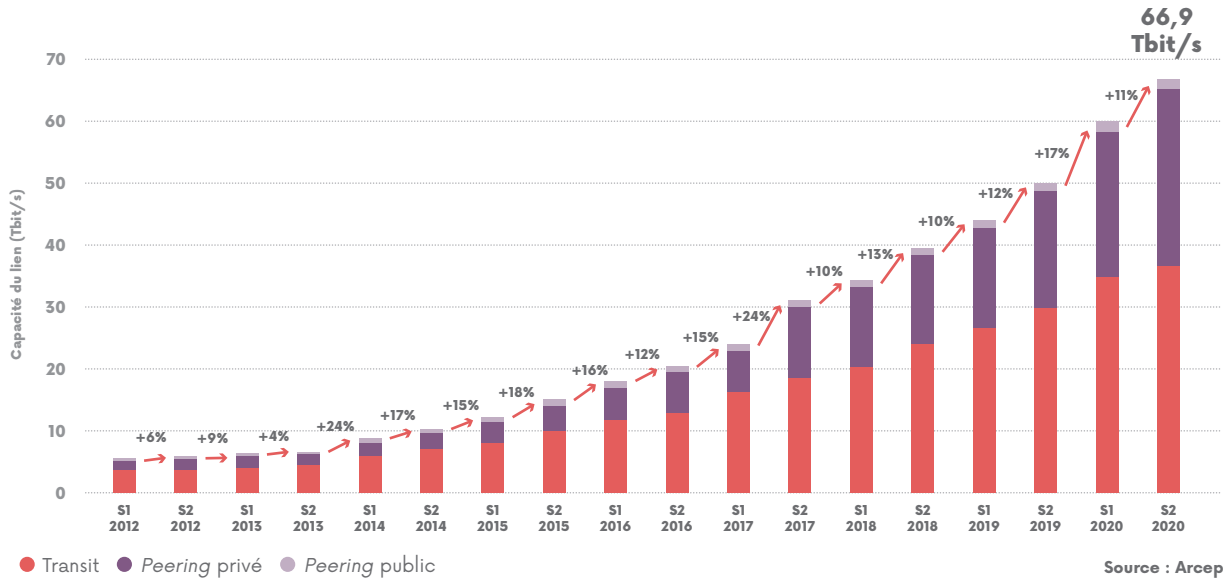


Source : Arcep

2.3 Évolution des capacités installées

Les capacités installées à l'interconnexion ont connu une augmentation du même ordre de grandeur que le trafic entrant. Les capacités installées à fin 2020 sont estimées à 66,9 Tbit/s, soit un facteur de 2,4 par rapport au trafic entrant. Ce ratio n'exclut pas l'existence d'épisodes de congestion, qui peuvent survenir entre deux acteurs sur un ou des lien(s) particulier(s) en fonction de leur état à un instant donné.

ÉVOLUTION DES CAPACITÉS DES INTERCONNEXIONS DES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2020



Source : Arcep

2.4 Évolution des modalités d'interconnexion

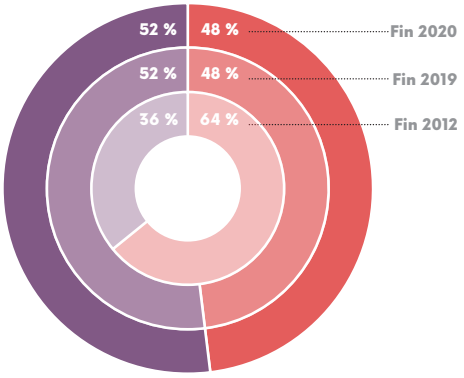
Peering vs Transit

Généralement, la part de *peering* augmente d'une façon régulière. Cette croissance est principalement due à l'augmentation des capacités installées en *peering* privé entre les FAI et les principaux fournisseurs de contenu.

Cependant, entre fin 2019 et fin 2020, une augmentation concomitante du transit et du *peering* (privé comme public) est observée. Les parts respectives de *peering* (52 %) et de transit (48 %) n'ont pas évolué. Cette situation est due essentiellement à la substitution d'une partie du trafic de *peering* avec du trafic provenant des CDN internes.

ÉVOLUTION DES PARTS DE *PEERING* ET DE TRANSIT DES PRINCIPAUX FAI EN FRANCE

(en proportion du trafic entrant)



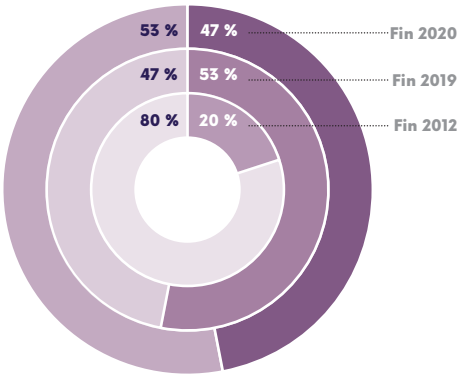
Source : Arcep

Peering gratuit vs *peering* payant

Contrairement à la tendance observée depuis plusieurs années, la part du *peering* payant a diminué pour passer de 53 % à fin 2019 à 47 % à fin 2020. Cette situation s'explique d'une part par l'augmentation du *peering* gratuit (*peering* privé entre acteurs de taille comparable et *peering* public) et d'autre part, par le transfert de trafic du *peering* payant entre FCA et FAI vers des CDN internes.

ÉVOLUTION DES PARTS DE *PEERING* GRATUIT ET PAYANT POUR LES PRINCIPAUX FAI EN FRANCE

(en proportion du trafic entrant)



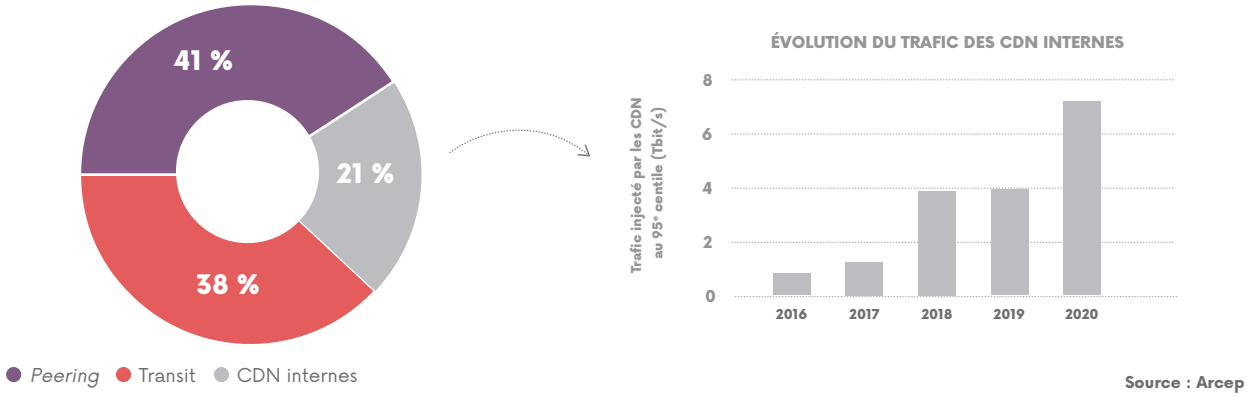
Source : Arcep

2.5 Répartition du trafic par mode d'interconnexion

Entre fin 2019 et fin 2020, le trafic provenant des CDN internes vers les clients des principaux FAI en France a presque doublé (+82 %) pour atteindre environ 7,1 Tbit/s. Le taux de trafic provenant des CDN internes (21 %) a lui aussi augmenté par rapport à l'année dernière (17 %). Cette augmentation pourrait s'expliquer par la modification des usages lors de la crise sanitaire, notamment l'augmentation de la vidéo à la demande qui recourt principalement à des CDN internes dans le réseau des différents opérateurs.

Ce taux varie fortement d'un FAI à l'autre : chez certains opérateurs ce trafic ne constitue même pas 1 % du trafic vers les utilisateurs finaux alors que pour d'autres, il constitue plus de 40 % du trafic entrant injecté dans leurs réseaux. Par ailleurs, le ratio de trafic entrant/sortant varie entre 1/5 et 1/11 en fonction de l'opérateur. Autrement dit, les données disponibles au niveau des CDN internes sont consultées entre 5 et 11 fois en moyenne.

RÉPARTITION ENTRE LES DIFFÉRENTS MODES D'INTERCONNEXION DU TRAFIC VERS LES CLIENTS DES PRINCIPAUX FAI EN FRANCE (FIN 2020)



Source : Arcep

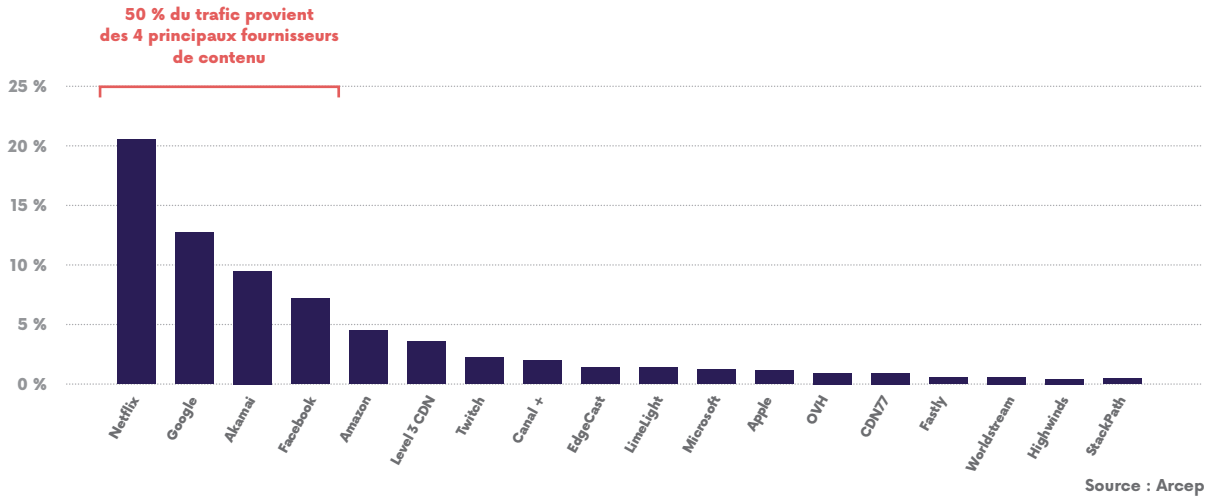
2.6 Décomposition du trafic selon l'origine

50 % du trafic vers les clients des principaux FAI en France provient de quatre fournisseurs : Netflix, Google, Akamai et Facebook. Ceci indique une concentration de plus en plus nette du trafic entre un petit nombre d'acteurs dont la position sur le marché des contenus est renforcée.

Par ailleurs, l'écart se creuse entre le volume de trafic provenant de Netflix et celui des autres fournisseurs de contenu.

La présence de plusieurs CDN dans la décomposition du trafic présentée ci-dessous confirme le rôle important de ces acteurs dans l'acheminement du trafic internet. Par exemple, Disney+ apparaît dans ce classement au travers de ses différents CDN.

DÉCOMPOSITION SELON L'ORIGINE DU TRAFIC VERS LES CLIENTS DES PRINCIPAUX FAI EN FRANCE (FIN 2020)



Source : Arcep

Évolution des tarifs

Les fourchettes de tarifs de transit et de *peering* n'ont pas connu d'évolution depuis l'année dernière. D'après les données recueillies, les prestations de transit se négocient toujours entre moins de 10 centimes d'euro HT et plusieurs euros HT par mois et par Mbit/s. Quant au *peering* payant, il se situe dans une fourchette comprise entre 25 centimes d'euro HT et plusieurs euros HT par mois et par Mbit/s[8].

Dans la majorité des cas, les CDN internes sont gratuits. Néanmoins, il arrive que ceux-ci soient payants dans le cadre plus large de la prestation de *peering* payant que le FCA a contracté par ailleurs avec le FAI.

8. Les fourchettes de tarifs ne reflètent que les tarifs des acteurs ayant répondu au questionnaire payent pour les prestations de transit, *peering* ou CDN internes.

La parole à



RAPHAËL NICOUD

*Président – **Aqua Ray***

AQUA RAY OBTIENT LA CERTIFICATION TIER IV POUR SON *DATACENTER*, RETOUR D'EXPÉRIENCE

Aqua Ray a rénové son centre de données Aurora à Ivry-sur-Seine. Ce projet s'est conclu avec succès en janvier 2021 par l'obtention de la certification Tier IV délivrée par l'*Uptime Institute*. Le *datacenter* Aurora d'Aqua Ray est pour l'instant le seul du Grand Paris à en bénéficier.

TIER IV ? QU'EST-CE QUE CELA SIGNIFIE ?

L'*Uptime Institute* est une entreprise américaine qui a su imposer sa classification « Tier » qui répartit les centres de données selon 4 niveaux de fiabilité sur le marché mondial.

Cette classification se concentre sur 2 points essentiels liés à l'activité des centres de données : l'alimentation électrique et le refroidissement des équipements qui sont censés y être hébergés.

Si votre centre de données est « Tier I » ou « Tier II », c'est que le centre de données doit être mis à l'arrêt en cas de maintenance sur certains équipements.

À partir du niveau « Tier III », vous pouvez intervenir sur n'importe quel maillon de la chaîne pour effectuer une maintenance planifiée sans interrompre la production.

Le niveau « Tier IV » indique que le centre de données est conçu pour faire face à un incident ou une panne sans impact sur la production.

Ainsi, un départ de feu dans une salle UPS, détruisant un onduleur ou un champ de batteries de façon inopinée ne devrait pas avoir d'impact sur la production d'un centre de données Tier IV, alors que cela pourrait être le cas sur un centre de données Tier III qui n'a pas nécessairement été conçu pour cela.

L'ALIMENTATION ÉLECTRIQUE D'UN *DATACENTER* TIER IV

C'est souvent une idée reçue : il n'est pas nécessaire de prévoir une double adduction du site par le réseau public d'acheminement de l'électricité pour faire certifier son centre de données au niveau Tier IV. À vrai dire, aussi paradoxal que cela puisse paraître, il n'est même pas nécessaire de le faire raccorder au réseau tout court.

Par contre, ce à quoi veillera l'*Uptime Institute*, ce sera votre capacité à assurer sur site une production autonome d'électricité à même de couvrir 105 % des besoins en énergie du site dans les pires des scénarios : charge maximale, météo capricieuse et panne d'un des générateurs par exemple.

Aucune technologie n'est imposée, aucune technique particulière n'est requise, tant que votre design permet de répondre aux exigences de la tolérance de panne. Mais l'*Uptime Institute* vérifiera par exemple que chaque câble électrique est correctement dimensionné, et que chaque câble peut être coupé, toujours sans impact sur la production.

Chez Aqua Ray, nous avons opté pour une installation très simple reposant sur des générateurs Diesel en formation 2N : chaque chaîne d'alimentation est indépendante (y compris au niveau des cuves de fuel) et est capable de couvrir seule 105 % des besoins en énergie du site.

LA CLIMATISATION D'UN *DATACENTER* TIER IV

Là encore, aucune technique n'est imposée, pour peu que vous sachiez démontrer que les équipements hébergés dans votre *datacenter* vont toujours être dans un environnement climatique conforme aux préconisations de l'ASHRAE (ambiance entre 18 et 27° C).

Contrairement au niveau Tier III, le niveau Tier IV prévoit tout de même une contrainte supplémentaire : le « *continuous cooling* ». En cas d'incident ou de maintenance, aucune période de flottement n'est tolérée sur le système de climatisation.

Concevoir un réseau d'eau glacée compatible Tier IV redondant y compris au niveau des multiples vannes est complexe et coûteux. Nous avons donc opté chez Aqua Ray pour la détente directe. Nos blocs « clim » en formation 2N sont par ailleurs raccordés électriquement au réseau « haute qualité », c'est-à-dire derrière les onduleurs, ce qui n'est pas classique. Cela nous a permis de répondre à l'exigence du « *continuous cooling* ».

LES AUTRES POINTS DE VIGILANCE

La double adduction réseau, le cloisonnement coupe-feu et la stratégie de surveillance/monitoring automatisé du site font par exemple également partie des contraintes. Par contre il s'agit bien d'une classification axée sur la fiabilité du service et non par exemple sur sa sécurisation. Les techniques de contrôle d'accès et de détection d'intrusion par exemple n'y sont pas abordées. C'est pourquoi lorsqu'on choisit un centre de données, il convient de prêter attention à ces questions en complément des critères Tier III ou Tier IV, par exemple en vérifiant la conformité ISO 27000 des installations.

La parole à



FRANCK SIMON

*Président - **Société France-IX Services***

FRANCE-IX, PLATEFORME MULTISERVICES DE RÉFÉRENCE LEADER DE L'INTERCONNEXION EN FRANCE

RÔLE DE FRANCE-IX DANS L'INTERCONNEXION EN FRANCE & FUSION ENTRE FRANCE-IX ET REZOPOLE

Lors de sa création en 2010, France-IX s'est concentrée sur l'établissement d'une structure neutre et indépendante, fournissant un service de qualité pour un prix juste, en adéquation avec le marché, afin d'y attirer les réseaux internationaux et d'en faire l'une des plateformes européennes majeures d'interconnexion.

En 2020, France-IX a atteint un niveau de maturité avec plus de 450 réseaux connectés (*via* ses points de présence de Paris et Marseille) et un niveau de trafic dépassant le Terabit par seconde. Dans le même temps, la compétition entre les principaux points d'échange internet internationaux s'est renforcée : dans ce contexte, le moment était venu de faire évoluer la stratégie de France-IX et de consolider ce qui en fait sa spécificité, à savoir être la plateforme de référence pour l'accès aux contenus ainsi qu'aux acteurs français et francophones.

Même si France-IX peut s'appuyer sur un réseau d'opérateurs revendeurs pour couvrir les sites sur lesquels nous ne sommes pas physiquement présents, il était important de développer notre capillarité nationale.

Afin de renforcer sa position de plateforme multiservices leader en France, la fusion avec Rezopole s'est imposée assez naturellement dans la mesure où les deux structures disposaient d'un ADN associatif commun, et que Rezopole a su constituer le plus gros ensemble de points d'échanges internet régionaux en France, et a démontré une expertise réelle dans la fourniture de services à valeur ajoutée pour ses membres. L'offre de services France-IX va ainsi être élargie, à destination notamment des entreprises, tout en couvrant un périmètre géographique étendu, notre objectif étant de couvrir 2 villes par an durant les 3 prochaines années.

IMPACT DU 1ER CONFINEMENT SUR LES INFRASTRUCTURES

Le 1er confinement a été une période complexe à gérer, autant pour la continuité des opérations, que le développement commercial. Dès les premières annonces, allant dans le sens d'un confinement, nous avons anticipé en préinstallant de nombreux ports 10 Gbit/s et 100 Gbit/s sur l'ensemble de nos sites, et c'est cela qui nous a permis de traiter les demandes durant le confinement malgré les restrictions d'accès que nous avions dans beaucoup de *datacenters*. Ceci dit, la hausse du trafic des uns a été compensée par la baisse du trafic des autres durant cette période, et le trafic qui a stagné sur la période de janvier à juin 2020 n'a réellement redécollé qu'à la fin de l'été et a ensuite connu une croissance régulière jusqu'à décembre 2020.

FUTURS ENJEUX POUR FRANCE-IX

Outre le développement de son périmètre géographique, et le fait de permettre à ses membres de bénéficier d'une plateforme fortement interconnectée (*via* des passerelles entre les villes), France-IX va développer son offre de services : le *peering* public sera complété par des solutions de *peering* privé d'autant qu'une grande partie des échanges se fait justement par ce type de solutions.

Il est également important de continuer à sensibiliser les entreprises à l'importance de se connecter à des plateformes comme la nôtre pour les soutenir dans leur transformation numérique, *via* des formations adaptées.

Ponctuellement, des solutions d'hébergement, en partenariat avec les *datacenters*, pour répondre à des demandes d'acteurs internationaux qui réclament un guichet unique, seront possibles.

Nous travaillons à la révision de notre place de marché, dans la mesure où nous avons une marge de progression assez forte. Notre programme de revendeurs va aussi être reconsidéré avec un accompagnement de ces derniers pour mieux les former à nos produits et services, d'autant qu'ils nous réclament une automatisation des processus de commande et de livraison des ressources (configuration automatique des circuits) en intégrant des API.

Les challenges pour France-IX sont multiples et sont révélateurs de la transformation indispensable des plateformes d'interconnexion : il est probable que celles qui n'envisagent pas de diversifier leur offre de services ni d'établir des partenariats avec d'autres structures pour consolider leur position seront amenées à décliner. Le marché évolue et les points d'échange ne sont plus des structures exclusivement dédiées aux opérateurs et fournisseurs de contenu même s'ils en demeurent des acteurs-clés.

CHAPITRE 3

ACCÉLÉRER LA TRANSITION VERS IPv6

À retenir

105 participants à la task-force IPv6 co-pilotée par l'Arcep et Internet Society France : rejoignez la task-force !

Les opérateurs qui se sont vu attribuer des fréquences 5G sont tenus de rendre leur réseau mobile compatible à compter du **31 décembre 2020.**

Le taux d'utilisation d'IPv6 progresse en France pour atteindre **plus de 42 %** en décembre 2020.

L'IPv4 et l'IPv6, pour *Internet Protocol* version 4 ou version 6, sont des protocoles utilisés sur internet pour permettre d'identifier chaque terminal sur le réseau (ordinateur, téléphone, serveur, etc.). Les adresses IP publiques sont enregistrées et routables sur internet, elles sont donc uniques mondialement. IPv4 et IPv6 ne sont pas compatibles : un équipement ne disposant que d'adresses IPv4 ne peut pas dialoguer avec un équipement ne disposant que d'adresses IPv6. La transition ne se fait pas en remplaçant le protocole IPv4 par IPv6, mais en rajoutant IPv6 en plus d'IPv4[1].

1 La fin d'IPv4, la transition indispensable vers IPv6

Le protocole IPv4, utilisé sur internet depuis 1983, offre un espace d'adressage de près de 4,3 milliards d'adresses IPv4[2]. Or le succès d'internet, la diversité des usages et la multiplication des objets connectés ont eu comme conséquence directe l'épuisement progressif des adresses IPv4, certaines régions du monde étant touchées plus que d'autres. Les principaux opérateurs français (Bouygues Telecom, Orange, SFR)[3] ont déjà affecté entre environ 92 % et 95 % des adresses IPv4 qu'ils possèdent, à fin juin 2020[4].

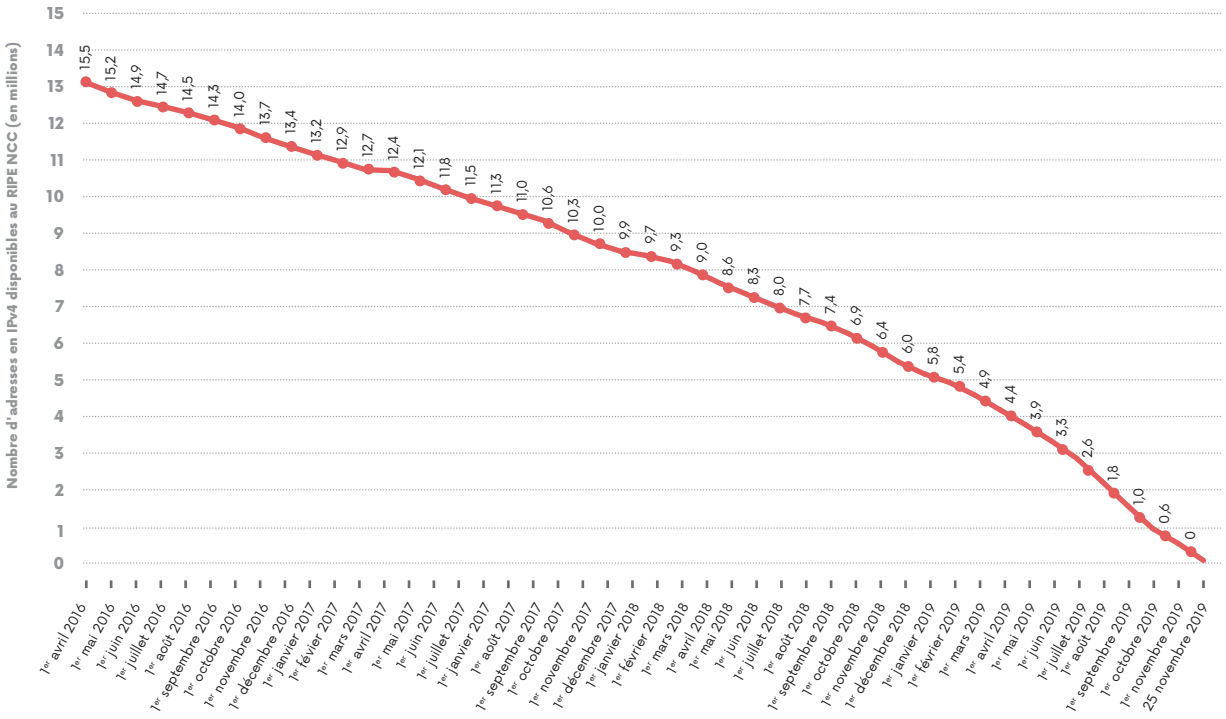
Les spécifications d'IPv6 ont été finalisées en 1998. Elles intègrent des fonctionnalités pouvant renforcer la sécurité par défaut et optimiser le routage. Surtout, IPv6 offre une quasi-infinité d'adresses : 667 millions d'IPv6 pour chaque millimètre carré de surface terrestre[5].

Du fait de la complexité actuelle d'internet, la migration d'IPv4 vers IPv6 ne peut se réaliser que progressivement, d'abord en parallèle d'IPv4 (phase de cohabitation), puis, quand tous les acteurs auront migré, en remplacement total d'IPv4 (phase d'extinction). La transition vers le protocole IPv6 a démarré en 2003. Cependant, en 2020, internet n'en est encore qu'au début de la phase de cohabitation[6].

Dans l'édition 2019 de son rapport sur l'état d'internet en France, l'Arcep a estimé que l'épuisement du stock d'adresses IPv4 serait effectif vers la fin du second trimestre de 2020, mais le rythme des acquisitions des derniers blocs d'IPv4 s'est accéléré et l'épuisement des adresses IPv4 s'est produit fin 2019. Au 25 novembre 2019, le RIPE NCC (le registre régional qui alloue les adresses IP pour l'Europe et le Moyen-Orient) a en effet annoncé la pénurie d'IPv4, après avoir effectué l'attribution du dernier /22 IPv4 à partir des dernières adresses restantes.

1. Dans certains cas, notamment sur les réseaux mobiles, IPv6 est déployé à la place d'IPv4. Dans ce cas-là, des mécanismes de traduction de protocoles sont mis en place sur le réseau (NAT64 et DNS64) et sur le terminal (464XLAT).
2. Les adresses IPv4 sont codées sur 32 bits. Au maximum 2^{32}, soit 4 294 967 296 adresses peuvent donc être attribuées simultanément en théorie.
3. Free n'a pas communiqué le nombre d'adresses IPv4 déjà affectées.
4. Données recueillies par l'Arcep auprès de FAI conformément à la décision n° 2020-0305.
5. Les adresses IPv6 sont codées sur 128 bits. Au maximum 2^{128} (soit environ $3{,}4 \times 1^{038}$) adresses peuvent donc être attribuées simultanément en théorie.
6. L'Arcep précise que les constats et travaux évoqués concernent uniquement le réseau internet et ne s'appliquent pas à l'interconnexion privée entre deux acteurs, notamment l'interconnexion des réseaux de deux opérateurs pour la terminaison d'appel vocal en mode IP.

HISTORIQUE D'ÉPUISEMENT DES ADRESSES IPv4



Source : données RIPE NCC

Une liste d'attente existe, permettant de récupérer des adresses IPv4 rendues au RIPE NCC, même si peu d'adresses le sont en pratique. Le RIPE NCC explique que ces attributions, nécessairement limitées, ne pourront pas répondre aux besoins d'adresses IPv4 pour les réseaux aujourd'hui. Faire perdurer internet en IPv4 ne l'empêchera pas de fonctionner, mais l'empêchera de grandir, en raison des risques que présentent les solutions permettant de continuer le fonctionnement d'internet sur IPv4 malgré le manque d'adresses :

- Le partage d'adresses IPv4 entre plusieurs clients peut provoquer le dysfonctionnement de certaines catégories de services sur internet (systèmes de contrôle de maison connectée, jeux en réseau, etc.). En plus, ce partage augmente le risque de se voir refuser l'accès à un service, par exemple quand l'IP est mise sur liste noire à cause du comportement frauduleux d'un autre colocataire de la même adresse IPv4. Un autre effet collatéral du partage d'IPv4 est de rendre difficile l'identification d'un suspect sur la base de son adresse IP pour les enquêtes judiciaires, obligeant parfois les enquêteurs à ouvrir des enquêtes sur des personnes qui n'ont pour seul tort que de partager la même adresse IPv4 avec un suspect.
- L'achat d'adresses IPv4 est possible sur un marché secondaire, mais le prix des adresses est susceptible d'ériger une barrière à l'entrée significative à l'encontre des nouveaux acteurs. Par ailleurs, les adresses IPv4 achetées sur le marché secondaire peuvent bloquer certains services bancaires ou de vidéo à la demande tant que la mise à jour de la géolocalisation des adresses n'est pas effective.

Ces pratiques augmentent le risque de voir se développer un internet scindé en deux, IPv4 d'un côté et IPv6 de l'autre. Par exemple, certains hébergeurs proposent désormais des offres IPv6-*only* et les sites hébergés sur ces serveurs ne sont alors pas accessibles aux clients d'opérateurs IPv4-*only*.

Face à cette pénurie annoncée et aux risques encourus, la transition vers un nouveau protocole de communication sur internet apparaît comme un enjeu majeur de compétitivité et d'innovation. Dans le rapport élaboré avec le concours de l'Afnic décrivant l'état d'IPv6 en France remis au Gouvernement en juin 2016, l'Arcep proposait plusieurs leviers d'action dans l'objectif d'accompagner et d'accélérer la transition. Depuis, elle publie chaque année son baromètre de la transition vers IPv6, dans une optique de régulation par la donnée. Elle a également amorcé une démarche de co-construction avec l'écosystème internet en France afin de fédérer la communauté et de permettre d'accélérer cette transition.

Quels sont les « scénarios de sortie » d'IPv4 plausibles ?

Le scénario de sortie d'IPv4 n'est pas connu et est très difficile à prévoir à ce jour. Si l'on essaie malgré tout d'imaginer les différentes étapes d'un tel scénario, on arrive par exemple à une séquence telle que celle-ci :

1. La quasi-totalité des offres d'accès internet grand public commercialisées proposent de l'IPv6 activé par défaut en plus de l'IPv4.
2. La quasi-totalité des offres d'accès internet grand public, pro et entreprise proposent de l'IPv6 activé par défaut. Une connectivité IPv4 est toujours proposée.
3. Une part non négligeable des sites web sont hébergés en IPv6 uniquement, malgré des poches de résistance à l'IPv6 pour l'accès proposé par quelques entreprises à leurs salariés. Ces sites ne sont plus accessibles depuis une entreprise qui bloque l'IPv6.
4. Une part non négligeable des offres des fournisseurs d'accès à internet ne proposent plus de connectivité IPv4. Il n'est plus possible de consulter des sites web hébergés en IPv4 uniquement.
5. La majorité des sites web abandonnent IPv4, devenu inutile. IPv4 n'est plus utilisé sur internet, mais peut continuer à être utilisé pour des réseaux privés.

Workshop IPv6 du BEREC

Face à la pénurie d'adresses IPv4 que connaît l'Europe depuis plus d'un an, la transition vers IPv6 s'est imposée comme un enjeu majeur d'innovation et de compétitivité. Dans ce contexte, le BEREC a organisé le 7 octobre dernier un *workshop* interne afin de faire un état des lieux du déploiement d'IPv6 en Europe. Les principaux objectifs de ce *workshop* étaient de donner un aperçu de l'état d'IPv6 en Europe, mettre en évidence les problèmes liés au retard du déploiement d'IPv6, recueillir des informations sur les actions des États membres / ARN pour favoriser la transition vers IPv6, partager les bonnes pratiques et échanger sur les actions qui pourraient être menées au niveau du BEREC pour favoriser le déploiement d'IPv6 en Europe.

En plus des témoignages des régulateurs belge (BIPT), finnois (Traficom) et français (Arcep) sur leurs actions pour favoriser le déploiement, le RIPE NCC, *Internet Society* et Europol ont apporté leur expertise sur le sujet tout en soulignant l'objectif commun qui est de généraliser le déploiement d'IPv6 pour garantir les évolutions futures d'internet. Le *workshop* était l'occasion de présenter les résultats du questionnaire interne auquel les différents membres du BEREC ont répondu en amont du *workshop*. Ce questionnaire concernait l'impact de la pénurie d'IPv4 au niveau national, les actions nationales mises en place, les différents cadres juridiques pour encadrer le déploiement d'IPv6, ainsi que des propositions d'action à mener au sein du BEREC pour accélérer la transition vers IPv6.

Lors du *workshop*, le BEREC a rappelé l'importance de l'IPv6 pour internet et son rôle en tant que condition préalable essentielle à une Europe numérique. Cependant, actuellement, les trois quarts de la population de l'Espace économique européen (EEE) n'ont pas accès à IPv6 et il existe de grandes différences entre les pays dans le déploiement de ce protocole. En effet, certains pays ont environ la moitié de leurs utilisateurs en IPv6 (Belgique, Allemagne, Grèce, Suisse, France), tandis que d'autres n'ont pas commencé le déploiement de ce protocole (Malte, Monténégro, Serbie, etc.). Par ailleurs, des disparités importantes entre les pays sont observées en ce qui concerne la collecte de données, les effets de la pénurie d'IPv4, les compétences des autorités dans la transition vers l'IPv6 ou encore les mesures prises au niveau national pour favoriser cette transition.

Plusieurs propositions d'actions à mener au sein du BEREC ont émergé suite au *workshop*, notamment sensibiliser davantage les États membres / ARN sur les avantages de la transition vers l'IPv6 ou mettre en place une plateforme de partage d'expériences et de bonnes pratiques.

À la suite de ce *workshop*, deux autres *workshops* ont été planifiés pour alimenter le plan de travail du BEREC de 2022 : un *workshop* externe rassemblant les acteurs IPv6 au niveau européen en mai 2021 et un *workshop* interne en juin 2021.

Les différentes actions entreprises par le BEREC sur IPv6 visent à partager les bonnes pratiques et à encourager les acteurs à accélérer la transition, afin qu'internet continue de fonctionner comme un moteur d'innovation et de croissance.

La parole à



ALEXANDRE PETRESCU

*Ingénieur chercheur – **Commissariat à l'énergie atomique et aux énergies alternatives (CEA)***

PROBLÈME DE L'ADRESSAGE IPv6 POUR AUTOMOBILES CONNECTÉES AUX RÉSEAUX MOBILES

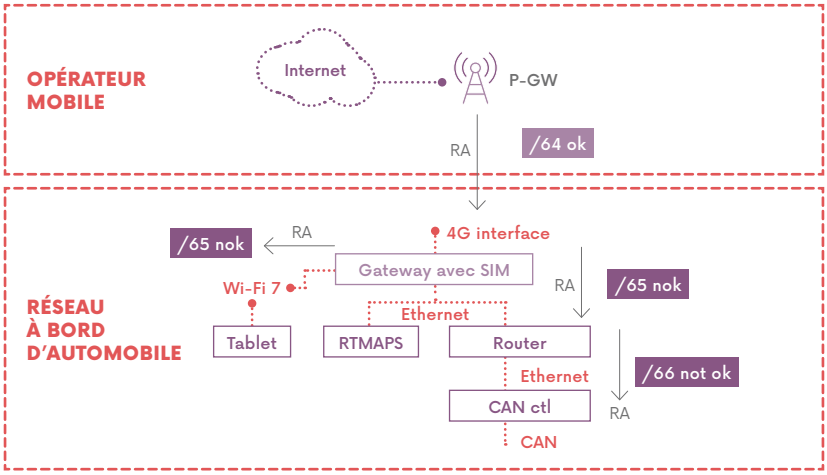
« IPv6 » est un acronyme donné couramment au protocole de communication de la couche « réseau » sur internet, ou alors *Internet Protocol version* 6 en anglais. Ce protocole est conçu fondamentalement de la même manière que la version précédente. Une différence très importante se situe dans la longueur d'adresses (128 bits pour IPv6). Ce protocole a été développé avec une exigence très importante : pouvoir accueillir un très grand nombre d'ordinateurs, beaucoup plus que ce qui était disponible il y a 40 ans. En même temps, il a fallu assurer une joignabilité complète entre n'importe lequel de deux ordinateurs connectés. C'était un vrai défi qui a été surpassé. Il reste toutefois d'autres défis de l'IP pour la mobilité.

Aujourd'hui, les automobiles sont connectées à l'internet en IPv4 et en NAT. Leur caractéristique fondamentale est d'être mobiles dans des grandes régions. Mais le système d'adressage et routage de l'internet est fait pour des entités fixes, même s'il est déployé à très grande échelle géographique. Certains des ingrédients fondamentaux de l'IP, comme l'utilisation de table de routage finies, et d'algorithmes de routage dans des graphes fixes, rendent très difficiles les connexions stables pour automobiles. En revanche, les réseaux cellulaires d'opérateurs de téléphonie mobile constituent des très bons candidats pour connecter ces automobiles de par leur large couverture sans fil. De plus, le support local de mobilité offert par des protocoles utilisés dans les réseaux cellulaires peut résoudre certains problèmes de manque de support de mobilité dans l'internet à l'échelle globale.

Pourtant, dans les spécifications et déploiement de l'IP d'aujourd'hui il reste des problèmes d'adressage qui rendent impossible l'utilisation de l'IP dans les automobiles connectées aux réseaux mobiles. Un des problèmes d'adressage est celui de la limite du préfixe de 64 bits. Les causes de ce problème sont les suivantes :

- L'architecture d'adressage IP de l'internet (RFC4291) tout comme l'Interface ID sur Ethernet (RFC2464) pour le protocole d'auto-configuration d'adresse le plus largement utilisé (*SLAAC – Stateless Address Autoconfiguation*) observent tous deux une limite rigide à l'intérieur de l'adresse, à la frontière du 64e bit. On ne peut utiliser SLAAC ni avec un préfixe /63 et ni /65. Le protocole DHCPv6-PD (délégation de préfixe) est bloqué par des constructeurs de modems mobiles populaires.
- Les opérateurs de téléphonie mobile cellulaire en France et partout dans le monde offrent un préfixe de longueur de précisément 64 bits[1] pour chacun des utilisateurs. Ceci est particulier aux opérateurs mobiles ; les opérateurs fixes ont déjà offert des préfixes de longueurs plus courtes que /64 ; par exemple /56 aux box à la maison.
- Une automobile connectée contient des nombreux ordinateurs à son bord groupés dans de nombreux sous-réseaux. Pour des raisons de coûts, un seul de ces ordinateurs – la *gateway* – est connecté directement au réseau cellulaire, et est le seul à disposer de *credentials* d'autentifications comme une carte SIM.

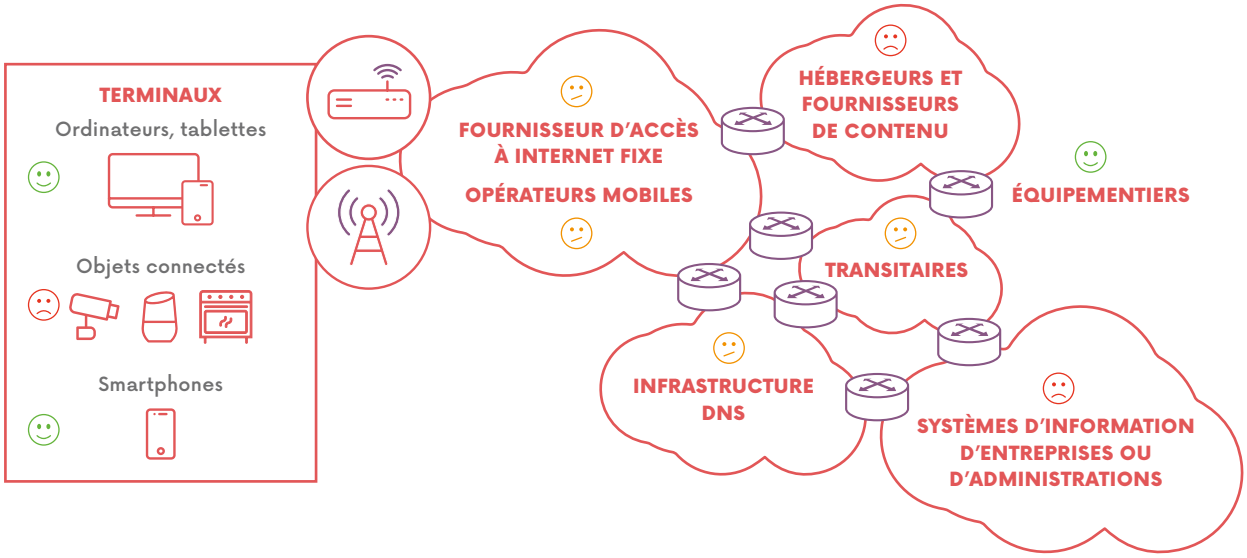
La combinaison de toutes ces causes mène à **l'impossibilité d'utiliser IPv6 dans des automobiles connectées à l'internet.** Ceci est illustré dans la figure suivante, par les rectangles indiquant « /65 nok » :



1. Idéalement, un opérateur offrirait un préfixe de longueur plus courte que /64 à la *gateway* d'une automobile, par exemple un /56. De cette manière la *gateway* pourrait former des sous-préfixes de longueur /64 à utiliser dans les sous-réseaux à bord de véhicule avec le protocole d'autoconfiguration SLAAC.

2 Baromètre de la transition vers IPv6 en France

ÉTAT D'AVANCEMENT DE LA TRANSITION VERS IPv6 AU NIVEAU DES DIFFÉRENTS MAILLONS DE LA CHAÎNE TECHNIQUE



Migration vers IPv6 totale ou élevée · Migration vers IPv6 partielle · Migration vers IPv6 faible ou nulle

Source : Arcep

Le baromètre annuel de la transition vers IPv6 a pour objectif de mieux informer les utilisateurs sur ce sujet. Ce baromètre, qui compile à la fois des données produites et mises à disposition par des tiers (Cisco, Google et Afnic) et des données recueillies par l'Arcep directement auprès des principaux opérateurs français[7], donne un aperçu de l'état du déploiement d'IPv6 en France pour les différentes parties prenantes impliquées dans la transition. L'Arcep a publié l'édition 2020 de ce baromètre le 4 décembre 2020.

L'édition 2020 du baromètre a été enrichie par rapport aux éditions précédentes grâce, d'une part, à l'élargissement de la collecte d'informations 2020 aux principaux opérateurs sur le marché « entreprises », et d'autre part, à l'ajout d'indicateurs sur l'avancement de la transition vers IPv6 pour les différents sites web et services en ligne de l'État. Comme exposé ci-après, les parties prenantes se trouvent à différentes étapes de la transition.

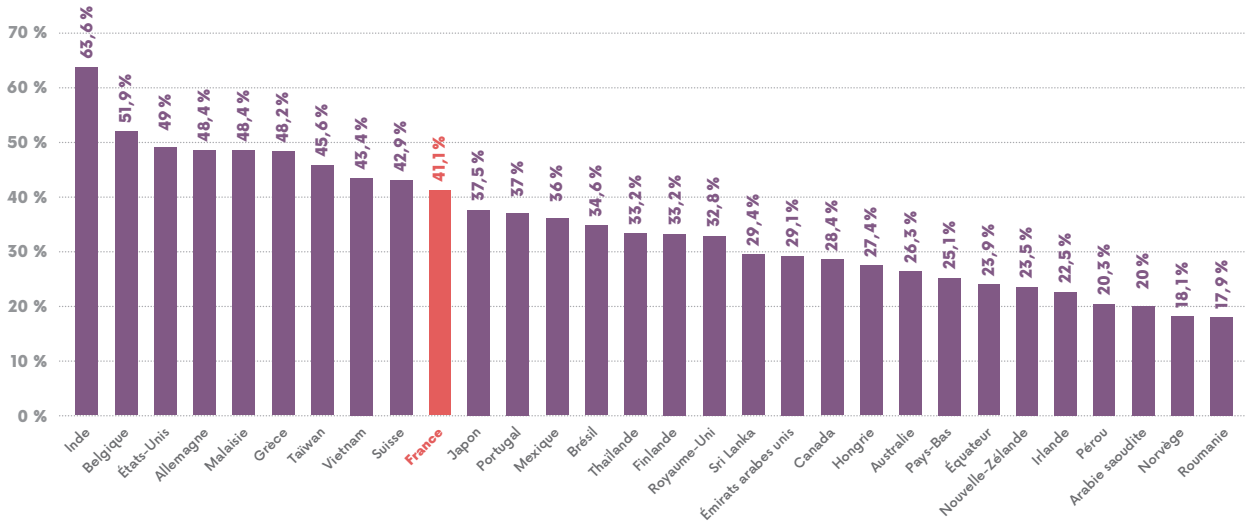
Les résultats confirment la progression du taux d'utilisation d'IPv6 en France qui était de plus de 45 % en mars 2021, tel qu'observé par Google. Il est à noter que, lors du premier confinement qu'a connu la France à la suite de la pandémie de Covid-19, le taux d'IPv6 est passé d'environ 37 % à 43 % entre mi-mars et fin avril 2020. Ce taux a légèrement baissé après le confinement. Cela pourrait notamment s'expliquer par l'augmentation du trafic issu des accès grand public, plus fréquemment activés en IPv6 que les accès entreprise. Ce taux a de nouveau augmenté suite aux migrations de certains opérateurs mobile fin 2020.

Au niveau mondial, la France se situe aujourd'hui dans le top 10 en termes de taux d'utilisation d'IPv6 d'après les quatre principales sources de données publiquement disponibles pour évaluer l'utilisation d'IPv6 (Google, Akamai, Facebook et Apnic)[8]. La France se classe en cinquième position au niveau européen, derrière la Belgique, l'Allemagne, la Grèce et la Suisse.

L'Arcep propose sur son site des statistiques IPv6, sur le top 100 des pays avec le plus d'internautes, mis à jour tous les deux mois.

7. Décision n° 2020-0305 de l'Arcep relative à la mise en place d'enquêtes dans le secteur des communications électroniques.
8. D'après la médiane des données « Google IPv6 adoption », « Akamai IPv6 adoption », « Facebook IPv6 adoption », « Apnic IPv6 preferred » d'octobre 2020. L'agrégation des données entres les pays est réalisée au prorata du nombre d'utilisateurs d'internet (source Wikipédia, données en date du 20/10/2020). La médiane entre les 4 sources est calculée pays par pays, avant d'être agrégée au prorata du nombre d'utilisateurs d'internet dans chaque région.

TOP 30 DES PAYS EN TERMES D'UTILISATION D'IPv6



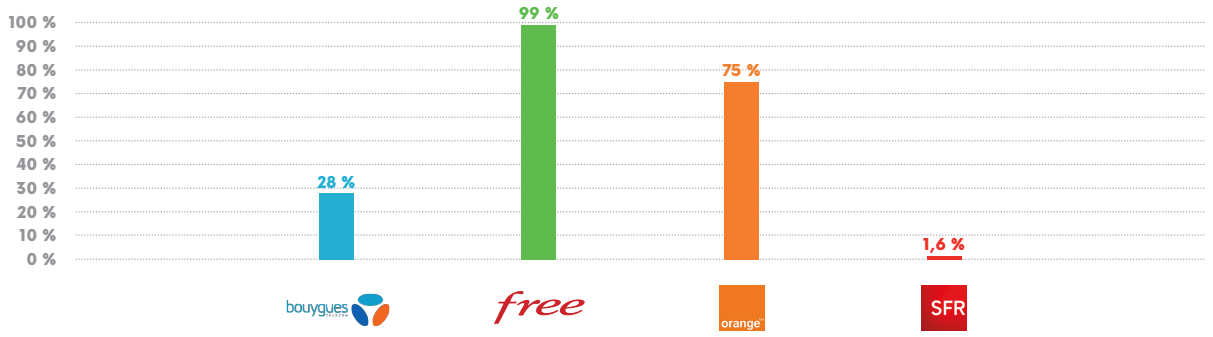
Source : Médiane des données « Google IPv6 adoption », « Akamai IPv6 adoption », « Facebook IPv6 adoption », « Apnic IPv6 preferred » d'octobre 2020. Seuls sont considérés les pays du Top 100 avec le plus d'internautes.

Le baromètre montre en détail l'état de la transition au niveau de chaque acteur de l'écosystème.

2.1 Fournisseurs d'accès à internet fixe

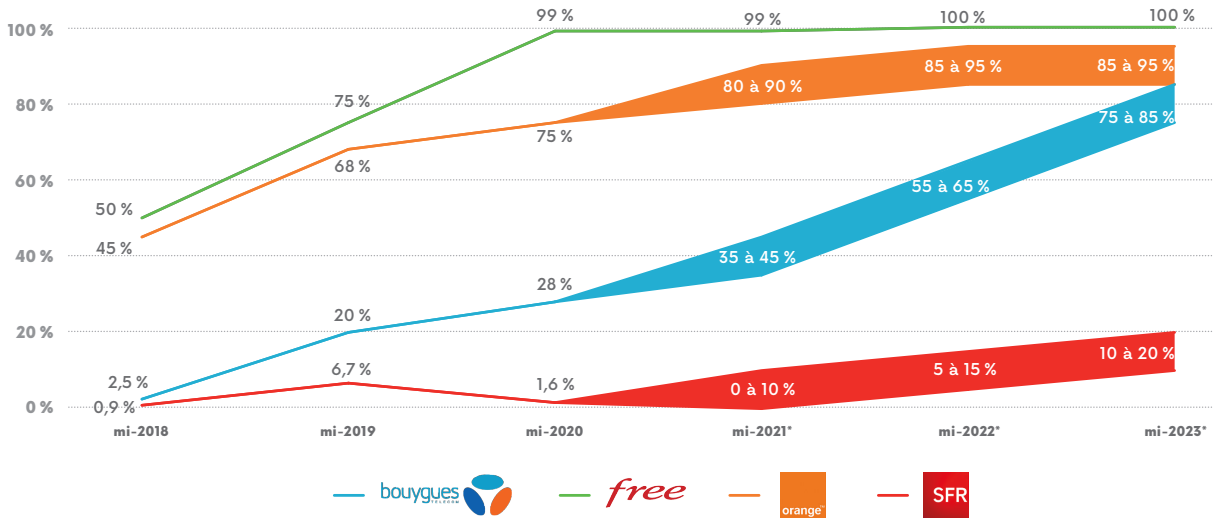
Les schémas suivants exposent la situation actuelle du déploiement d'IPv6 ainsi que les prévisions au niveau du réseau fixe des principaux opérateurs en France.

RÉSEAU FIXE : TAUX DE CLIENTS ACTIVÉS EN IPv6



Source : données à fin juin 2020, recueillies par l'Arcep auprès des opérateurs.

RÉSEAU FIXE : ÉVOLUTION DU TAUX DE CLIENTS ACTIVÉS EN IPv6



* Chiffres susceptibles d'évoluer

Source : données à fin juin 2020, recueillies par l'Arcep auprès des opérateurs.

Sur le réseau fixe, en ce qui concerne les principaux opérateurs télécoms en France, l'Arcep constate des progrès mais appelle les opérateurs à poursuivre et renforcer encore plus leurs efforts :

- Le taux de clients activés en IPv6 sur le réseau de SFR toutes technologies confondues a diminué en passant de 6,7 % à mi-2019 à 1,6 % à mi-2020. Cette régression, principalement liée à la diminution des clients activés en FttH, est préoccupante en raison de la pénurie d'IPv4. Les activations à venir demeurant également insuffisantes (entre 5 % et 15 % à mi-2022 et entre 10 % et 20 % à mi-2023), SFR est invité à accélérer fortement sa transition vers IPv6 sur son réseau fixe, en particulier sur le FttH, et à entamer cette transition sur le câble. Une grande majorité des clients n'activant pas IPv6 manuellement, SFR est encouragé à réaliser cette activation par défaut de façon systématique.
- Malgré une progression du nombre de clients activés en IPv6 et des prévisions encourageantes (entre 75 % et 85 % à mi-2023), le rythme de déploiement d'IPv6 par Bouygues Telecom reste insuffisant pour faire face à la pénurie. Bouygues Telecom est à nouveau encouragé à poursuivre et accélérer les efforts de déploiement d'IPv6 sur son réseau fixe.
- Sur les réseaux fixes, les taux actuels de clients activés de Free et d'Orange sont relativement élevés (respectivement 99 % et 75 % environ) et ont progressé. Les projections à mi-2023 sont encourageantes (100 % pour Free et entre 85 % et 95 % pour Orange).
- Bouygues Telecom, Free et SFR sont invités à entamer au plus vite la transition sur la 4G fixe. Orange, ayant l'intégralité de ses clients 4G fixe IPv6-ready, est en particulier invité à réaliser l'activation d'IPv6 par défaut sur cette technologie.

En général, IPv6 est activé par défaut pour ces quatre opérateurs et ne nécessite donc pas d'action de l'utilisateur. Concernant les opérateurs qui ont entre 5 000 et 3 millions de clients grand public sur le marché fixe, les opérateurs qui avaient entamé leur transition continuent le déploiement, avec en particulier les initiatives de Coriolis, K-Net et OVH Télécom qui poursuivent leur transition vers IPv6 engagée depuis plusieurs années, Orne THD qui a déjà migré l'intégralité de ses clients depuis 2019 et Vialis qui a débuté sa transition cette année. Même si plusieurs opérateurs prévoient d'accélérer leur transition en 2021 (Coriolis Telecom, Vialis, Zeop) et qu'un opérateur supplémentaire (Ozone) envisage d'entamer sa transition l'année prochaine, le déploiement semble encore insuffisant pour répondre à la pénurie d'IPv4. Plus d'informations sont disponibles dans le baromètre IPv6[9].

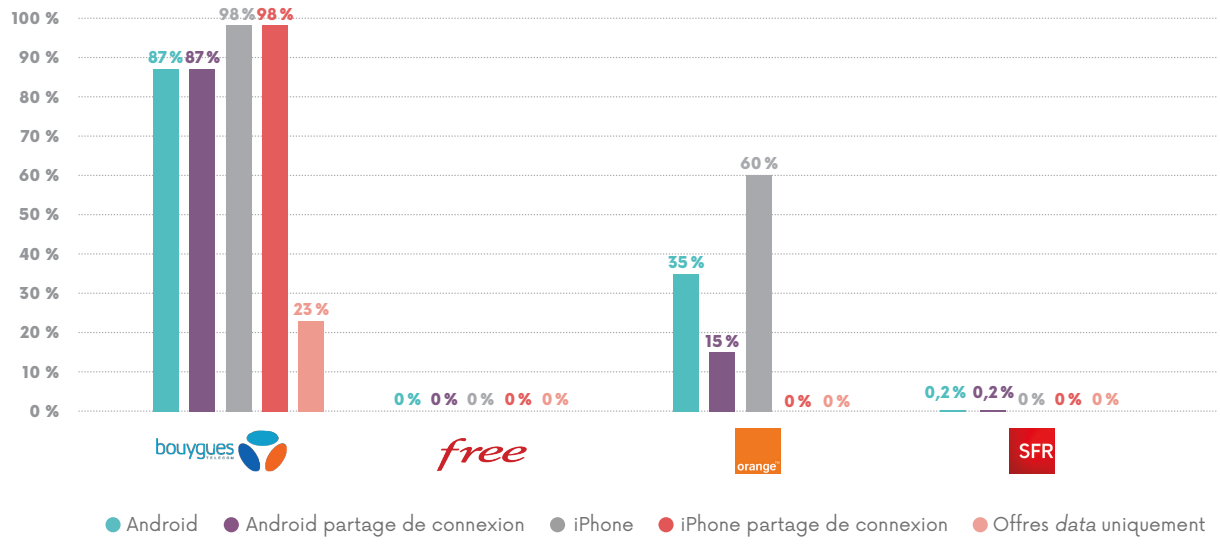
Comme indiqué précédemment, afin d'améliorer le suivi de la transition vers IPv6, l'Arcep a élargi la collecte d'informations aux opérateurs aux principaux opérateurs sur le marché « entreprises » qui proposent des offres « Pro » sur le réseau fixe. L'Arcep constate que le déploiement est insuffisant et appelle les opérateurs à proposer IPv6 dans leurs offres à destination des entreprises. Plus d'informations sont disponibles dans le baromètre IPv6[10].

9. Baromètre Arcep IPv6 2020, « Les opérateurs ayant entre 5 000 et 3 millions de clients sur le réseau fixe » : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2020_de_la_transition_vers_IPv6.pdf#page=9
10. Baromètre Arcep IPv6 2020, « Les opérateurs proposant des offres "Pro" sur le réseau fixe » : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2020_de_la_transition_vers_IPv6.pdf#page=10

2.2 Opérateurs mobiles

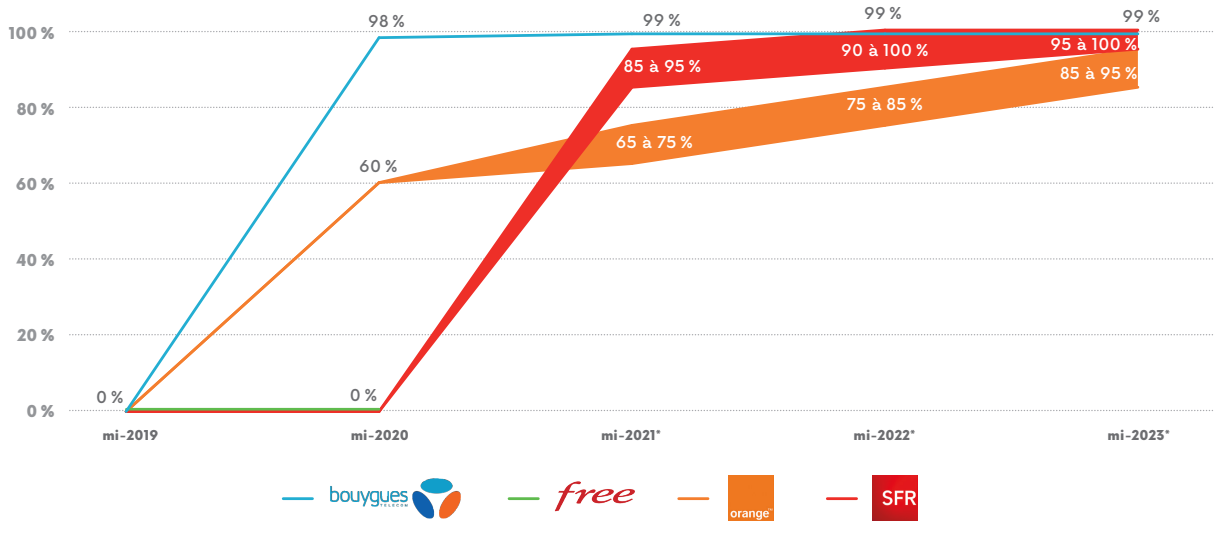
Les schémas suivants exposent la situation actuelle du déploiement d'IPv6 ainsi que les prévisions au niveau du réseau mobile des principaux opérateurs en France.

RÉSEAU MOBILE : TAUX DE CLIENTS ACTIVÉS EN IPv6



Source : données à fin juin 2020, recueillies par l'Arcep auprès des opérateurs.

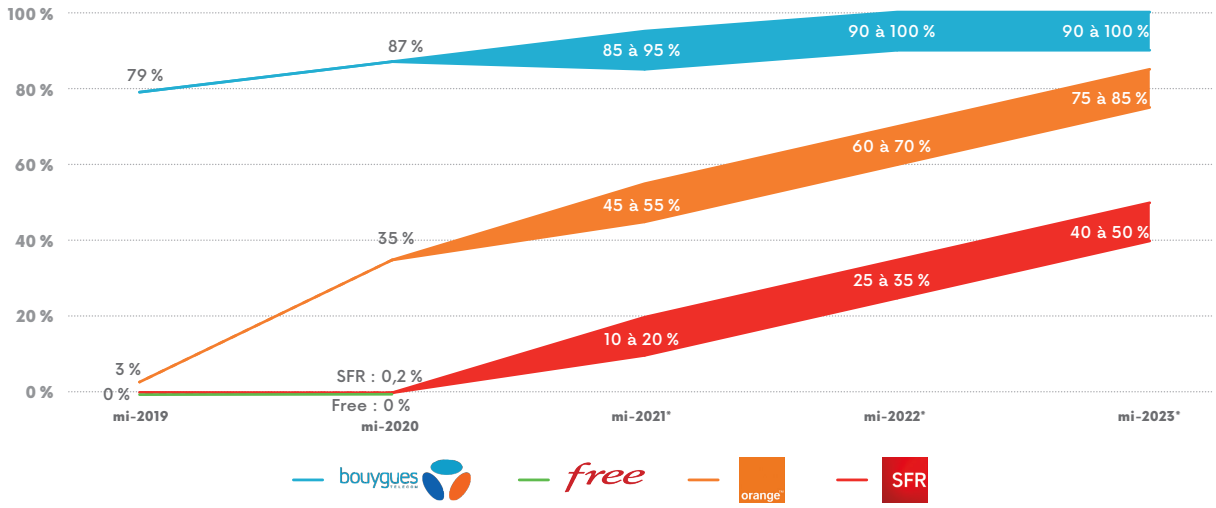
iPHONE : ÉVOLUTION DU TAUX DE CLIENTS ACTIVÉS EN IPv6



* Chiffres susceptibles d'évoluer

Source : données à fin juin 2020, recueillies par l'Arcep auprès des opérateurs.

ANDROID : ÉVOLUTION DU TAUX DE CLIENTS ACTIVÉS EN IPv6



* Chiffres susceptibles d'évoluer

Source : données à fin juin 2020, recueillies par l'Arcep auprès des opérateurs.

Malgré le retard dans le déploiement d'IPv6 sur le réseau mobile, l'Arcep constate que les prévisions sont encourageantes et invite les opérateurs à poursuivre leurs efforts pour accélérer la transition :

- Bouygues Telecom a mené un déploiement notable sur les réseaux mobiles, avec 87 % de clients Android et 98 % de clients iPhone activés en IPv6 à mi-2020.
- Le déploiement d'IPv6 sur le réseau mobile d'Orange est aussi à noter (35 % de clients Android et 60 % de clients iPhone activés en IPv6). Orange est invité à poursuivre les activations en IPv6 des terminaux mobiles.
- SFR a activé 100 % de clients IPv6-*ready* en novembre 2020. Tous les clients SFR titulaires d'un iPhone sont passés en IPv6 activé avec la mise à jour iOS 14.3, diffusée en décembre 2020. Au premier semestre 2021, SFR a commencé à activer IPv6 avec les mises à jour de certains terminaux Android récents. SFR est encouragé à accélérer les activations des terminaux Android en IPv6.
- Il est particulièrement regrettable que Free Mobile n'en soit qu'au début de la transition de son réseau mobile à ce jour et n'ait pas été en mesure de transmettre des prévisions.
- Les opérateurs sont invités à accélérer le déploiement d'IPv6 sur l'intégralité de leurs offres, notamment « *data* uniquement ».

Parmi les opérateurs ayant entre 5 000 et 3 millions de clients, Zeop est l'unique opérateur mobile ayant entre 5 000 et 3 millions de clients qui a commencé à activer IPv6 sur son réseau (23 % à mi-2020) et prévoit 40 % de clients activés en IPv6 d'ici mi-2021. Le retard étant encore plus marqué que sur le fixe, les opérateurs qui ont entre 5 000 et 3 millions de clients sur le réseau mobile sont encouragés à entamer rapidement la transition vers IPv6. Plus d'informations sont disponibles dans le baromètre IPv6[11].

En ce qui concerne les opérateurs proposant des offres « Pro » sur le réseau mobile, des disparités importantes entre les opérateurs sont observées. Les opérateurs sont donc invités à initier et accélérer le déploiement d'IPv6 sur l'intégralité de leurs offres à destination des entreprises. Plus d'informations sont disponibles dans le baromètre IPv6[12].

11. Baromètre Arcep IPv6 2020, « Les opérateurs ayant entre 5 000 et 3 millions de clients sur le réseau mobile » : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2020_de_la_transition_vers_IPv6.pdf#page=16
12. Baromètre Arcep IPv6 2020, « Les opérateurs proposant des offres « Pro » sur le réseau mobile » : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2020_de_la_transition_vers_IPv6.pdf#page=17

La parole à



FRÉDÉRIC LASOROSKI

*Responsable Performance réseau - **Bouygues Telecom***

LE SUPPORT D'IPv6 DANS LES RÉSEAUX EST INÉLUCTABLE

L'usage de l'internet mobile et les besoins en connectivité *data* ont explosé ces 15 dernières années : avènement des smartphones, box 4G, objets communicants, voitures connectées… Dans le même temps, les générations de réseaux mobiles se sont succédé en cohabitant – de la 2G à la 5G – multipliant d'autant plus les besoins en adresses IP, et posant aux opérateurs de vrais problèmes de gestion. Bouygues Telecom a compris, il y a plus de 10 ans, que le support d'IPv6 dans les réseaux serait à terme inéluctable.

Deux difficultés cependant existaient, limitant et retardant sa mise en œuvre :

- La nécessité de faire cohabiter dans les réseaux fixes et mobiles IPv4 et IPv6, et d'utiliser pour cela des mécanismes complexes et coûteux.
- Le support d'IPv6 dans les terminaux et les box.

Rapidement, les équipementiers ont implémenté l'IPv6, suivis des fournisseurs d'applications, mais l'absence, pendant longtemps, de mécanismes de transition sur les terminaux, a empêché la mise en œuvre commerciale à grande échelle. Sur les mobiles, l'implémentation d'une adresse IPv6-*only* n'a pu être envisageable qu'avec l'intégration du 464XLAT dans la version Android 4.3.

Bouygues Telecom a su relever ces différents défis ! Elle a ainsi fait évoluer l'ensemble de son réseau ces dernières années pour supporter IPv6. Dès novembre 2015, Bouygues Telecom, premier opérateur français à lancer commercialement le service VOLTE, a activé IPv6 sur l'APN IMS. La mise en œuvre s'est ensuite poursuivie pour le service *data* mobile : pour les terminaux Android à compter de novembre 2017, puis iOS en septembre 2019. Au 31 janvier 2021, pour les clients Grand Public, 89 % des terminaux Android et 98 % du parc Iphone disposaient d'un *firmware* activant par défaut IPv6 pour le service *data* mobile. Bouygues Telecom continue aujourd'hui le déploiement d'IPv6 sur tous les segments de marché. La croissance importante du marché des objets communicants a conduit Bouygues Telecom à intégrer, dès aujourd'hui par défaut, IPv6 dans les offres IoT.



PATRICK AINARD-SIMONET

*Chef de projet IPv6 - réseau mobile - **Orange***

VERS UN RÉSEAU MOBILE IPv6-*ONLY*

Il y a plusieurs années, pour anticiper la pénurie d'adresses IPv4 annoncée, Orange a commencé la transformation de son réseau mobile pour le rendre compatible avec le protocole IPv6, même s'il existe un mécanisme de partage d'adresses IPv4 sur le réseau mobile qui le rend économe vis-à-vis de la ressource rare que constituent les adresses IPv4.

L'objectif était de connecter en IPv6 nos clients Grand Public de manière transparente, c'est-à-dire sans intervention de leur part et sans régression de la qualité de service. Dès 2019, Orange a commencé à activer IPv6 et aujourd'hui, plus de la moitié de nos clients utilisent des smartphones configurés en IPv6-*only*, sans que ce changement ne se soit traduit par une augmentation des sollicitations du service client.

Parallèlement, Orange a étendu l'accès *via* IPv6 aux clients Professionnels et Entreprises, au Machine-to-Machine et à l'internet des objets (IoT). Il est à noter qu'Orange a mis en place sur son réseau les évolutions nécessaires pour répondre à des architectures spécifiques à certaines entreprises, mais ces dernières doivent elles aussi posséder une infrastructure compatible pour interfonctionner en IPv6 avec notre réseau.

Concernant le domaine de l'IoT, IPv6 permettra de disposer de la quantité colossale d'adresses nécessaire, les opérateurs comme les entreprises ont donc intérêt à adopter ce protocole. Orange est prêt, mais ce changement doit s'opérer aussi dans les équipements du client.

En conclusion, alors que notre réseau était IPv4-*only* il y a encore quelques années, aujourd'hui IPv4 et IPv6 cohabitent, ce qui génère de la complexité, notamment en termes d'exploitation. La prochaine étape sera d'avoir un réseau IPv6-*only*. C'est en cela que la « task-force IPv6 », mise en place par l'Arcep, joue un rôle essentiel pour inciter l'ensemble des acteurs à déployer IPv6. Cette adhésion de l'ensemble des acteurs est une condition indispensable pour aller vers IPv6-*only* et profiter des avantages apportés par le protocole IPv6.

Sollicités par l'Arcep, Free et SFR n'ont pas souhaité s'exprimer dans cette rubrique.

Respect de l'obligation de compatibilité IPv6 pour les opérateurs qui se sont vu attribuer des fréquences 5G

L'Arcep a introduit une obligation de support d'IPv6 pour les opérateurs qui se verront attribuer des fréquences 5G dans la bande 3,4-3,8GHz en France métropolitaine[1] : « *Le titulaire est tenu de rendre son réseau mobile compatible avec le protocole IPv6 à compter du 31 décembre 2020* ». L'objectif, tel que précisé dans les motifs, est d'assurer l'interopérabilité des services et ne pas freiner l'utilisation de services uniquement disponibles en IPv6, dans un contexte d'augmentation du nombre de terminaux et d'une pénurie d'adresses IPv4 au RIPE NCC.

Cette obligation est motivée par l'émergence sur internet de services accessibles uniquement en IPv6 (pas de connectivité IPv4). Certaines offres d'hébergement ne proposent plus d'IPv4 par défaut[2] et l'IPv6 est donc la seule solution possible pour accéder au NAS d'un client qui est connecté à un fournisseur d'accès à internet qui utilise du Carrier-Grade NAT (CGN)[3]. Il est donc important que tous les clients puissent activer de l'IPv6 sur leur offre mobile, afin d'accéder à la totalité de l'internet.

L'Arcep a également proposé dans sa consultation publique relative à l'attribution de nouvelles fréquences (700 MHz, 900 MHz et 3,5 GHz) une obligation d'IPv6 :

- pour les réseaux mobiles à La Réunion et Mayotte[4] ;
- pour les réseaux mobiles aux Antilles et en Guyane[5].

1. Décision relative aux modalités et aux conditions d'attribution d'autorisations d'utilisation de fréquence dans la bande 3,4- 3,8 GHz : https://www.arcep.fr/uploads/tx_gsavis/19-1386.pdf
2. Exemple avec la contribution d'Ikoula dans le rapport sur l'état de l'internet en France 2020.
3. Voir lexique.
4. Consultation publique Arcep du 18 décembre 2020 sur les modalités d'attribution de fréquences dans les bandes 700 MHz et 3,4 - 3,8 GHz à La Réunion et dans les bandes 700 MHz et 900 MHz à Mayotte.
5. Consultation publique Arcep du 2 octobre 2020 sur les modalités d'attribution de fréquences dans les bandes 700 MHz et 3,4 - 3,8 GHz aux Antilles et en Guyane.

Tutoriel

COMMENT ACTIVER IPv6 SUR SON MOBILE ?

L'Arcep propose sur son site internet[1] un tutoriel qui vous explique pas à pas comment activer IPv6 sur votre smartphone Android. Les iPhone ne permettent pas actuellement aux utilisateurs de faire eux-mêmes la modification de protocole, c'est votre opérateur qui fait la demande de modification à Apple.
Pour rappel, la politique d'activation d'IPv6 des principaux opérateurs est la suivante[2] :

RÉSEAU MOBILE : POLITIQUE D'ACTIVATION D'IPv6

	bouygues	free	orange	SFR
IPv6 activé par défaut sur Android	Android 4.4 ou versions supérieures, *via* une mise à jour du constructeur du terminal	Non communiqué	Samsung : Android 9 ou versions supérieures Autres constructeurs : nouveaux produits à partir de mai 2020	Non (activation par le client depuis son terminal*)
IPv6 activé par défaut sur Android en partage de connexion	Android 4.4 ou versions supérieures, *via* une mise à jour du constructeur du terminal	Non communiqué	Samsung : Android 10 ou versions supérieures Autres constructeurs : nouveaux produits à partir de janvier 2021	Non (activation par le client depuis son terminal)
IPv6 activé par défaut sur iPhone	iPhones 5S et plus récents équipés d'iOS 12.2 ou versions supérieures	Non communiqué	iPhones 7 et plus récents équipés d'iOS 13 ou versions supérieures	iPhone 6S et plus récents équipés d'iOS 14.3 ou versions supérieures
IPv6 activé par défaut sur iPhone en partage de connexion	iPhones 5S et plus récents équipés d'iOS 12.2 ou versions supérieures	Non communiqué	iPhones 7 et plus récents équipés d'iOS 14 ou versions supérieures	iPhone 6S et plus récents équipés d'iOS 14.3 ou versions supérieures
IPv6 activé par défaut sur les offres *data* uniquement	Mise à jour progressive des terminaux compatibles	Non communiqué	Nouveaux produits à partir de janvier 2021	Non (activation par le client depuis son terminal)

Source : données à fin juin 2020, recueillies par l'Arcep auprès des opérateurs.

Si votre mobile vous propose une mise à jour, n'hésitez pas à l'installer : outre les correctifs comblant des failles de sécurité, permettant de limiter le risque de piratage, la mise à jour pourrait vous apporter IPv6.
Retrouvez sur le site de l'Arcep comment activer IPv6 sur votre mobile Android selon votre opérateur : https://www.arcep.fr/demarches-et-services/utilisateurs/activer-ipv6-mobile.html.

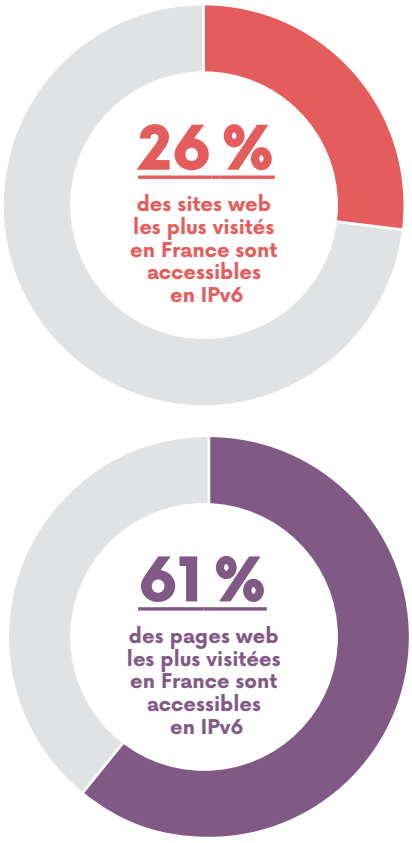
1. https://www.arcep.fr/demarches-et-services/utilisateurs/activer-ipv6-mobile.html
2. Plus d'informations sont disponibles dans le baromètre 2020 de la transition vers IPv6 en France.

2.3 Hébergeurs web

Les hébergeurs de sites web représentent encore l'un des principaux goulots d'étranglement dans la migration vers IPv6 : sur les principaux sites visités par les Français selon le classement Alexa, seuls 26 % sont accessibles en IPv6 (contre 27 % en octobre 2019)[13]. On considère un site comme accessible en IPv6 lorsqu'il dispose d'un enregistrement IPv6 (« AAAA ») au niveau du serveur DNS. Le taux de pages web accessibles en IPv6 (contenus IPv6) est, quant à lui, significativement plus élevé (61 %)[14]. La raison en est que les petits fournisseurs de contenu proposent souvent des sites web (au nombre de pages consultées généralement faible) non compatibles avec IPv6.

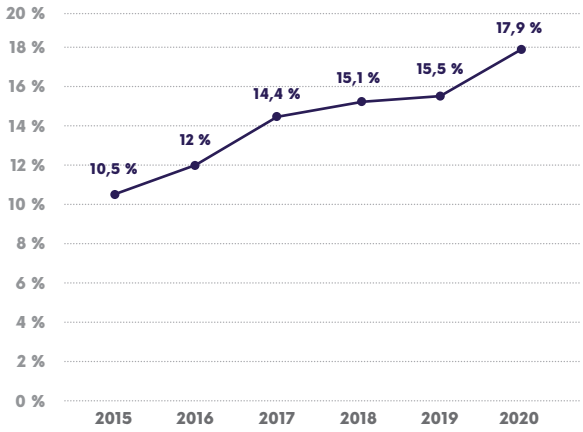
Le taux de sites disponibles en IPv6 est uniquement de 17,9 % lorsque l'on considère les 3,62 millions de sites web en.fr, .re, .pm, .yt, .tf et.wf[15]. Ce pourcentage est en augmentation depuis 2015, mais le rythme de cette évolution semble loin de pouvoir permettre une transition complète dans les prochaines années.

Même si plusieurs hébergeurs proposent IPv6 dans leurs offres, le taux de sites web accessibles en IPv6 est très faible pour tous les acteurs du Top 10 (en nombre de noms de domaine) car il n'est pas activé par défaut. Parmi les acteurs du Top 10, seuls IONOS 1&1 et Cloudflare ont plus des trois quarts des sites avec de l'IPv6, leurs déploiements constituent donc des exemples à suivre.



Source : 6lab Cisco au 02/11/2020 (6lab.cisco.com). Données sur le top 730 d'Alexa en France (www.alexa.com/topsites/countries).

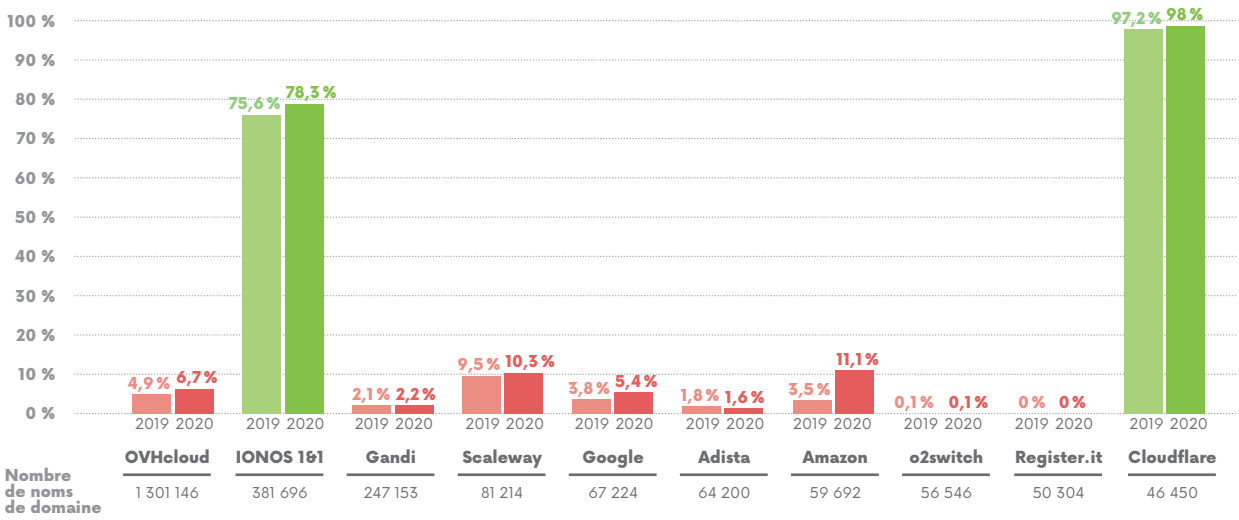
ÉVOLUTION DU TAUX DES SITES WEB ACCESSIBLES EN IPv6 sur les noms de domaine .fr, .re, .pm, .yt, .tf et.wf



Source : données Afnic à août 2020.

13. Cisco 6lab au 02/11/2020 (6lab.cisco.com). Données sur le Top 730 d'Alexa en France https://www.alexa.com/topsites/countries
14. *Ibidem*.
15. Données Afnic, août 2020. Pour ces données, les Top 10 et 100 sont définis en termes de nombre de noms de domaine hébergés.

TAUX DE SITES WEB ACCESSIBLES EN IPv6 sur les noms de domaine .fr, .re, .pm, .yt, .tf et .wf



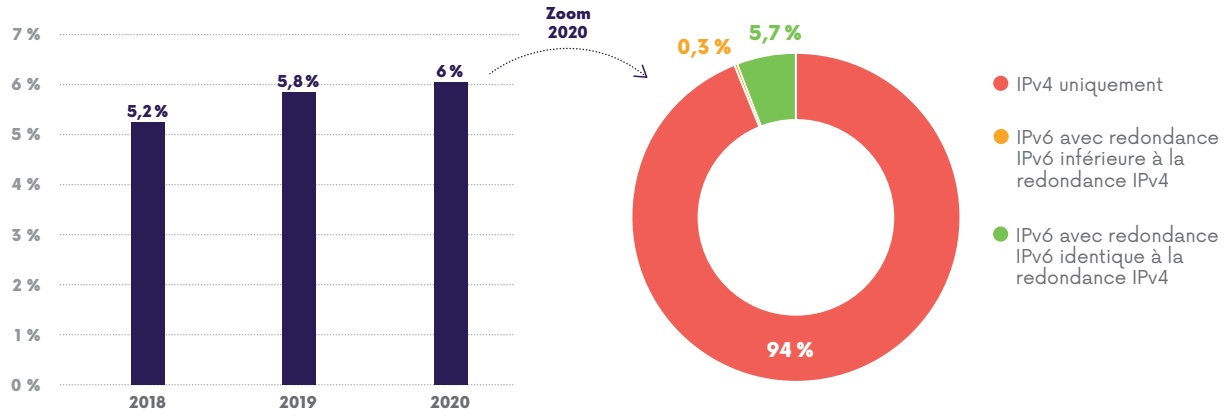
Source : données Afnic à août 2020.

2.4 Hébergeurs mail

La transition des hébergeurs mail connaît également un très fort retard : seuls 6 % des serveurs mail sont à ce jour adressés en IPv6 sur l'intégralité des .fr, .re, .pm, .yt, .tf et .wf[16] (contre 5,8 % à mi-2019). Il est à noter qu'un certain nombre d'entre eux comportent un niveau de redondance en IPv6 inférieur à celui atteint en IPv4, et est donc susceptible de poser des problèmes de résilience.

Cette année encore, le taux d'hébergement mail reste alarmant. Le retard sur ce maillon de la chaîne d'internet, s'il n'est pas comblé dans les prochaines années, pourrait obliger à conserver plus longtemps IPv4, avec des coûts inhérents. Seul Google se démarque avec plus de 95 % de noms de domaines en IPv6 pour le mail.

TAUX D'HÉBERGEMENT MAIL ACCESSIBLE EN IPv6 sur les noms de domaine .fr, .re, .pm, .yt, .tf et .wf



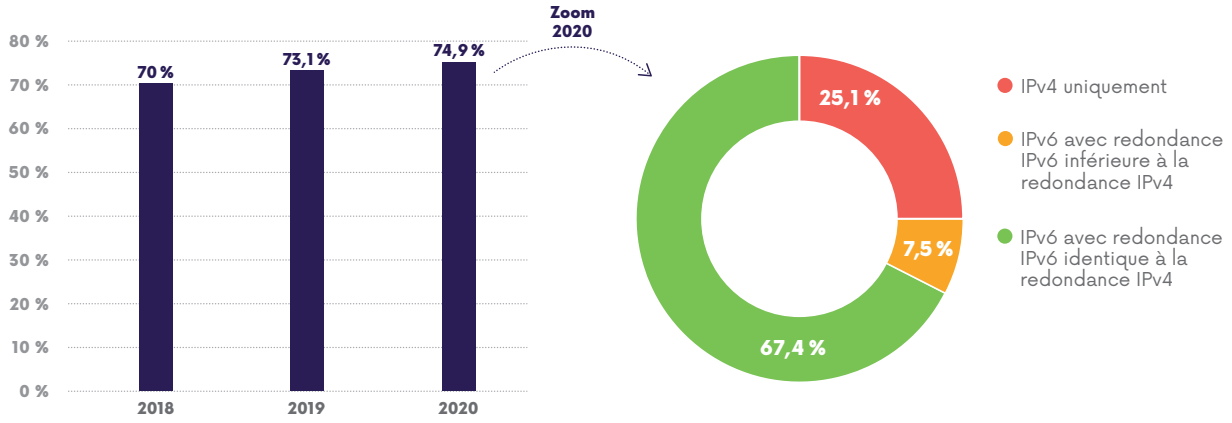
Source : données Afnic à août 2020.

16. Données Afnic, août 2020.

2.5 Infrastructure DNS

L'infrastructure DNS permet de traduire un nom de domaine, par exemple www.arcep.fr, en une adresse IP. C'est aujourd'hui le secteur le plus en avance dans la transition vers IPv6 avec environ 75 % des serveurs faisant autorité[17] supportant IPv6. Environ 67 %[18] des serveurs DNS garantissent une résilience d'IPv6 équivalente à celle d'IPv4 (niveau de redondance identique).

TAUX DE SERVEURS DNS ACCESSIBLES EN IPv6 sur les noms de domaine .fr, .re, .pm, .yt, .tf et .wf



Source : données Afnic à août 2020.

2.6 Sites web et services en ligne de l'État (.gouv.fr)

L'exemplarité de l'État dans la transition vers IPv6 étant un des leviers importants pour accélérer la migration, le baromètre a été enrichi cette année avec des indicateurs sur l'avancement de cette transition pour les différents sites web et services en ligne de l'État. L'étude actuelle concerne les 243 sites ayant un suffixe en .gouv.fr et disponibles en HTTPS[19].

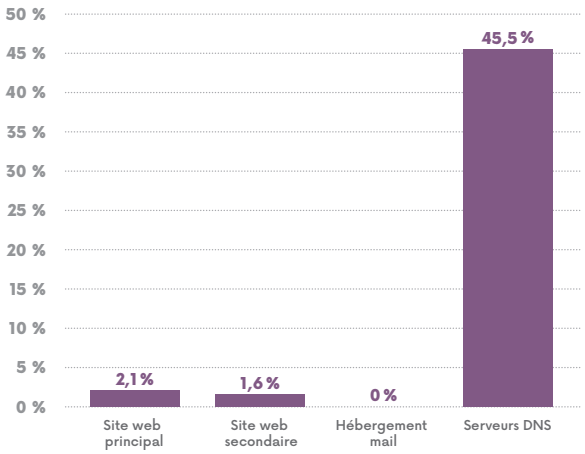
La transition vers IPv6 des serveurs DNS est relativement avancée, avec 45,5 % des serveurs en IPv6. L'hébergement mail est par contre uniquement réalisé en IPv4 et le taux de sites web en IPv6 est seulement de 2,1 % pour les sites principaux[20] et de 1,6 % pour les sites secondaires[21].

Même si quelques sites sont disponibles en IPv6, il est regrettable que la grande majorité ne soit encore accessible qu'en IPv4. Le déploiement en IPv6 des sites web et services en ligne de l'État apparaît donc encore très insuffisant, en particulier pour répondre à l'objectif d'exemplarité de l'État en matière de transition vers IPv6. Une attention accrue pourrait être portée à la compatibilité IPv6 lors des évolutions techniques des sites web existants et lors d'appels d'offres pour la création de nouveaux services en ligne.

Pour plus d'information sur l'état de déploiement d'IPv6, le baromètre de la transition vers IPv6 est disponible sur le site de l'Arcep[22].

La prochaine édition de ce baromètre sera publiée au second semestre 2021.

TAUX D'IPv6 SUR LES SITES WEB ET SERVICES EN LIGNE DE L'ÉTAT (.gouv.fr et disponibles en HTTPS)



Source : tests réalisés par l'Arcep en novembre 2020 à partir des données Afnic.

17. Un DNS faisant autorité est un serveur DNS qui fait autorité pour un domaine, c'est-à-dire qu'il détient l'information quant à la résolution d'adresse pour le domaine.
18. Données Afnic, août 2020.
19. Sur les 1 009 noms de domaine avec un suffixe en .gouv.fr existants au mois d'août 2020, seuls les 243 domaines répondant en HTTPS avec un certificat TLS valide ont été pris en compte, afin d'exclure de l'analyse les noms de domaine non maintenus ou ne proposant pas de sites web.
20. Site principal : site proposé par défaut par un moteur de recherche.
21. Site secondaire : site qui redirige vers le site principal (si le site principal est préfixé par « www », le site secondaire est sans le préfixe « www » et inversement).
22. https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2020_de_la_transition_vers_IPv6.pdf

Vers de l'IPv6-*only* au niveau du réseau et services du gouvernement fédéral des États-Unis

Le 19 novembre dernier, la présidence des États-Unis a publié un mémorandum[1] qui vise à achever la transition vers le protocole IPv6 au niveau du réseau fédéral et de ses services. L'objectif est de mettre à jour les orientations sur le déploiement opérationnel et l'utilisation d'IPv6 par le gouvernement fédéral.

Le gouvernement américain fait en effet le constat que toutes les mesures mises en place pour prolonger la durée de vie des adresses IPv4 ajoutent des coûts et de la complexité à l'infrastructure du réseau et soulèvent d'importants obstacles techniques et économiques à l'innovation. Il rappelle qu'une transition complète vers IPv6 est la seule option viable pour assurer la croissance future et l'innovation dans la technologie et les services internet.

Cette démarche n'est pas une première pour les États-Unis. En effet, elle s'appuie sur des initiatives qui ont débuté en 2005 pour favoriser l'adoption d'IPv6 et consolidées par un mémorandum en 2010 qui visait notamment à rendre les services publics (par exemple web, e-mail, DNS, FAI, etc.) disponibles en IPv6 natif et à mettre à niveau les applications clientes internes qui communiquent avec les serveurs internet publics et les réseaux d'entreprise prenant en charge l'IPv6 natif.

En complément, ce mémorandum de 2020 fixe les exigences pour achever le déploiement d'IPv6 dans tous les systèmes d'information des services fédéraux et regroupe des propositions pour aider les agences de l'État à surmonter les obstacles qui les empêchent de migrer vers de l'IPv6-*only*. Pour ce faire, certaines mesures spécifiques que les agences devraient prendre pour achever la transition vers IPv6 sont définies, notamment :

- préparer une infrastructure IPv6-*only*, en définissant un calendrier clair avec des échéances précises (par exemple : migrer au moins 80 % des terminaux IP sur les réseaux fédéraux fonctionnent en IPv6-*only* d'ici fin 2025 ; identifier et justifier les systèmes d'information fédéraux qui ne peuvent pas être migrés en IPv6 et fournir un calendrier de remplacement ou de retrait de ces systèmes ;
- veiller à ce que les futures acquisitions d'équipements incluent les exigences IPv6 ;
- faire évoluer les spécifications IPv6 en prenant en compte les recommandations de l'IETF[2] relatives à IPv6. Un accent sera mis sur la sécurité, l'IoT, les services *cloud*, le SDN[3] et les réseaux virtualisés ;
- assurer une sécurité adéquate, notamment en incluant IPv6 dans les projets de sécurité, en utilisant des solutions de sécurité compatibles avec IPv6 et capables de fonctionner dans des environnements IPv6-*only* et en suivant les bonnes pratiques pour sécuriser le déploiement et le fonctionnement des réseaux IPv6 ;
- définir les rôles et responsabilités à l'échelle du gouvernement, avec une liste des actions à mener par les différentes administrations et agences de l'État pour soutenir la transition vers IPv6.

Ainsi, ce mémorandum indique clairement que *« l'intention stratégique est que le gouvernement fédéral fournisse ses services d'information, exploite ses réseaux et accède aux services d'autrui en utilisant IPv6*-only. *»*

1. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf
2. *Internet Engineering Task Force*.
3. Voir lexique.

3 Les travaux de la task-force dédiée à IPv6 rassemblant l'écosystème d'internet

3.1 La task-force IPv6 est ouverte à l'ensemble de l'écosystème

L'Arcep et *Internet Society* France ont mis en place une task-force dédiée à IPv6 et ouverte à l'ensemble des acteurs de l'écosystème internet (opérateurs, hébergeurs, entreprises, secteur public, etc.). Elle a pour objectif de favoriser l'accélération de la transition vers le protocole IPv6 en permettant aux participants d'aborder des problèmes spécifiques et de partager les bonnes pratiques.

Le premier axe de travail identifié à l'issue de la première réunion de la task-force de novembre 2019 est d'encourager les entreprises à effectuer leur transition vers IPv6. La task-force a donc travaillé cette année à la réalisation d'un guide destiné aux entreprises et expliquant pourquoi il est important de déployer IPv6 dans son entreprise.

3.2 Le guide « Entreprises : pourquoi passer à IPv6 ? »[23]

Ce guide[24] vise à sensibiliser les entreprises sur l'importance de la transition vers IPv6 et à répondre aux principales questions :

- Quels sont les inconvénients si je reste en IPv4 sur mon réseau local ou si mon site web reste en IPv4 ?
- Dans quels délais est-il possible de migrer mon entreprise vers IPv6 ?
- Quelles parties de l'infrastructure de mon entreprise basculer en IPv6 ?
- Faut-il déployer les ordinateurs et serveurs en double pile ou en IPv6-*only* (en interne) ?

En ce qui concerne la dernière question, vous retrouverez notamment quelques éléments de comparaison de ces deux procédés de transition :

	DOUBLE PILE (*DUAL-STACK*)	IPv6-*ONLY*
Accès IPv4/IPv6	- Accès à la fois à IPv4 et à IPv6 permettant une migration en douceur	- Pas d'accès en IPv4 : des mécanismes de traduction d'adresses comme le NAT64+DNS64 ou des reserve proxys spécialisés sont nécessaires pour accéder aux ressources IPv4-*only*
Configuration	- Nécessite de configurer à la fois IPv4 et IPv6	- Nécessite de que l'ensemble des postes possèdent de l'IPv6 avant d'entamer le retrait d'IPv4 (enxemple typique lors de la dépendance à la téléphonique SIP) - Configuration plus simple
Sécurité	- Différence de politiques de sécurité au niveau des *firewalls* - Différence de services disponibles sur les serveurs double pile - Définition des règles des IPS/IDS doublées	- Une seule configuration de sécurité

Vous pourrez également découvrir dans ce guide quatre témoignages d'entreprises qui ont déjà effectué ou sont en train d'effectuer leur transition vers IPv6 :

- EDF, un exemple de migration vers IPv6 du système d'information d'un groupe qui compte 18 millions d'adresses IP et qui est arrivé au bout de ses IPv4 privés. Plutôt que de faire ce qu'ils nomment des « bidouilles » de recouvrement d'IPv4, EDF à décider de passer certaines parties de son réseau en IPv6-*only* ;
- Schneider Electric, une grande industrie qui réfléchit à la transition vers IPv6 de son réseau interne car certaines succursales ont besoin d'accéder à des ressources internet qui sont en IPv6-*only* et des problèmes de sécurité ont été remontés sur des connexions au LAN des box internet qui ont de l'IPv6 activé ;
- Digdeo, une société de services en logiciels libres qui a fait le pari d'en finir avec les réseaux NAT[25] en IPv4. Le passage à IPv6 a permis de résoudre les problèmes de NAT pour le personnel devant accéder à des ressources *backend* ;
- L'Olympique Lyonnais, une PME qui a réussi à intégrer la migration vers IPv6 dans le projet global de construction du nouveau stade de l'Olympique Lyonnais, qui permet à plus de 60 000 personnes de communiquer en même temps pendant un match.

23. https://www.arcep.fr/uploads/tx_gspublication/guide-entreprises-IPv6_dec2020.pdf
24. Pour rappel, cette restitution ne constitue en rien une prise de position de l'Arcep sur la pertinence, la faisabilité ou la priorité des axes de travail. Elle décrit uniquement les informations remontées par les différents participants à la task-force IPv6. Les priorités des actions à mettre en place se feront en concertation avec la communauté des participants.
25. Voir lexique.

3.3 Rejoignez la task-force IPv6

Pour vous accompagner dans la mise en œuvre de cette transition, la task-force poursuivra ses travaux avec la réalisation d'un guide méthodologique sur « Comment déployer IPv6 ? » qui sera prochainement disponible.

Les personnes qui souhaitent contribuer à ces travaux, partager un retour d'expérience ou mettre en place IPv6 sont invitées à faire part à l'Arcep de leur intérêt pour rejoindre la task-force *via* le code QR ci-contre.

MOOC Objectif IPv6 : un exemple de formation au service de la transition vers IPv6

Le MOOC Objectif IPv6 est une plateforme de formation gratuite et sous licence *Creative Commons* permettant l'acquisition des compétences-clés pour la mise en œuvre et la gestion d'un réseau IPv6 opérationnel. Il a été conçu par des enseignants-chercheurs des écoles membres de l'Institut Mines-Télécom et de l'Université de La Réunion, ainsi que des professionnels des réseaux. Hébergé sur la plateforme Fun MOOC, il a attiré plus de 2 000 inscrits en 2019.

Ce cours a pour objectif d'aider le participant à évoluer vers la mise en œuvre d'IPv6 dans une approche orientée vers l'opérationnel :

- après un exposé des concepts en vidéo, un support de cours complet détaille notamment la mise en œuvre opérationnelle ;
- des travaux pratiques permettent de mettre en application le protocole IPv6 dans un réseau fonctionnel virtualisé sur un poste ;
- des exercices d'approfondissement permettent des études de cas réels rencontrés sur le terrain.

Le MOOC Objectif IPv6 s'adresse aussi bien aux étudiants, professionnels ou amateurs intéressés par les évolutions d'internet. Il décrit un protocole et des mécanismes des réseaux informatiques. Il n'est pas nécessaire de maîtriser le protocole IPv4. Des rappels sur des détails précis sont donnés au besoin tout au long du cours.

Ce MOOC permet à la personne qui le suit :

- d'expliquer les différents types d'adresses IPv6, leur notation et leurs usages ;
- de créer un plan d'adressage IPv6 en tenant compte des évolutions du réseau ;
- de mettre en application les mécanismes nécessaires à un réseau IPv6 opérationnel ;
- de planifier la gestion d'un réseau IPv6 (détecter les pannes, assurer le bon fonctionnement et la sécurité) ;
- d'expliquer le besoin d'interopérabilité des réseaux et services entre IPv6 et IPv4 ;
- d'appliquer des solutions dans différents contextes d'interopérabilité.

Une septième session sera proposée prochainement, avec une partie de son cours mis à jour.

Tutoriel

LES ACCÈS IPv6-*ONLY* ET LE MÉCANISME 464XLAT

Bouygues Telecom, Free et Orange proposent par défaut à leurs clients mobiles un accès à internet en IPv6 sans proposer d'accès natif IPv4, ce qui nécessite d'utiliser un mécanisme pour accéder aux ressources de l'internet disponibles uniquement en IPv4. SFR propose de la double pile : IPv4+IPv6.

01. Le couple DNS64+NAT64 : une solution pour accéder en IPv6 côté client à un site hébergé en IPv4-*only*

Comme une partie importante d'internet est accessible uniquement en IPv4, Bouygues Telecom et Orange proposent un DNS64 : le résolveur DNS n'envoie pas une adresse IPv4 pour les sites hébergés en IPv4-*only*, mais une IPv6 spéciale : c'est une IPv6 qui pointe vers une plateforme NAT64, placée sur le réseau de l'opérateur. La plateforme NAT64 permet de faire communiquer la pile réseau IPv6 du client avec internet IPv4. La plateforme NAT64 fait une traduction d'adresse classique (NAT) mais en remplaçant l'IPv4 privée par une adresse IPv6.

02. Encapsulation de l'adresse destination IPv4 dans l'adresse IPv6

Le DNS64 génère une IPv6 construite à partir du préfixe réservé 64:ff9b::/96. Les 32 derniers bits de l'IPv6 créé sont les 32 bits de l'adresse du site en IPv4. La plateforme NAT64 sur le réseau de l'opérateur récupère l'IPv4 de destination dans l'IPv6 destination qu'il a reçu. L'opérateur sait alors créer une traduction NAT à la volée vers l'IPv4 de destination, et envoyer le paquet sur l'internet IPv4.

03. Certains usages ne fonctionnent pas avec le DNS64 : naissance du 464XLAT

Certaines applications et services peuvent ne pas fonctionner coté client avec une IPv6. C'est par exemple le cas quand une application utilise une IPv4 littérale (87.65.43.21) au lieu d'utiliser des noms DNS qui seraient résolus par le DNS64. Par exemple une application *peer-to-peer* a de fortes chances d'utiliser une IPv4 littérale à la place d'un nom de domaine. On se retrouve également en IPv4 quand une application ne fait pas appel au DNS64 proposé par le système d'exploitation, mais utilise son propre résolveur DNS qui n'est pas DNS64.

Historiquement, le 464XLAT est né de développeurs équipés de Nokia N900 qui ont cherché à utiliser le service IPv6-*only* proposé par T-Mobile aux USA. Plusieurs applications ne fonctionnaient pas, malgré la présence d'un DNS64 et d'un NAT64 chez l'opérateur. Ces développeurs ont commencé à expérimenter la traduction locale d'IPv4 en IPv6 sur le smartphone Nokia N900 en août 2010. Cela a permis à diverses applications de fonctionner correctement sur des réseaux IPv6-*only* qui, autrement, nécessiteraient IPv4. Cette même idée et ce même code ont ensuite été portés sur Android et intégrés au projet Android Open Source[1] en novembre 2012. Cela a donné naissance à la RFC6877[2], publiée en avril 2013.

Le 464XLAT est intégré à partir d'Android 4.3 Jellybean, sortie en juillet 2013. Pour le partage de connexion IPv6 lorsqu'il n'y a qu'un seul préfixe /64 délégué au combiné, il a fallu attendre la RFC7278[3], publiée en juin 2014 et son intégration à Android à partir de 5.1 Lollipop sortie en mars 2015.

1. Soumission du logiciel nécessaire pour le CLAT au projet Android Open Source.
2. RFC6877 : *« 464XLAT: Combination of Stateful and Stateless Translation »*.
3. RFC7278 : *« Extending an IPv6 /64 Prefix from a Third Generation Partnership Project Mobile Interface to a LAN Link »*.

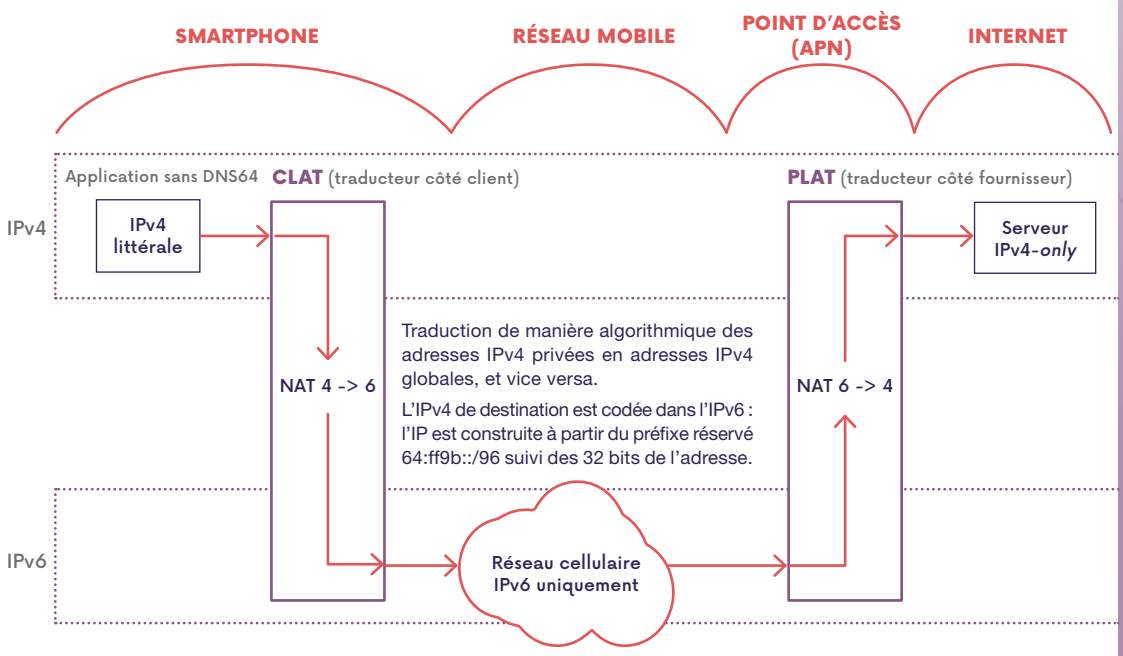
04. Le 464XLAT : une solution lorsque le client force l'utilisation de l'IPv4

Le 464XLAT consiste à introduire le CLAT (partie cliente du NAT) dans le système d'exploitation du client, pour que les applications disposent en apparence d'une adresse IPv4 privée fonctionnelle alors que le terminal n'est connecté qu'à un réseau IPv6-*only*.

Les IPv4 utilisées côté smartphone appartenant généralement à la petite plage 192.0.0.0/29, ce sont les mêmes IP pour chaque terminal. Le CLAT va traduire algorithmiquement les IPv4 en IPv6 pour le flux sortant, comme le ferait le DNS64 en utilisant le préfixe réservé 64:ff9b::/96 ou un autre préfixe découvert *via* une requête DNS vers un nom de domaine particulier : ipv4only.arpa (voir RFC 8683). Dans tous les cas, les 32 derniers bits sont les 32 bits de l'adresse du site en IPv4.

Coté opérateur, c'est le PLAT, la plateforme NAT64, qui récupère l'IPv4 de destination dans l'IPv6 destination qu'il a reçue, afin de former l'IPv4 destination, envoyé sur l'internet IPv4.

ARCHITECTURE RÉSEAU 464XLAT, SPÉCIFIÉE DANS LA RFC 6877



05. Est-il possible pour un opérateur de ne pas mettre de DNS64 ? (L'intégralité du trafic à destination de serveurs IPv4 passe par le 464XLAT)

Oui, il est possible de ne pas faire de DNS64, avec pour avantage de permettre au client de faire du DNSSEC[4], mais pour inconvénient de rajouter une latence imperceptible et d'avoir potentiellement un impact sur la batterie d'alimentation de l'appareil[5]. Une charge du processeur peut également affecter négativement les très hauts débits utilisant le CLAT : c'est pour cette raison que la majorité des opérateurs mettent en place un DNS64 qui habituellement permet d'écouler plus de 99 % du trafic IPv4 sans risque de régression du débit ou d'impact sur l'autonomie du terminal.

En absence de DNS64, les terminaux qui n'ont pas de CLAT, ou qui n'arrivent pas à l'activer, se retrouvent sans aucune connectivité IPv4.

06. Pourquoi sous Android l'IPv4 publique utilisée par le DNS64 est différent de celle utilisée pour le 464XLAT ?

De nombreux mobiles Android utilisent une IPv6 source pour le CLAT différente de l'IPv6 source utilisée pour les flux qui partent directement sur internet. La plateforme NAT64 de l'opérateur va attribuer une adresse IPv4 source différente aux flux provenant de deux IPv6 source distinctes. Il en résulte que l'IPv4 source utilisée par le NAT64 pour un même mobile est différente si la requête est réalisée *via* le DNS64 ou *via* le CLAT.

4. Voir lexique.
5. Source : RFC8683 Using 464XLAT with/without DNS64.

La parole à



PASCAL RULLIER

*CEO - **Blue Networks Technologies***

L'IPv6, PROTOCOLE DE L'AVENIR ?

Certains opérateurs, hébergeurs le considèrent ainsi. La plus grande difficulté est d'intégrer IPv6 dans les services proposés. Certains matériels installés en 2021 ne sont pas encore compatibles à l'IPv6. Cependant, avec la pénurie d'IPv4 et le RIPE qui incite fortement le déployer, le passage à l'IPv6 est inévitable. Rester en IPv4 seulement amène à « gratter les fonds de tiroirs » ou à trouver des contournements[1]. Pourquoi ne pas franchir le pas ?

Le déploiement d'IPv6 doit être fait à tous les niveaux : il faut choisir du matériel qui gère correctement l'IPv6, mais aussi, être formé à l'IPv6. Lors de déploiement de matériel, l'IPv6 doit être systématiquement intégré au même titre que l'IPv4. Au niveau services, même principe, par exemple, rajouter l'entrée DNS v6 sans oublier son entrée reverse v6[2]. Les développeurs doivent aussi intégrer la couche réseau IPv6 au même titre qu'IPv4. Son intégration permanente sera de plus en plus naturelle.

BLNT, opérateur plombier, intègre systématiquement l'IPv6 sur les réseaux qu'il déploie ou loue sur de la fibre noire ou éclairée auprès d'agglomérations ou de délégataires. Sur des réseaux loués, comme pour le FTTH avec une offre activée, les spécificités techniques pour l'IPv6 fonctionnent, mais seulement sur le papier pour l'instant. L'implémentation n'est pas forcément totalement déployée ou est trop complexe. Restons simples ! Comme en FTTO où l'opérateur d'immeuble n'assure que le transport réseau pur, l'opérateur plombier implémente par-dessus l'IPv4 et l'IPv6 en même temps.

De même, des prestataires n'utilisent pas IPv6 et préfèrent faire des redirections de ports vers des adresses IPv4 privées en interne. Il faut s'y mettre[3].

1. « IPv6, l'avenir d'internet ? » par Cécile Morange.
2. « *RFC 8501: Reverse DNS in IPv6 for Internet Service Providers* » par Stéphane Bortzmeyer.
3. « Entreprises : pourquoi passer à IPv6 ? » document réalisé par la task-force IPv6.



JACKY HAHN

*Directeur TV, Internet et Téléphonie - **Vialis***

DÉPLOIEMENT DE L'IPv6 SUR LES RÉSEAUX VIALIS

Vialis, opérateur 100 % alsacien, est présent sur le réseau câblé de Colmar et environs, sur le réseau FTTH d'initiative publique alsacien et apporte aussi son savoir-faire à de nombreux réseaux partenaires en marque blanche. Dès 2015, Vialis obtenait ses premières adresses IPv6 auprès du RIPE, et si le déploiement de ces IP auprès de nos clients s'est accéléré depuis un an, le chemin parcouru a été long.

Notre objectif est de déployer l'IPv6 en toute transparence pour le client final. La multiplicité des technologies sur lesquelles Vialis est présente nous a contraints, dès 2015, à mettre en place des maquettes de tests et a permis de valider une solution de CGNAT (*Carrier Grade NAT* – translation et partage d'IP).

Notre démarche de déploiement de l'IPv6 a été la suivante :

1. Validation de la fourniture de transit IPv6 auprès des fournisseurs et des points d'interconnexions.
2. Vérification de la compatibilité de l'ensemble des équipements réseaux et clients avec l'IPv6. Ce travail a été titanesque car il nécessite la mise à jour d'équipements en HNO et l'*upgrade* de systèmes avec des interventions sur des équipements d'anciennes générations.
3. Mise en place d'une véritable plateforme IPv6 redondée pour les services DNS, DHCP…
4. Configuration du routage IPv6 de l'ensemble des équipements des points de présence et de cœur de réseau.
5. Activation de l'IPv6 sur des clients-tests pour un réseau identifié et validation du bon fonctionnement.
6. Déploiement de l'IPv6 sur l'ensemble du réseau concerné.

Pour effectuer une transition en douceur, nous maintenons les services IPv4 en parallèle des déploiements IPv6, tout en accompagnant nos clients et nos partenaires et en garantissant le fonctionnement optimal de l'ensemble des services internet, téléphonie et télévision. Notre objectif de déploiement de 50 % à l'horizon juin 2021 reste d'actualité et sera atteint malgré le contexte actuel.

La parole à



BENOÎT DESMARECAUX

*Directeur technique associé - **iBloo Pro***

ENSEIGNER L'IPv6 AVANT MÊME DE PARLER D'IPv4

L'IPv6 est une façon de penser et de concevoir le réseau totalement différente de l'IPv4.

Technologie encore méconnue, l'IPv6 fait « peur » à beaucoup de monde (grand public, professionnels, prestataires informatiques).

Nous avons mené l'implémentation de l'IPv6 au sein de notre réseau jusque chez le client final dès la conception de notre *backbone* en *Dual-Stack*. Et nous nous sommes aperçus que l'IPv6 simplifie énormément de choses, notamment :

- L'adressage des équipements, grâce aux protocoles DHCPv6-PD.
- Le routage : on a donc des équipements moins demandeurs en ressources.
- La sécurité, puisque :
  - à ce jour, « scanner » les ports sur un bloc IPv4 /22 ne prend pas beaucoup de temps pour un hacker, contrairement à scanner un bloc /32 d'IPv6 ;
  - la gestion de pare-feu s'avère plus simple, puisque plus d'IP privée, ni de NAT/PAT (*Network Address Translation/Port Address Translation*).
- Il n'y a plus de gestion de partage de ressources NAT/PAT, ni de traçabilité en cas d'enquête judiciaire.

Pour le bon développement de l'IPv6 en France, il est essentiel d'aider les institutions publiques à préparer un plan de formation de leurs intervenants/enseignants dans les cursus post-bac.

En effet :

- L'IPv6 est encore survolé par les programmes post-bac, même dans les filières spécialisées réseau, alors que ce devrait être un réflexe, voire un point essentiel du cursus.
- Les prestataires informatiques locaux n'ont pas la connaissance nécessaire sur l'IPv6 et l'évitent.
- Les services publics sont en retard. Exemple : les serveurs de temps pool.ntp.org sont trop faiblement compatibles IPv6.

Selon nous, afin que l'IPv6 prenne la place qu'il devrait avoir, il faut commencer par l'enseigner avant même de parler de l'IPv4. Ceci pour que l'IPv6 soit un réflexe, et l'IPv4 une « adaptation » et non l'inverse.



LAURENT PAVOINE

*Directeur commercial - **K-net***

IPv6 SUR LES OFFRES ACTIVÉES DES RÉSEAUX D'INITIATIVE PUBLIQUE

La grande majorité des opérateurs d'infrastructure avec lesquels nous travaillons ont réalisé un véritable travail de fond sur l'IPv6 ! Ce qui nous permet d'avoir désormais plus de 85 % d'abonnés IPv6-*ready*.

Toutefois, malgré un fonctionnement globalement satisfaisant nous rencontrons quelques difficultés selon les opérateurs d'infrastructure et chez certains d'entre eux l'IPv6 n'est pas encore disponible.

- Covage a déployé très efficacement IPv6 sur la plus grande majorité de ses plaques et il ne reste que quelques mises à jour à réaliser. Des opérations qui sont prévues et planifiées.
- Altitude a basculé sur une nouvelle architecture ces dernières années et l'IPv6 fonctionne bien. Il ne reste que quelques clients à migrer d'ici juin 2021.
- Axione fonctionne parfaitement et totalement en IPv6.
- Le SIEA a implanté l'IPv6 sur une majorité de plaques et les discussions sont en cours pour une migration DHCPv6 sur les plaques restantes.
- Parmi les opérateurs d'infrastructure nationaux avec lesquels nous travaillons, il n'en reste désormais que deux qui n'ont pas encore implémenté l'IPv6.

Le stock d'IPv4 libre s'amenuise très rapidement. Les spéculations des IPv4 vont bon train puisqu'elles s'échangent actuellement à un cours avoisinant les 30 $.

Si les opérateurs d'infrastructure ont bien pris conscience de l'urgence et de l'intérêt de l'IPv6, encore faut-il que les fournisseurs de contenus supportent cette technologie. C'est surtout sur ce point qu'en France, l'adoption d'IPv6 reste encore un peu en retrait. En effet, si les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) sont IPv6-*ready*, il reste encore beaucoup (trop) de sites uniquement accessibles en IPv4. C'est ce constat qui nous empêche aujourd'hui d'offrir des services « IPv6-*only* » à tous nos abonnés, car ils n'auraient alors accès qu'à une partie de l'internet, à ce jour…

PARTIE 2

Veiller à l'ouverture d'internet

CHAPITRE 4
Garantir la neutralité d'internet

CHAPITRE 5
Plateformes, maillons structurants de l'accès à internet

CHAPITRE 4

GARANTIR LA NEUTRALITÉ D'INTERNET

À retenir

12 mois
de suivi pour l'Arcep et ses homologues européens sur la résilience des réseaux pendant la crise sanitaire.

Décembre 2020 : lancement d'une nouvelle version de **Wehe** comprenant un test de différenciation amélioré et un nouveau test de détection de blocage de port.

304 signalements
remontés en 2020 *via* la plateforme J'alerte l'Arcep.

Le règlement européen n° 2015/2120 garantit l'accès pour tous à un internet ouvert. L'Arcep est chargée de sa mise en œuvre en France et veille au respect de la neutralité du net par les fournisseurs d'accès à internet (FAI). Pour assurer sa mission, l'Autorité dispose d'une pluralité d'outils techniques, réglementaires et collaboratifs, qu'elle mobilise dans cet objectif.

1 La neutralité du net et les principes fondateurs d'internet

Les principes fondateurs d'internet, notamment l'ouverture « *by design* », font d'internet un espace de liberté d'expression, de communication, d'accès au savoir et de partage, mais aussi d'innovation. L'émergence du concept de neutralité du net a pour objectif de protéger l'exercice de ces libertés fondatrices d'internet. En effet, le principe de neutralité du net exclut la création d'accès à internet « à plusieurs vitesses », par une gestion favorisant certains flux d'information au détriment d'autres (pratiques discriminantes), ou la création d'accès à internet limités (à certains contenus ou à certaines plateformes). Ainsi, le principe de neutralité du net vise à assurer que le fonctionnement d'internet reste en accord avec les principes fondateurs qui le gouvernent.

1.1 L'ouverture d'internet par défaut

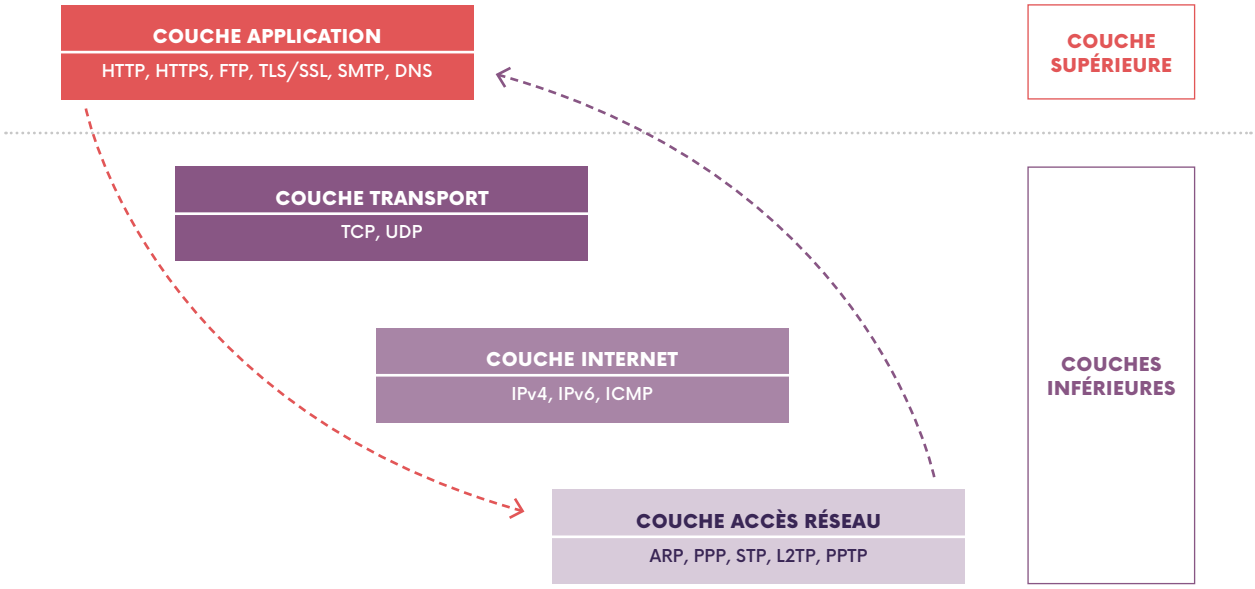
Internet est un réseau ouvert, dont le fonctionnement repose sur une architecture stratifiée en différentes couches, appelées couches réseaux. Chaque couche réseau fonctionne de manière autonome et répond à une fonctionnalité propre d'internet, comme par exemple l'accès au réseau, le transport des données ou encore le fonctionnement d'une application. La séparation effective des couches réseaux provient de l'utilisation de standards de communication propres à chaque couche réseau, appelés protocoles réseaux, qui assurent la communication entre les éléments d'une même couche. *In fine*, l'architecture d'internet repose sur un modèle théorique commun : le modèle TCP/IP, nommé d'après ses deux principaux protocoles[1].

Plusieurs principes intrinsèques au fonctionnement d'internet découlent du modèle TCP/IP : le fonctionnement autonome des couches réseaux (*layering principle*), le principe du « meilleur effort » dans l'acheminement des données (*best effort principle*), le principe de bout-en-bout (*end-to-end principle*) ou encore le principe de transparence du réseau (*network transparency*).

Chaque couche réseau fonctionne de manière autonome : la segmentation des différentes fonctionnalités d'internet implique que les couches réseaux inférieures se concentrent sur l'acheminement des données utiles qui leur sont confiées (adressage et routage de l'information transmise), laissant la responsabilité des autres fonctionnalités (traitement et présentation des données acheminées) à la couche supérieure, dite applicative (cf. schéma synthétique du modèle TCP/IP p. 72).

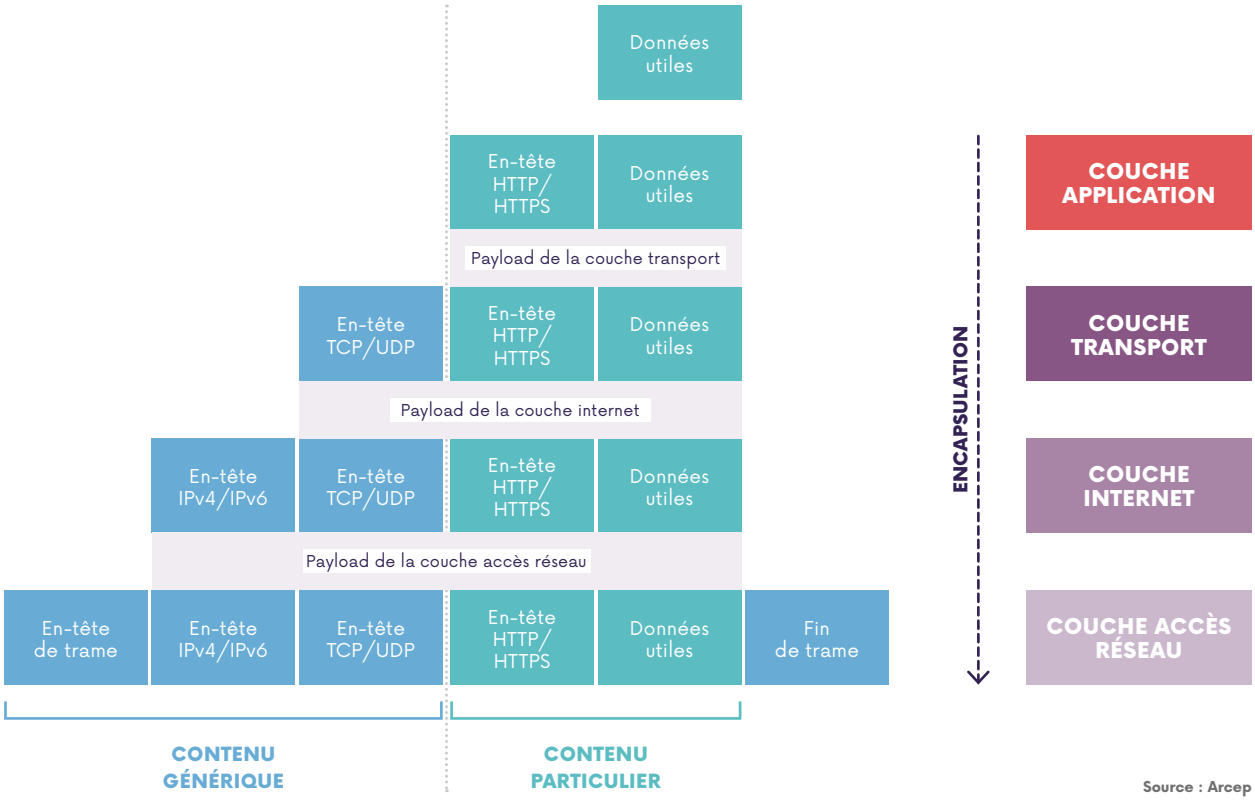
1. Les protocoles TCP/IP sont les protocoles communément utilisés. Néanmoins d'autres protocoles de fonctionnement existent, notamment le protocole UDP. Voir le schéma synthétique du modèle TCP/IP (p. 72) pour une liste non exhaustive des autres protocoles utilisés au sein des différentes couches réseaux.

SCHÉMA SYNTHÉTIQUE DU MODÈLE TCP/IP



Source : Arcep

SCHÉMA SYNTHÉTIQUE DU MÉCANISME D'ENCAPSULATION



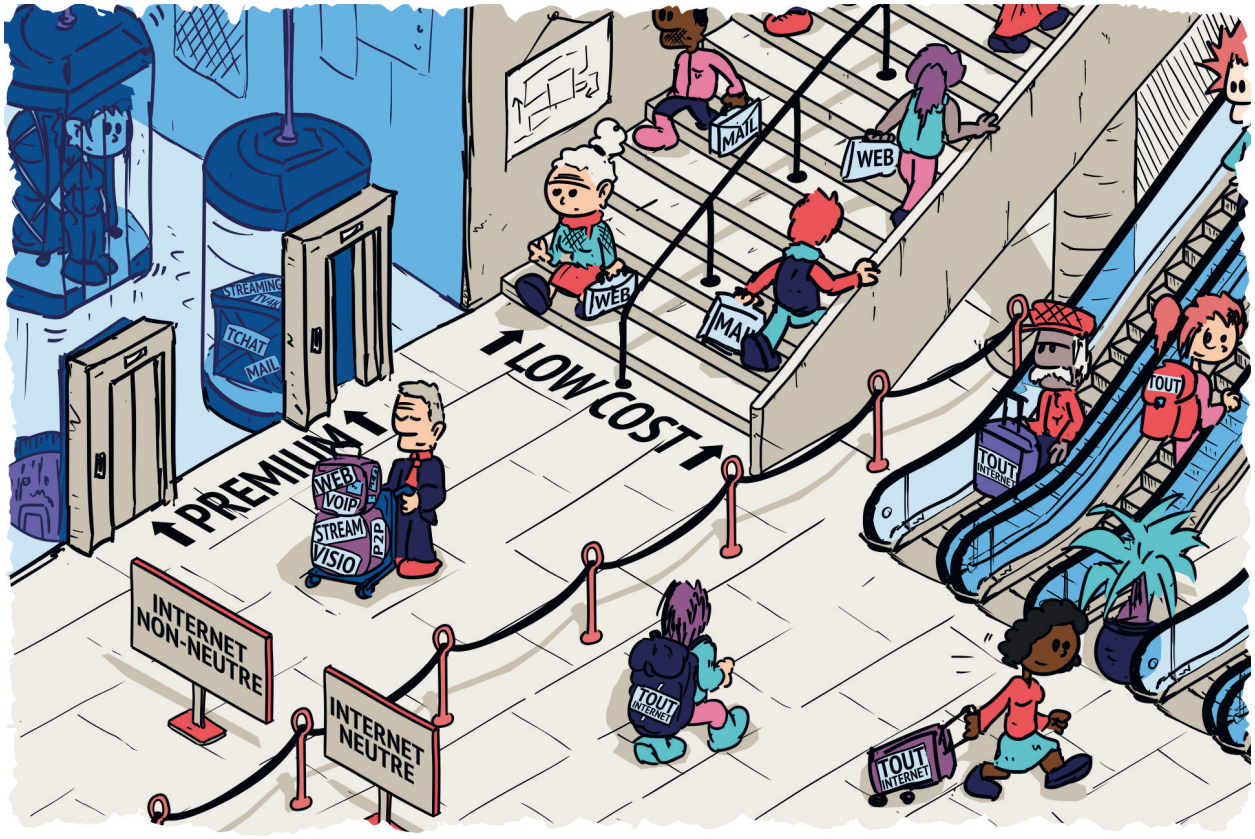
Source : Arcep

Pour éviter que les données transmises se perdent lorsqu'elles passent successivement les couches réseaux, chaque couche réseau ajoute des informations essentielles aux données transmises, qui sont regroupées dans un en-tête positionné au début de chaque paquet de données transféré par la couche précédente (cf. schéma synthétique du mécanisme d'encapsulation p. 72).

Seules les informations contenues dans l'en-tête destiné à une couche réseau sont utilisées par cette dernière. À titre d'exemple, la couche transport utilise les informations de l'en-tête « transport » pour acheminer les données reçues, mais n'est théoriquement pas en mesure de savoir si les données reçues de la couche applicative sont celles d'un e-mail, d'une vidéo ou d'une page web. Cela implique *de facto* la circulation des données transmises de manière indifférenciée et de la meilleure manière possible dans les différentes couches traversées, conformément au principe du « meilleur effort ». Selon le principe de « bout-en-bout », seuls les services de la couche applicative s'assurent de vérifier de l'intégralité et de la conformité des données transmises. Enfin, la segmentation des différentes fonctionnalités d'internet en couches réseaux rend le fonctionnement des couches réseaux inférieures transparent pour les services appartenant à la couche applicative. Ainsi, l'utilisateur final est en théorie libre d'utiliser le terminal ou le système opérateur de son choix, car leur fonctionnement reste indépendant du fonctionnement des couches réseaux inférieures.

1.2 L'innovation grâce à l'ouverture d'internet par défaut

L'architecture d'internet selon le modèle TCP/IP permet une segmentation de ses fonctionnalités et le recours à des conventions communes de fonctionnement que sont les protocoles réseaux. Cette uniformisation offre un cadre homogène au sein duquel les utilisateurs finaux disposent d'une égalité de traitement dans l'accès ou la diffusion par les réseaux de leurs contenus, de leurs services ou de leurs applications. En effet, internet incite les utilisateurs finaux à avoir une participation active dans la création de nouveaux contenus au niveau de la couche applicative, en disposant d'un cadre connu et en leur évitant de prendre en compte le fonctionnement des couches réseaux inférieures (cf. le principe de transparence du réseau). De plus, le recours à des protocoles réseaux, communément admis au sein d'une même couche, réduit les coûts de création d'un nouveau service par l'utilisateur final, favorisant *de facto* l'innovation. Ainsi, internet reste un environnement moteur de l'innovation.





1.3 Le principe de neutralité du net protège les principes fondateurs d'internet

Les principes fondateurs d'internet, explicités brièvement ci-dessus, innervent le principe même de neutralité du net : garantir la circulation des contenus, des services et des applications de la meilleure manière possible, indépendamment de l'origine et du contenu des paquets en circulation ; n'utiliser que les en-têtes de données nécessaires à l'acheminement des paquets en circulation[2] ou encore assurer le libre recours à l'équipement de son choix par l'utilisateur final. *In fine*, la neutralité du net est un cadre réglementaire qui préserve l'ouverture « *by design* » d'internet, offrant aussi des externalités positives importantes en matière d'innovation et de protection des droits des utilisateurs finaux.

Les principes essentiels au fonctionnement d'internet promeuvent un acheminement non discriminatoire des flux de données, assurant en conséquence un accès aux contenus, services et applications en ligne, ainsi qu'une diffusion indifférenciée, des services et des applications en ligne. Cette liberté permet à chaque utilisateur final de décider librement la manière dont il utilise internet. Cette capacité à recevoir et à communiquer librement contribue directement à promouvoir certains droits des utilisateurs finaux : le maintien de la diversité et du pluralisme des contenus médiatiques, la liberté d'expression ou encore le droit d'accès à l'information. Préserver la neutralité d'internet, c'est aussi préserver l'exercice effectif des droits fondamentaux des utilisateurs finaux.

L'année 2020 a pourtant été marquée par de nombreuses limites à la neutralité du net dans plusieurs pays du monde, au risque de restreindre les droits fondamentaux des populations concernées.

En Asie, plusieurs États mettent en œuvre continuellement des pratiques dénoncées comme limitant l'ouverture d'internet, en contrôlant l'accès aux contenus ou aux informations par leur population. En Chine, l'accès à internet est filtré par le « *Grand Firewall chinois* » qui contrôle les informations qui entrent et qui sortent du pays. En Birmanie, les autorités au pouvoir ont ordonné à plusieurs reprises des coupures d'internet et l'usage restreint des réseaux sociaux afin de limiter les échanges entre manifestants et soutiens de la précédente dirigeante du pays. Au Vietnam, les autorités brident les débits d'accès à certains réseaux sociaux afin qu'ils acceptent leurs demandes de censure.

Au Moyen-Orient, différentes pratiques ont été décriées : certains États restreignent l'accès à la totalité d'internet pour leur population. En Iran, seul un internet « national » dont le contenu est approuvé par le Gouvernement sera prochainement accessible aux Iraniens. Au Qatar, certains services sont interdits d'accès, tels que les services de communication VoIP[3]. Enfin aux Émirats arabes unis, plusieurs contenus jugés politiquement sensibles ne sont pas accessibles, ainsi que les services de communication VoIP ou encore les services VPN[4] dont l'usage est pénalement répréhensible.

Les États-Unis font également l'objet de vives critiques concernant la restriction de l'accès à certains services en ligne. Le 6 août 2020, l'administration américaine a pris un décret bannissant deux applications chinoises, *TikTok* et *WeChat*, des magasins d'applications au motif d'un risque pour la sécurité nationale. Toutefois, la juridiction fédérale américaine a suspendu ce décret estimant qu'un tel acte administratif posait de sérieuses questions au regard de la liberté d'expression, illustrant à nouveau le lien étroit entre droits fondamentaux et neutralité d'accès à internet. De plus, la nomination de la nouvelle présidente par intérim de la *Federal Communications Commission* (FCC), Jessica Rosenworcel, favorable à la neutralité du net, pourrait conduire une politique réglementaire très différente de celle mise en œuvre par la FCC ces dernières années.

2. Cf. p. 66 du rapport 2020 sur l'état d'internet en France.
3. Voir lexique.
4. Voir lexique.



Les travaux de l'UNESCO sur l'universalité de l'internet

Ce lien entre ouverture d'internet et défense des droits fondamentaux a aussi été réaffirmé par l'UNESCO dans sa définition des indicateurs relatifs à l'universalité de l'internet. Dans son rapport publié en 2019[1], l'UNESCO recense plus de 300 indicateurs répartis en 5 catégories.

Les quatre principes identifiés comme essentiels à l'universalité de l'internet sont les principes dits « D-O-A-M » :

D – l'internet est fondé sur les Droits humains

O – il est Ouvert

A – il devrait être Accessible à tous

M – il est alimenté par la participation de Multiples acteurs.

À ces indicateurs s'ajoutent des indicateurs transversaux qui abordent les questions de genre et les besoins spécifiques des enfants, le développement durable, la confiance et la sécurité, ainsi que les aspects juridiques et éthiques de l'internet.

Ces indicateurs visent à aider les gouvernements nationaux à mieux accompagner le développement d'un internet ouvert et protecteur des droits fondamentaux des utilisateurs finaux.

1. UNESCO, *Indicateurs de l'UNESCO sur l'universalité de l'internet : cadre pour évaluer le développement de l'internet*, 2019, https://unesdoc.unesco.org/ark:/48223/pf0000367859

La parole à



WINSTON MAXWELL

Directeur d'études Droit et Numérique – ***Télécom Paris, Institut Polytechnique de Paris***

QUEL FUTUR POUR LA NEUTRALITÉ DU NET AUX ÉTATS-UNIS ?

La neutralité du net aux États-Unis a été enfermée dans un débat étroit sur la question de savoir si les fournisseurs d'accès à internet (FAI) sont des « transporteurs publics » en vertu de l'*US Communications Act*. La FCC a fait des allers-retours sur cette question en fonction du parti politique qui contrôlait la Maison Blanche, et chacune des décisions de la FCC a été contestée devant les tribunaux. Les États-Unis n'ont jamais adopté de loi sur la neutralité du net, laissant le régulateur fédéral avec seulement quelques fondements statutaires auxquels raccrocher une politique de neutralité. L'élection de Joseph Biden changera-t-elle les choses en permettant peut-être l'adoption d'une loi nationale sur la neutralité du net ? Probablement pas.

La neutralité du net reste politiquement source de division, et beaucoup de choses ont évolué depuis l'ordonnance de la FCC sur la neutralité du net en 2015. Les FAI, qu'ils soient fixes ou mobiles, contrôlent toujours les goulots d'étranglement sur l'accès à internet, et ont toujours les moyens et les raisons de discriminer. Mais peu de cas de blocage réel ou de discrimination inappropriée au niveau des réseaux d'accès sont avérés. Les questions actuelles tournent autour du *zero-rating* et de la manière dont les niveaux de qualité de services différenciés à venir avec la 5G cohabiteront avec les principes de la neutralité. La plupart des discriminations et des abus de ce pouvoir de goulot d'étranglement se sont produits au niveau des grandes plateformes de réseaux sociaux, appelant à la réglementation des « *Big Tech* », y compris le démantèlement de certaines grandes plateformes.

L'administration Biden soutiendra la neutralité du net, mais n'en fera peut-être pas une priorité, préférant plutôt se concentrer sur la réglementation des plateformes, le déploiement de la 5G, la cybersécurité et la réduction de la fracture numérique. Lorsque l'administration Trump à la tête de la FCC a annulé l'ordonnance de 2015 sur la neutralité du net prise par l'administration Obama, la Californie a adopté sa propre loi sur la neutralité du net, que l'administration Trump a rapidement contestée devant les tribunaux. L'administration Biden a mis un terme au procès engagé par le gouvernement fédéral contre la Californie, laissant la Californie et d'autres États libres d'appliquer leurs propres lois sur la neutralité du net. La loi californienne ressemble à celle prise en Europe et servira de test pour savoir comment la neutralité du net peut, par exemple, réglementer les nouveaux services de la 5G. La nouvelle FCC pourrait potentiellement réédicter l'ancienne ordonnance de 2015, qualifiant ainsi les FAI de transporteurs publics, mais la FCC restera sur un terrain fragile en l'absence d'une nouvelle loi fédérale.

Le débat acharné sur la réglementation des plateformes nous amène à nous demander si la neutralité pourrait dépasser les FAI, en s'appliquant potentiellement aux grandes plateformes de réseaux sociaux et aux systèmes d'exploitation des terminaux mobiles. Les préjudices, que la neutralité du net vise à éviter, existent également à d'autres niveaux de l'écosystème d'internet. Par exemple, le problème de donner une préférence indue aux fournisseurs de contenu qui ont un lien capitalistique ou contractuel avec le FAI existe également pour certaines plateformes et systèmes d'exploitation des terminaux mobiles. Le problème de la limitation du choix des contenus que les internautes peuvent consulter ou publier existe également, bien que sous des formes différentes, à différents niveaux de l'écosystème d'internet. Brider l'innovation, une autre préoccupation de la neutralité du net, fait aussi partie du débat sur les plateformes.

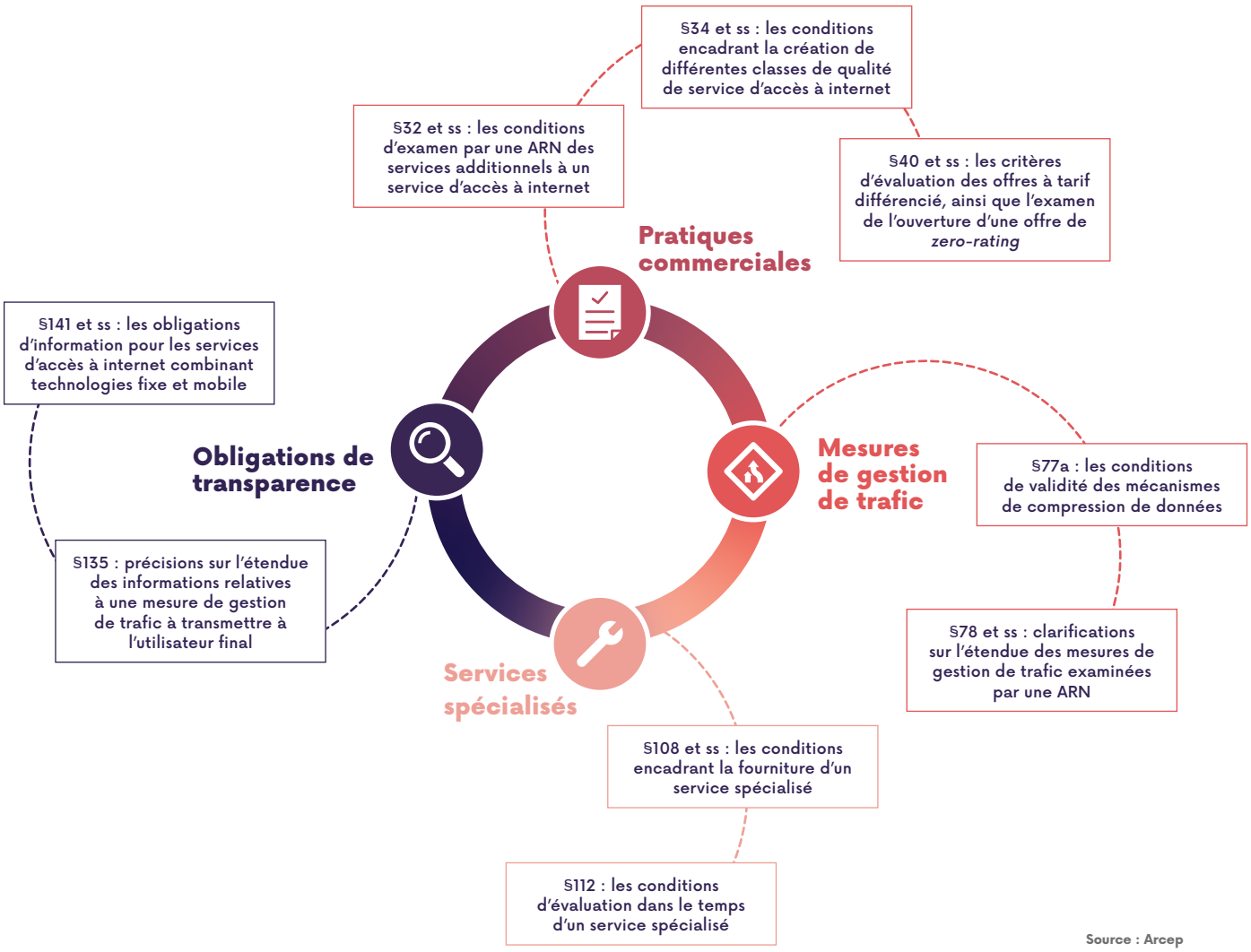
Sommes-nous en mesure de créer des principes de neutralité communs qui s'appliqueraient à tous les goulots d'étranglement de la chaîne de valeur d'internet ? Il ne sera pas facile de trouver des principes communs, car les problèmes ne sont pas identiques entre les réseaux sociaux, les systèmes d'exploitation des terminaux mobiles et les réseaux d'accès. Néanmoins, en se concentrant sur les préjudices causés par toutes les formes de goulot d'étranglement sur internet, la neutralité du net pourrait être transformée en principes directeurs d'équité sur internet qui s'appliqueraient aux plateformes, aux systèmes d'exploitation des terminaux mobiles et aux réseaux d'accès. Un nouvel aspect majeur du débat concerne la liberté d'expression sur internet. Au commencement d'internet, toute forme de filtrage de contenu était considérée comme une ingérence inacceptable dans la liberté d'expression et le bon fonctionnement du marché des idées. Plus récemment, un discours ouvert et non filtré sur les réseaux sociaux a conduit à l'apparition de contenus extrêmes et manipulateurs omniprésents, représentant une menace pour les institutions démocratiques, que la liberté d'expression et la neutralité du net sont censées protéger. Toute nouvelle approche de la neutralité devrait prendre en compte ce changement et considérer comment la modération de contenus en ligne à n'importe quel niveau de l'écosystème d'internet peut préserver les valeurs de la liberté d'expression sans conduire à un effondrement des processus démocratiques, des débats raisonnés et de la confiance en la science.

2 Une participation active renouvelée au niveau européen

En 2020, l'Arcep et ses homologues ont contribué activement à la finalisation des lignes directrices révisées relatives à la mise en œuvre du règlement internet ouvert. Publiées le 16 juin 2020, ces lignes directrices conservent la structure des lignes directrices précédentes, elles-mêmes calquées sur la structure du règlement internet ouvert, organisé autour de quatre thèmes principaux : les pratiques commerciales, les mesures de gestion de trafic, les services spécialisés et les obligations de transparence. Les clarifications apportées sont nombreuses et portent notamment sur l'analyse des offres de *zero-rating*, les conditions pour la création de différentes classes de qualité de service d'accès à internet ou encore les critères d'analyse des services dits « spécialisés ».

La révision des lignes directrices a aussi permis d'aborder la question de l'accès par les FAI aux noms de domaine (ou aux URL) à des fins de gestion de trafic ou à des fins de facturation. Pour rappel, le règlement internet ouvert permet aux FAI d'accéder uniquement aux informations contenues dans l'en-tête du paquet IP et dans l'en-tête du protocole de la couche transport, excluant ainsi d'avoir recours aux informations appartenant au contenu dit « spécifique »[5]. Pour approfondir leurs connaissances sur ce sujet, l'Arcep et ses homologues européens ont poursuivi leurs échanges avec l'écosystème en organisant le 12 novembre 2020 un événement au sein du BEREC relatif aux mécanismes d'identification du trafic dans les réseaux. Plusieurs intervenants extérieurs (équipementiers, fournisseurs de contenu et opérateurs) ont eu l'opportunité de présenter leurs positions sur les enjeux qui entourent l'identification des flux de trafic au regard des dispositions du règlement internet ouvert[6].

RÉVISIONS PRINCIPALES DES LIGNES DIRECTRICES RELATIVES À LA NEUTRALITÉ DU NET



Source : Arcep

5. Pour une explication détaillée de la distinction entre contenu générique et contenu spécifique, voir le schéma synthétique du mécanisme d'encapsulation ci-dessus ou p. 66 du rapport 2020 sur l'état d'Internet en France.
6. *BEREC public virtual workshop on traffic identification* - BEREC (europa.eu).

RAPPORTS DU BEREC SUR LA RÉSILIENCE DES RÉSEAUX EN EUROPE PENDANT LA CRISE SANITAIRE

MARS 2020

19 | Déclaration commune du BEREC et de la Commission européenne BoR(20)66
25 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)82
27 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)73

AVRIL

01 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)77
03 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)78
08 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)80
15 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)81
17 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BOR(20)83
22 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)85
24 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)86
29 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)87

MAI

07 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)88
14 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)89
20 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)90
28 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)117

JUIN

04 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)119
11 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)120
18 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)127
25 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)133

JUILLET

30 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)142

AOÛT

27 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)146

SEPTEMBRE

30 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)177

OCTOBRE

29 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)202

NOVEMBRE

30 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)233
30 | Synthèse des mesures réglementaires des EM liées à la crise de Covid-19 BoR(20)234

DÉCEMBRE

17 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(20)249

MARS 2021

31 | Rapport du BEREC sur l'état des réseaux pendant la crise de Covid-19 BoR(21)58

Source : Arcep

Les autorités de régulation nationales (ARN) ont aussi étroitement collaboré entre elles sur la résilience des réseaux en Europe pendant la crise sanitaire de Covid-19. Dès les premières semaines, l'Arcep et ses homologues ont tenu un rapport bi-hebdomadaire, puis mensuel et enfin trimestriel sur la résilience de leurs réseaux. En parallèle de ce *reporting* régulier, les ARN ont échangé sur les possibles mesures de gestion de trafic pour les opérateurs afin de faire face à la demande accrue de connectivité, en particulier avec la généralisation du télétravail, de la téléconsultation ou de l'enseignement en ligne. Les membres du BEREC et la Commission européenne ont publié une déclaration commune le 19 mars 2020[7], qui rappelle la possibilité offerte aux opérateurs par le règlement internet ouvert de prendre des mesures de gestion de trafic exceptionnelles afin d'éviter ou d'atténuer les effets d'une congestion imminente, exceptionnelle ou temporaire dans leur réseau. *In fine*, une augmentation du trafic a été constatée sur l'ensemble des réseaux en Europe pendant la crise sanitaire sans qu'aucune congestion majeure soit observée.

Première interprétation par la Cour de justice de l'Union européenne du règlement européen relatif à la neutralité du net

Fin 2018 et début 2019, la Cour de Budapest a saisi la Cour de justice de l'Union européenne de plusieurs questions préjudicielles portant sur des offres de *zero-rating* proposées par l'opérateur national Telenor (Affaires jointes C-807/18 et C-39/19)[1].

L'opérateur hongrois proposait des offres commerciales où l'accès à certains services en ligne n'était pas décompté du volume de données du reste d'internet et n'était pas bridé ou bloqué une fois ce volume de données épuisé. L'opérateur justifiait cette pratique au motif que ses clients avaient librement contracté ses offres et que l'interdiction de discrimination énoncée à l'art 3.3 du règlement internet ouvert n'était dès lors pas applicable. De plus, l'examen au regard de l'article 3.3 n'était possible selon lui qu'à l'issu d'un examen préalable de l'incidence de ces offres sur l'exercice des droits des utilisateurs finaux, conformément à l'article 3.2.

Dans son arrêt, la Cour de justice ne fait pas droit à l'opérateur Telenor et conclut que le fonctionnement d'une application *zero-ratée* après le *data cap* alors que le reste d'internet est bridé ou bloqué est une pratique contraire *per se* à l'article 3.3, sans que l'ARN soit tenu d'examiner au préalable cette pratique au regard de l'article 3.2.

Si une pratique tarifaire de *zero-rating* n'est pas contraire *per se* au règlement internet ouvert, la Cour précise qu'il est impossible pour un opérateur d'utiliser la liberté contractuelle et l'article 3.2 pour justifier l'implémentation de mesures de gestion de trafic, telles que celles décrites ci-dessus. De même, la Cour précise qu'une pratique commerciale où le client ne dispose d'un accès sans restriction qu'à certaines applications *zero-ratées* est susceptible de constituer une limitation de l'exercice des droits des utilisateurs finaux énoncés à l'article 3.1.

1. *CJUE, 15 septembre 2020, Telenor MagyarországZrt./Nemzeti Média-és Hírközlési Hatóság Elnöke, (Aff. Jointes, C-807/18 et C-39/19).*

7. Déclaration conjointe de la Commission européenne et du BEREC sur la manière de faire face à la demande accrue de connectivité des réseaux due à la pandémie liée au Covid-19.

La parole à




VÉRONIQUE NEY & KLAUS NIEMINEN

*Co-responsables du groupe de travail sur l'internet ouvert - **BEREC***

MÉCANISME DE SUIVI SPÉCIAL DU BEREC SUR L'ÉTAT DU TRAFIC INTERNET COMPTE TENU DE LA CRISE DE COVID-19

En 2020, les autorités réglementaires nationales (ARN) ont dû faire face aux effets de la crise de la Covid-19 sur la gestion des réseaux de leurs fournisseurs d'accès à internet (FAI). Dans une déclaration commune[1] avec la Commission européenne le 19 mars 2020, le BEREC s'est engagé à mettre en place un mécanisme de *reporting* spécial pour assurer un suivi régulier de la situation du trafic internet dans chaque État membre afin de pouvoir répondre rapidement aux éventuels problèmes de capacité qui pourraient résulter d'une augmentation dans l'utilisation d'internet, en raison des mesures d'urgence liées à la Covid-19 prises dans toute l'Union européenne.

Dans la déclaration commune, le BEREC a déclaré que « *conformément au règlement [Internet ouvert (UE) n°2015/2120], les opérateurs sont autorisés à appliquer des mesures exceptionnelles de gestion du trafic, notamment pour prévenir la congestion imminente du réseau et pour atténuer les effets d'une congestion exceptionnelle ou temporaire du réseau, toujours à condition que des catégories de trafic équivalentes soient traitées de manière égale. Cela pourrait devenir pertinent à la suite des mesures de confinement prises pour faire face à la crise de Covid-19. Les opérateurs peuvent se prévaloir de cette exception, si les mesures de gestion du trafic qu'ils envisagent sont nécessaires pour résoudre ou prévenir la congestion et qu'elles ne sont maintenues qu'aussi longtemps que nécessaire.* » La déclaration commune énumère les considérations dont les opérateurs doivent tenir compte en cas de congestion imminente du réseau. Elle invite également les opérateurs à coopérer étroitement avec les ARN et à les informer en temps utile de toute mesure prise afin d'assurer la transparence nécessaire aux particuliers et aux entreprises et de faire en sorte que les ARN puissent s'acquitter de manière efficiente et efficace de leurs tâches de surveillance.

Les données recueillies auprès des opérateurs européens indiquent que le trafic internet a augmenté pendant la période de confinement. Cependant, cette augmentation du trafic internet n'a pas conduit à une congestion générale des réseaux. À partir d'avril 2020, les volumes de trafic ont commencé à se stabiliser et un nombre croissant d'ARN ont réduit la fréquence de collecte de données auprès des opérateurs sur l'état de leurs réseaux.

Le BEREC, en étroite coopération avec le BEREC Office[2], a publié un premier rapport de suivi le 8 avril 2020, puis une mise à jour hebdomadaire de ce rapport jusqu'à fin juin 2020. Ces rapports résumaient l'état du trafic internet et les mesures prises par les différentes ARN et les opérateurs.

Depuis mai 2020, les rapports contiennent également des informations sur d'autres mesures prises dans le secteur des communications électroniques par les ARN, les organismes gouvernementaux, les institutions et les opérateurs depuis le début de la pandémie. Entre juillet et décembre 2020, les rapports ont été publiés sur une base mensuelle. À partir de 2021, les rapports de synthèse sont publiés sur une base trimestrielle avec une prochaine itération attendue fin juin.

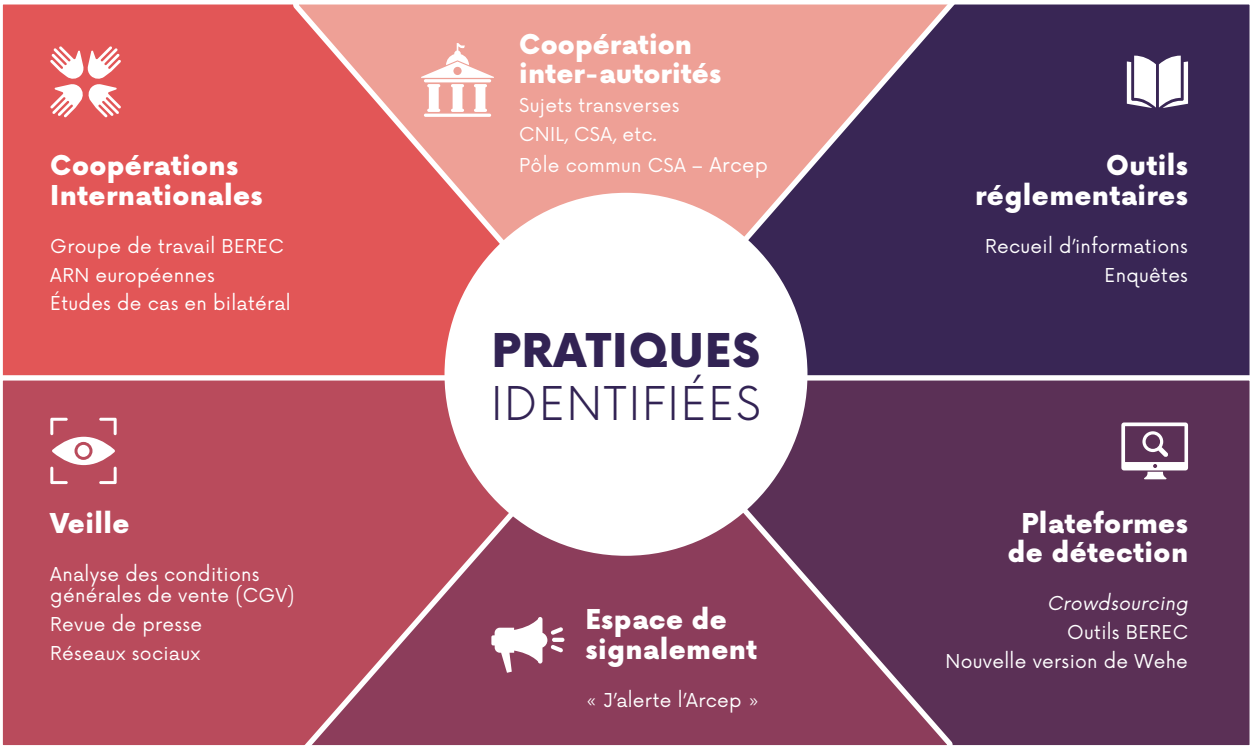
Tous les rapports publiés par le BEREC sont disponibles sur le site internet du BEREC[3]. 33 ARN ont contribué aux exercices de collecte d'informations.

1. https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9236-joint-statement-from-the-commission-and-the-body-of-european-regulators-for-electronic-communications-berec-on-coping-with-the-increased-demand-for-network-connectivity-due-to-the-covid-19-pandemic
2. Le *BEREC Office*, l'agence de support du BEREC, a été mis en place par le règlement (UE) 2018/1971 du Parlement européen et du Conseil du 11 décembre 2018.
3. Par exemple, le rapport de décembre est disponible sur https://berec.europa.eu/eng/news_and_publications/whats_new/7877-berec-publishes-an-updated-summary-report-onthe-status-of-internet-capacity

3 Une boîte à outils en constante évolution

Afin de veiller à la neutralité du net, l'Arcep s'est dotée d'une boîte à outils lui permettant de disposer d'une vue d'ensemble des pratiques relatives aux quatre pierres angulaires du règlement sur l'internet ouvert : les pratiques commerciales, les mesures de gestion de trafic, les services spécialisés et les obligations de transparence.

LA BOÎTE À OUTILS DE L'ARCEP EN MATIÈRE DE NEUTRALITÉ DU NET



Source : Arcep

Dans le cadre de sa mission de veille, les services de l'Autorité examinent de manière continue les conditions d'utilisation des offres des fournisseurs d'accès à internet. En 2020, l'Arcep a poursuivi son travail de veille, notamment sur les offres d'accès à internet commercialisées par les opérateurs ultramarins.

En complément de ce travail de veille, l'Autorité dispose d'outils réglementaires permettant de recueillir auprès des FAI des informations sur les règles de gestion de leurs réseaux.

Depuis 2017, l'Arcep met aussi à disposition des utilisateurs finaux une plateforme de signalement « J'alerte l'Arcep ». En 2020, 304 signalements relatifs à la neutralité du net ont été déposés sur cette plateforme. Les signalements déposés par les utilisateurs finaux ont permis à l'Autorité d'identifier rapidement de possibles infractions au principe de neutralité d'internet et de favoriser une résolution rapide des difficultés soulevées, détaillées dans la section suivante.

Au cours de l'année précédente, l'Arcep a poursuivi ses collaborations avec d'autres autorités de régulation françaises, notamment le Conseil supérieur de l'audiovisuel (CSA) avec lequel un pôle numérique commun a été mis en place fin 2020. Ainsi, les coopérations inter-autorités nationales permettent de croiser les compétences respectives de chacun afin de faire progresser l'analyse réglementaire sur des sujets communs et transversaux.

La coopération avec d'autres autorités de régulation s'est aussi intensifiée au niveau européen en 2020, en particulier avec la crise sanitaire. L'Arcep et ses homologues ont eu de nombreux échanges au sein du BEREC, notamment sur la question de la résilience de leurs réseaux en Europe. En parallèle, l'Arcep a également entretenu une coopération renforcée avec certaines autorités de régulation nationales au travers d'échanges bilatéraux sur des études de cas, permettant ainsi de mieux appréhender d'éventuelles situations nationales similaires à celles rencontrées par ses homologues.

DIFFÉRENTS *REPLAYS* TESTÉS PAR L'APPLICATION WEHE



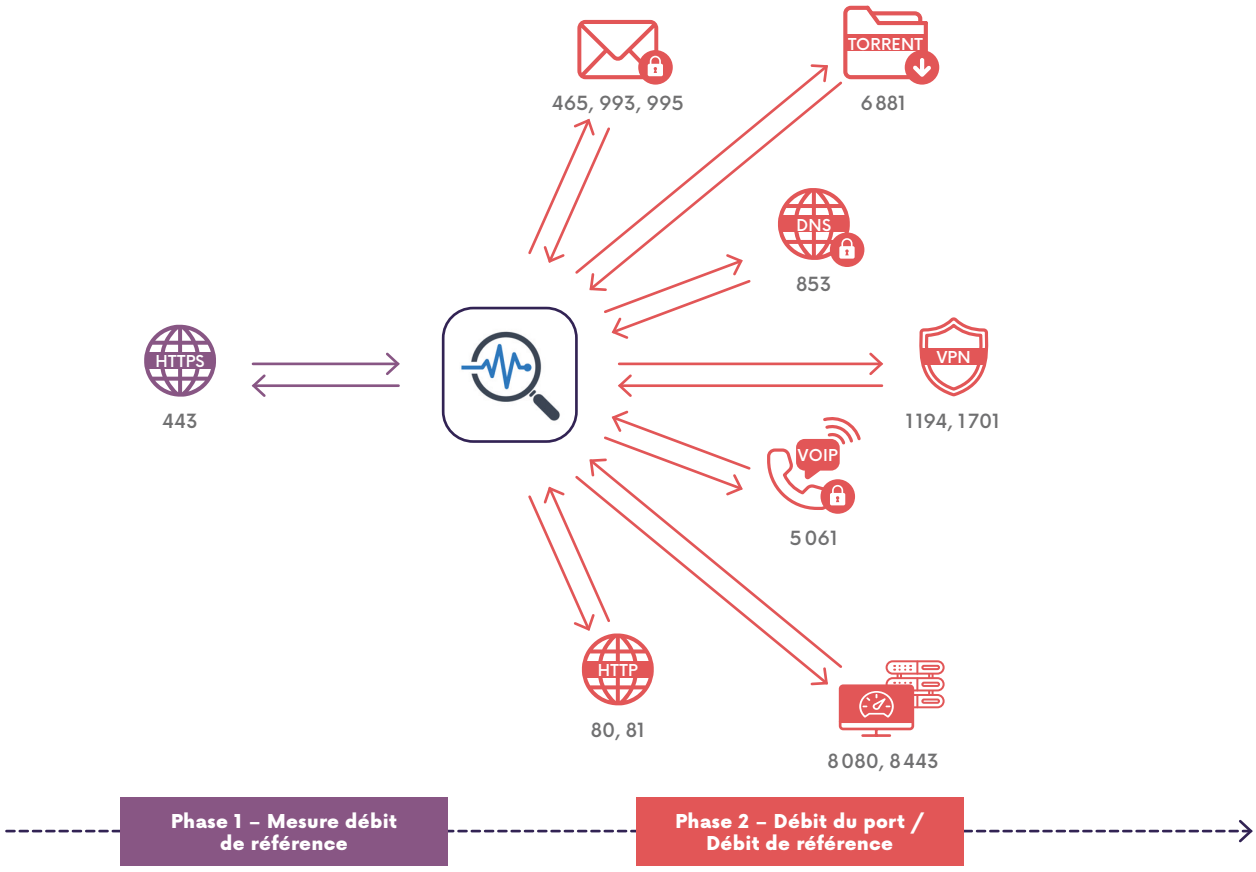
Source : Arcep

Depuis 2018, l'Arcep met à la disposition du grand public un outil de détection dénommé Wehe. L'outil est disponible gratuitement en français sous Android, iOS et dernièrement sous F-Droid. Développé en partenariat avec la *Northeastern University* de Boston et fondé sur un code en *open source*, Wehe analyse le trafic généré par l'application pour déterminer si l'opérateur est susceptible de brider ou de prioriser certains flux ou certains ports logiciels. L'Arcep a finalisé les travaux de mise à jour de l'application Wehe, dont la nouvelle version a été lancée fin décembre 2020. Plusieurs améliorations ont été apportées au test de différenciation : une mise à jour de la liste des services testés afin de correspondre aux services les plus communs en France, l'introduction de catégories de tests afin de faciliter la sélection des services testés par les utilisateurs et enfin une amélioration de la présentation des résultats de tests aux utilisateurs.

L'Arcep a également souhaité mettre à disposition des utilisateurs un test de détection d'éventuels blocages, bridages ou priorisations de ports logiciels, qui pourraient affecter les modalités d'accès à certains services par l'utilisateur final. En effet, l'accès à certains services ou applications en ligne s'effectue au moyen d'un port logiciel spécifique dont un éventuel blocage, bridage ou priorisation pourrait affecter les modalités d'accès au dit service par l'utilisateur final. Techniquement, le test de port compare le trafic https pour chacun des ports sélectionnés par l'utilisateur en le rapportant au trafic sur le port 443, défini comme port de référence.

En cas de dissemblance avérée dans les différents tests réalisés par Wehe, les utilisateurs sont invités à relayer leurs difficultés directement *via* la plateforme « J'alerte l'Arcep », afin que l'Autorité puisse examiner au cas par cas les incompatibilités potentielles avec le règlement internet ouvert.

SCHÉMA DE FONCTIONNEMENT DU TEST DE PORTS



Source : Arcep

La parole à



DAVID CHOFFNES

*Professeur associé – **Northeastern University de Boston***

LE LANCEMENT D'UNE NOUVELLE VERSION DE WEHE EN 2020

L'application Wehe, qui permet aux utilisateurs d'effectuer des tests depuis leurs appareils mobiles pour identifier de possibles violations à la neutralité du net, a connu un nombre important d'améliorations majeures l'année passée dans le cadre de notre collaboration avec l'Arcep. Les évolutions les plus notables concernent l'étendue des violations à la neutralité du net testées et la manière dont nous les testons.

Concernant l'étendue de ce que nous testons, nous avons inclus de nouvelles applications (dont des applications de visioconférence, compte tenu de leur popularité pendant la pandémie) ainsi que les applications les plus populaires en France. Les tests réalisés permettent de vérifier si un fournisseur d'accès à internet offre ou non à certaines applications de meilleures performances d'après les données échangées entre ces applications et les serveurs.

Nous avons également développé un nouveau test – ce test mesure les variations de performances sur les ports utilisés par certaines applications (par exemple, le port 80 pour HTTP, le port 443 pour HTTPS) –. Ces tests de ports nous ont obligés à relever de nouveaux défis, car contrairement aux tests basés sur le contenu, il n'est pas évident de définir les ports de référence sur lesquels le trafic resterait inchangé par un fournisseur d'accès à internet. Pour résoudre ce problème, nous avons utilisé le trafic du port 443 (HTTPS) comme port de référence. Ce dernier peut être priorisé ou dépriorisé par rapport à un autre trafic et Wehe montre simplement aux utilisateurs les performances du trafic pour chaque port, rapportées aux performances du port 443. Nous avons rencontré un autre défi inattendu avec le fait que certains fournisseurs d'accès à internet bloquent le trafic (par exemple, l'envoi de trafic HTTPS sur des ports autres que le port 443), vraisemblablement pour des raisons de sécurité. Nous avons adapté nos tests pour tenir compte de cette situation. Nous avons rencontré d'autres défis, tels que la définition de la quantité de données utilisées au cours du test ou encore la définition des seuils de détection pour identifier une violation à la neutralité du net. Grâce à une étroite collaboration avec l'Arcep et à l'accès à des serveurs en France, nous avons finalement pu résoudre ces problèmes.

Au cours de l'année passée, notre équipe a également réalisé le déploiement de Wehe au sein de Measurement Lab (M-Lab), qui offre l'accès à des centaines de serveurs à travers le monde. Ce déploiement a également soulevé de nouveaux défis, tels que le changement des applications et du logiciel serveur de Wehe afin de les rendre compatibles avec ce nouvel environnement, la protection de la vie privée des utilisateurs afin de garantir une collecte minimale de données depuis la plate-forme M-Lab et la configuration de ces nouveaux serveurs afin qu'ils puissent supporter de nombreuses utilisations simultanées. Plusieurs obstacles ont été rencontrés, mais le déploiement de Wehe sur M-Lab a finalement été un succès. Nous utilisons également toujours des serveurs en dehors de M-Lab, afin de nous assurer que les tests réalisés ne sont pas biaisés par une différenciation de traitement des serveurs *cloud* exécutant notre logiciel serveur.

Notre équipe a également amélioré la fiabilité et la facilité d'utilisation de notre application sous Android et sous iOS. Ce travail a conduit à la correction de différents bugs et échecs de fonctionnement, au perfectionnement des traductions et à la fourniture d'un compte rendu détaillé pour chaque test réalisé par un utilisateur. Nous avons également ajouté un lien pour alerter l'Arcep en cas de différenciation observée pouvant laisser supposer une violation à la neutralité du net. Nous continuons notre travail sur l'amélioration de la fiabilité et de l'intelligibilité de notre application, et nous remercions nos utilisateurs et l'Arcep pour leur patience et leurs contributions à améliorer le fonctionnement de l'application.

Rétrospectivement, les utilisateurs de Wehe ont collectivement exécuté près de 2 millions de tests relatifs à la neutralité du net depuis 2018, fournissant aux décideurs politiques, aux régulateurs et aux citoyens le moyen de comprendre les pratiques de différenciation mises en œuvre. À l'avenir, nous prévoyons d'aider les parties prenantes dans leur compréhension des réglementations locales, de continuer à rendre nos données et nos analyses publiquement accessibles pour aider à la préservation de la neutralité du net, et de travailler avec toutes les parties prenantes afin de soutenir un internet libre et ouvert, source d'innovations et d'équité, et ayant un impact positif considérable sur le monde.

4 État des lieux des pratiques observées

En 2019, la formation compétente de l'Autorité s'est penchée sur la conformité de l'ensemble des offres internet proposées en outre-mer au principe de neutralité du net. En 2020, l'Arcep s'est donc rapprochée de l'ensemble des opérateurs ultramarins afin de dresser un état des lieux sur cette question. Plusieurs échanges avec les opérateurs ont été menés durant l'année, en particulier sur les conditions générales d'utilisation de certaines offres d'accès à internet mobile. Au final, la majorité des points relevés n'étaient pas mis en œuvre techniquement d'après les opérateurs concernés. Ces clauses ont donc été rectifiées suite aux échanges avec les services de l'Autorité. Toutefois, un dialogue proactif avec les services de l'Autorité est toujours en cours avec deux opérateurs, dont l'un est actuellement en train de faire évoluer ses offres vers des pratiques plus respectueuses du règlement internet ouvert.

L'Autorité reste également attentive aux différents signalements reçus sur de possibles pratiques contraires à la neutralité du net, remontés notamment sur la plateforme « J'alerte l'Arcep ». Ces alertes ont conduit l'Autorité à examiner la question du blocage de certains ports logiciels. L'accès à un service ou à une application en ligne s'effectuant au moyen d'un port logiciel, le blocage empêche de fait l'accès au service. L'Autorité s'est donc fait l'écho des difficultés rencontrées par les utilisateurs auprès de deux opérateurs concernés, dont l'un a déjà modifié les mécanismes en place et l'autre examine les solutions possibles afin de maintenir un traitement égal du trafic sur les ports visés.

En 2019, l'Autorité s'est également intéressée à l'offre de Wi-Fi dans les trains. Proposée aux passagers, cette offre d'accès à internet, également considérée comme publiquement accessible, est soumise aux dispositions du règlement internet ouvert. Dans le cadre de ce dialogue avec la SNCF, les services de l'Arcep poursuivent l'examen de l'offre à bord des trains (échanges techniques, réalisations de tests, etc.). Les services de l'Arcep poursuivent ainsi le travail entamé et comptent sur la mobilisation de la SNCF pour s'assurer du respect du principe de neutralité du net.

Enfin, l'Autorité a initié une démarche de mise à jour de ses connaissances sur le fonctionnement des services de vidéo à la demande. L'objectif de cette démarche est de mieux cerner le fonctionnement et les contraintes techniques auxquelles sont soumis les services de vidéo à la demande et le cas échéant de pouvoir, dans un second temps, analyser les pratiques des opérateurs à la lueur des évolutions technologiques de la VoD[8]. Les services de l'Arcep vont donc se rapprocher de l'ensemble des acteurs contribuant au fonctionnement de la vidéo à la demande en France, à savoir les opérateurs télécoms, les fournisseurs de contenu vidéo à la demande, les hébergeurs proposant des solutions adaptées au stockage de contenu vidéo, les fournisseurs de contenu vidéo linéaire et en différé. L'Arcep invite également les parties prenantes intéressées au sujet à entrer dans un dialogue avec les services de l'Autorité.

8. Voir lexique.

La parole à



THOMAS SCHREIBER

*Membre de l'équipe en charge de la neutralité du net - **RTR**[1]*

LA FOURNITURE D'APPLICATIONS ET DE SERVICES : LE RÉGULATEUR AUTRICHIEN IMPOSE LE DROIT À UNE ADRESSE IPv4 PUBLIQUE

Le règlement européen internet ouvert – règlement (UE) n°2120/2015 – conçoit un internet véritablement ouvert : un internet auquel ne participent pas seulement quelques fournisseurs de contenu et de nombreux consommateurs de contenu, mais plutôt un internet avec des barrières d'accès très limitées et où chaque utilisateur final peut être à la fois créateur et consommateur de contenu.

Cette vision est consacrée à l'art. 3, paragraphe 1, du règlement internet ouvert, qui accorde aux utilisateurs finaux non seulement le droit d'accéder aux informations et au contenu de leur choix, mais également le droit de fournir des applications et des services auxquels d'autres personnes peuvent accéder. Ces services vont des appareils ménagers intelligents à usage personnel (par exemple, la surveillance de la température), au partage de fichiers avec le stockage en réseau (NAS), en passant par l'exploitation de serveurs web par des utilisateurs finaux pour des tiers.

Une condition préalable essentielle à l'auto-hébergement de services est l'accessibilité directe du service par l'utilisateur final à partir d'un internet public. En termes techniques, l'utilisateur final doit se voir attribuer une adresse IP publique qui permet d'identifier les serveurs hébergeant son service. Par analogie avec les réseaux téléphoniques, cela serait comparable à la condition première de disposer d'un numéro de téléphone pour qu'un utilisateur final puisse être joint par d'autres.

Alors qu'une adresse IP publique était auparavant attribuée par défaut, aujourd'hui, notamment sur les réseaux mobiles, les utilisateurs finaux se voient fréquemment attribuer des adresses IP privées (par l'utilisation de la technologie appelée *Network Address Translation* [NAT]). Exception faite des enjeux techniques, les raisons de cette pratique incluent notamment l'intérêt des FAI à conserver ces adresses IP publiques, car – avec IPv4 – celles-ci se raréfient. Cependant, si plusieurs clients sont tenus de partager une seule adresse IP privée *via* un NAT, cette pratique les prive de pouvoir fournir individuellement des services ou des contenus. Alors que certaines technologies, en particulier IPv6, pourraient résoudre certains des problèmes rencontrés, comme par exemple permettre aux utilisateurs finaux d'accéder à leurs propres appareils *via* des adresses IPv6, la fourniture uniquement d'une adresse IPv6 publique n'est pas – pour le moment – considérée comme une solution suffisante, car une grande partie d'internet ne possède pas encore de connectivité en IPv6. En revanche, la quasi-totalité de l'internet actuel permet une connectivité en IPv4.

En raison de ces éléments, l'Autorité de régulation autrichienne interprète l'art. 3, paragraphe 1 du règlement internet ouvert, comme donnant droit aux utilisateurs finaux à une adresse IPv4 publique, au moins dynamique, gratuite, dès lors que l'utilisateur final en fait la demande lorsqu'il souhaite par exemple offrir des services. L'utilisateur final peut ensuite utiliser cette adresse avec des services DNS dynamiques pour permettre le routage vers ses propres services. En conséquence, tout accord obligeant la perception d'une redevance supplémentaire à la mise à disposition d'une adresse IPv4 publique représente une restriction aux droits des utilisateurs finaux. Afin d'assurer des connexions *a minima* stables, les FAI se voient aussi interdire la possibilité de déconnecter les utilisateurs finaux quotidiennement, et ne sont autorisés à réaliser que de courtes déconnexions au plus une fois tous les 30 jours.

Une procédure de sanction contre l'opérateur historique autrichien concernant un service proposant une adresse IPv4 publique, uniquement sur demande et moyennant un coût supplémentaire, a été engagée en 2016. Une décision formelle a été prise fin 2017, interdisant à ce FAI de facturer des frais supplémentaires pour une adresse IPv4 publique dynamique et l'obligeant à rembourser une partie des frais déjà facturés. Dans la même décision, le FAI a également été autorisé à déconnecter les utilisateurs finaux au plus une fois tous les 30 jours. Alors que le FAI a fait appel de la décision, sa demande d'effet suspensif a été refusée par le tribunal administratif, permettant ainsi la mise en application de la décision dès 2018. À la mi-2020, le tribunal administratif (BVwG) a finalement rejeté le recours du FAI et a confirmé la décision de l'Autorité de régulation autrichienne. Toutefois, la décision n'est pas encore définitive.

Depuis 2018, l'Autorité de régulation autrichienne fait respecter le droit d'accès à une adresse IPv4 publique, au moins dynamique, auprès de tous les FAI autrichiens, quelle que soit leur taille. Étant donné que seuls certains utilisateurs finaux demandent une telle adresse IPv4 publique, la mise en œuvre de cette obligation, d'après notre expérience, était également possible pour les « nouveaux entrants » après des discussions informelles et n'a pas conduit à ce jour à de nouveaux recours formels.

De plus amples informations sur ce sujet et sur d'autres sujets concernant la neutralité du net en Autriche sont accessibles sur le site web de RTR à l'adresse : https://www.rtr.at/nn.

1. Autorité de régulation autrichienne de la radiodiffusion et des télécommunications.

CHAPITRE 5

PLATEFORMES, MAILLONS STRUCTURANTS DE L'ACCÈS À INTERNET

À retenir

L'année 2020 a marqué une évolution des débats : la question n'est plus de savoir si les grands acteurs du numérique posent des problèmes mais comment les résoudre.

À travers le monde, plusieurs propositions ont été faites pour mettre en place une régulation économique *ex ante* des grands acteurs du numérique. En Europe, la Commission européenne a publié le *Digital Markets Act* le **15 décembre 2020.**

La proposition de la Commission est une avancée majeure mais mérite d'être renforcée sur plusieurs aspects, en particulier l'ajout d'outils plus proactifs pour le régulateur.

Le règlement européen sur l'internet ouvert accorde des droits aux utilisateurs, tels que le droit d'accéder et de diffuser des informations et contenus en ligne. Mais il ne s'impose qu'aux fournisseurs d'accès à internet. Situés à une extrémité de la chaîne d'accès à internet, les terminaux (smartphones, assistants vocaux, les voitures connectées, etc.) et les écosystèmes fermés des plateformes dites structurantes se révèlent être des maillons faibles de l'ouverture d'internet.

L'Arcep a établi ce constat pour les terminaux dans son rapport[1] de 2018. La note publiée en décembre 2019[2] a prolongé cette étude aux opérateurs de plateformes numériques structurantes et a marqué l'élargissement de l'analyse par l'Autorité. La note a rappelé le constat qu'un nombre restreint d'acteurs sont devenus incontournables dans la vie numérique des citoyens et des entreprises en concentrant de nombreux services qui font partie intégrante du quotidien de chacun d'entre nous. Ces acteurs sont aujourd'hui en mesure de déterminer quels contenus et services peuvent être mis en ligne et à quelles conditions les utilisateurs peuvent y accéder. Concentrant de nombreux services, ils s'organisent en écosystèmes fermés au sein desquels les utilisateurs sont maintenus captifs, bridant leur liberté de choix. C'est en ce sens que ces écosystèmes se révèlent être des maillons faibles de l'ouverture d'internet.

L'année 2019 avait été marquée par la montée des enjeux de régulation de ces écosystèmes. L'année 2020 a vu une véritable bascule dans les débats, où la question n'est plus de savoir si ces acteurs posent des problèmes mais comment les résoudre. La Commission estime en particulier que le cadre juridique actuel ne lui permettrait pas de le faire : l'application par la Commission du droit de la concurrence européen (articles 101 et 102 du Traité sur le fonctionnement de l'Union européenne (TFUE)) demande des procédures particulièrement longues, et de tels délais peuvent être l'occasion pour les acteurs en cause de verrouiller leur position de marché d'une façon *irréversible*[3]. De plus, l'intervention ne peut avoir lieu qu'*ex post*, c'est-à-dire après la matérialisation d'une défaillance de marché. Comme l'indique un récent rapport de la Cour des comptes européenne[4] (CCE), *« en particulier dans l'économie numérique, il peut alors être trop tard pour s'attaquer à un problème de concurrence »*. Le rapport de la CCE souligne également que *« la Commission ne dispose actuellement d'aucun outil lui permettant d'intervenir* ex ante*, c'est-à-dire avant l'apparition de problèmes de concurrence »*. La Commission européenne s'est donc emparée du sujet de la régulation des plateformes en effectuant deux consultations publiques qui ont débouché sur deux propositions de règlement le 15 décembre 2020. Au travers du *Digital Services Act*, la commission propose de réviser la directive

1. https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018.pdf
2. https://www.arcep.fr/uploads/tx_gspublication/plateformes-numeriques-structurantes-caracterisation_reflexion_dec2019.pdf
3. Dans sont étude d'impact, la Commission indique ainsi : *"Moreover, – even when using interim measures (…) – competition law enforcement requires a detailed economic and legal analysis which, jointly with the procedural safeguards, bring the duration of the investigations to at least around two years and usually more than that. In markets characterised by powerful network effects and economies of scope, competition law interventions may mean not only delays in the interventions but also that irreparable effects such as tipping may no longer be reversible"*.
4. European Court of Auditors, Special Report 24/2020: EU audit report: merger control and antitrust proceedings, 19 November 2020, paragraphe 59.

Commerce électronique de 2000, notamment le régime de responsabilité à l'égard des contenus hébergés appliqué aux intermédiaires techniques. Cette proposition vise de façon plus large à garantir les meilleures conditions pour la fourniture de services numériques innovants dans le marché intérieur, à contribuer à la sécurité en ligne et à la protection des droits fondamentaux. Au travers du *Digital Markets Act* (voir encadré ci-contre), la Commission entend mettre en place une régulation économique *ex ante* des grands acteurs du numérique appelés « *gatekeepers* »[5].

1 Les développements observés sur le marché

L'année 2020 a été riche en actualités sur ces thématiques. De nombreuses plaintes contre les grands acteurs du numérique ont également été portées devant les autorités. La division antitrust du *Department of Justice* américain, suivie par une coalition d'États, a intenté un procès à Google en octobre 2020, alléguant un abus de position dominante sur le marché des services de recherche, notamment *via* des accords estimés anticoncurrentiels passés avec les fabricants d'appareils mobiles et les opérateurs de téléphonie mobile.

Après les trois sanctions contre Google entre 2017 et 2019, la Commission européenne a également ouvert d'autres enquêtes :

- sur les pratiques de Facebook et de Google en matière de collecte de données,
- sur la politique d'Apple en matière de magasins d'applications,
- sur les pratiques d'Apple concernant son portefeuille mobile : Apple Pay et les conditions d'accès à la puce NFC,
- et sur les conditions d'accès à la Buy Box[6] d'Amazon pour les vendeurs tiers de la marketplace.

Plusieurs enquêtes similaires sont en cours en Australie et au Royaume-Uni ainsi qu'au niveau national de certains pays européens (Allemagne, Italie, France).

Un front commun de développeurs[7] appelé « *Coalition for App Fairness* »[8] s'est récemment formé pour défendre leurs revendications face à Apple. Ils mettent en avant trois principales pratiques d'Apple qu'ils jugent problématiques : la commission de 30 % sur les achats *via* l'App Store, la limitation de liberté de choix de l'utilisateur et le fait de favoriser ses propres produits et fonctionnalités à disposition des utilisateurs.

Enfin, il a pu être observé une illustration des effets de verrouillage des utilisateurs liés aux effets de réseau lorsque les utilisateurs ont tenté de migrer vers Signal ou Telegram suite à un changement de conditions d'utilisation[9] de WhatsApp. De nombreux utilisateurs se sont ainsi plaints d'être contraints à garder un compte WhatsApp pour pouvoir continuer à communiquer avec certains de leurs contacts, ou de ne pas pouvoir récupérer leur historique de conversation, notamment par manque d'interopérabilité entre les messageries.

Le *Digital Markets Act*

Le 15 décembre 2020, la Commission européenne a publié une proposition de Règlement dit *Digital Markets Act* (DMA) qui entend mettre en place une régulation économique des grands acteurs du numérique. Le DMA a pour objectifs affichés de rendre les marchés numériques ouverts et équitables ainsi que d'harmoniser le cadre légal au niveau européen.

La proposition vise à désigner des entreprises qualifiées de contrôleur d'accès (ou *gatekeepers*) et liste les obligations qui s'appliquent à ces acteurs. À ces *gatekeepers*, la Commission estime désormais indispensable d'appliquer une réglementation *ex ante* asymétrique, selon des mécanismes qu'elle cherche à rendre les plus « automatiques » et opérants possibles, tout en comprenant des possibilités d'évolution. Ces mécanismes sont principalement constitués de deux types d'obligations et de pratiques prohibées qui doivent être respectées par les *gatekeepers* : une liste ne requérant aucune spécification (par exemple interdiction de lier les inscriptions à plusieurs services), et une liste dont les conditions de mise en œuvre peuvent être spécifiées par la Commission si celles proposées par le *gatekeeper* ne sont pas satisfaisantes (par exemple obligation de fournir une portabilité des données).

Cette avancée fait largement écho aux recommandations formulées par l'Arcep depuis 2018, en particulier en ce qu'elle cible les plateformes les plus structurantes, y compris les systèmes d'exploitation, services pour lesquels de nombreuses limitations à la liberté de choix des utilisateurs ont été mis en évidence[1]. Cependant, la proposition de la Commission mérite d'être renforcée sur plusieurs aspects (voir la section dédiée à la fin de la partie).

1. Rapport de l'Arcep, « Smartphones, tablettes, assistants vocaux : les terminaux, maillon faible de l'internet ouvert » (Février 2018).

5. Cette dénomination est largement similaire au concept d'opérateur de plateformes numériques structurantes de l'Autorité.
6. Ou « boîte d'achat », il s'agit d'une fonctionnalité marquée par un bouton visible pour certains produits Amazon qui permet à l'utilisateur d'acheter rapidement les produits qu'il recherche. Cette fonctionnalité n'est active que pour certains vendeurs sous certaines conditions. Pour les vendeurs, la présence de ce bouton sur leurs produits est essentielle à la réussite des ventes.
7. Spotify, Epic, ou encore Tile qui s'étaient déjà publiquement exprimés contre les pratiques d'Apple, sont membres de cette coalition.
8. https://appfairness.org/
9. https://9to5mac.com/2021/01/06/whatsapp-share-your-data-with-facebook/

2 Avancée des travaux de l'Autorité

L'Arcep a poursuivi ses travaux de veille et de communication en partenariat avec une diversité d'acteurs tout au long de l'année 2020. L'Autorité a mis à jour sa plateforme de signalement « J'alerte l'Arcep » en novembre en s'ouvrant à de nouveaux publics que sont les développeurs d'applications et à de nouvelles thématiques comme l'ouverture des terminaux. Les développeurs d'applications peuvent désormais utiliser une entrée dédiée sur « J'alerte l'Arcep », au même titre que les collectivités, les entreprises ou les particuliers. Ils sont en mesure de signaler à l'Arcep les problèmes relatifs aux outils ou services qu'ils rencontrent avec les fabricants de terminaux, les systèmes d'exploitation (OS), les moteurs de recherche ou encore les magasins d'applications. *Via* ces signalements, l'Arcep entend renforcer sa connaissance de cet écosystème, en s'appuyant sur l'expérience des développeurs. Leurs alertes peuvent porter sur plusieurs cas concrets, par exemple :

- « Les API que j'utilise changent régulièrement sans raison apparente » ;
- « Le magasin refuse mon application » ;
- « Le système d'exploitation ne m'informe pas ou pas assez ou pas en avance des mises à jour ».

Ces cas concrets ne sont bien entendu que des catégories fournies par l'Arcep pour faciliter le traitement des alertes. Les développeurs d'applications sont libres d'alerter l'Arcep sur tout autre type de problématique.

L'Autorité a aussi contribué[10] à la consultation publique de la Commission européenne sur le *Digital Services Act*[11]. L'Autorité a appelé l'Union européenne à se doter d'une régulation *ex ante* des plateformes structurantes et à faire à nouveau d'internet un espace de libre choix et de libre innovation. Cette contribution s'est accompagnée d'une note sur les remèdes qui pourraient être utilisés pour la régulation de ces plateformes. Cette « boîte à outils » s'inspire de la démarche mise en œuvre avec succès depuis plusieurs décennies dans le secteur des télécoms, notamment grâce aux mécanismes de remédiation sur mesure et de règlement des différends.

3 Avancée des travaux en France

En France, les autorités françaises ont mis en place en septembre le Pôle d'expertise de la régulation numérique (PEReN) qui apporte son évaluation et son assistance technique aux services de l'État et aux autorités administratives qui interviennent dans la régulation des plateformes numériques. Ce service à compétence nationale regroupera, à ces fins, une vingtaine de *data scientists* et experts en informatique et algorithmique. L'Autorité et le PEReN se rencontrent régulièrement et ont identifié plusieurs pistes d'études pour 2021. La task-force mise en place en mars 2020[12], dont l'Arcep fait partie, continue de poursuivre ses travaux d'élaboration des positions françaises. Cette task-force interministérielle[13] fournit des travaux de réflexion afin d'élaborer des argumentaires sur l'opportunité et la manière de réguler les plateformes numériques.

4 Avancée des travaux en Europe

En Europe, plusieurs propositions législatives ont vu le jour, en parallèle de celle de la Commission.

Le Royaume-Uni a annoncé[14] en décembre la mise en place d'un nouveau cadre de régulation pour certains acteurs du numérique. Une équipe dédiée est mise en place au sein de l'autorité de la concurrence anglaise. Cette unité a pour objectifs de (i) défendre les intérêts des consommateurs et des citoyens, (ii) être un centre d'expertise pour les marchés numériques, (iii) superviser les entreprises ayant un « statut stratégique sur le marché »[15]. En plus du mécanisme de désignation de ces entreprises, le cadre de régulation serait composé de trois piliers :

- Des codes de conduite : un ensemble de principes clairs visant à garantir la loyauté vis-à-vis des consommateurs et des entreprises ainsi qu'à protéger les concurrents des pratiques susceptibles de porter atteinte à une concurrence loyale. Ces codes de conduite ont pour objectif de prévenir et réduire les effets indésirables causés par le pouvoir de marché.
- Des interventions pro-concurrentielles comme la portabilité des données personnelles, l'interopérabilité, l'accès à des données qui peuvent amener plus de concurrence et d'innovation. Ces interventions visent à instaurer des changements de long terme en modifiant l'organisation du marché pour accroître structurellement sa contestabilité.
- Des règles spécifiques pour les opérations de concentration des entreprises avec SMS, afin de permettre un contrôle plus étroit des transactions.

10. https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/regulation-du-numerique-1.html
11. Le *Digital Services Act* a été finalement découpé en 2 textes différents par la Commission européenne. La partie à laquelle l'Arcep a contribué est maintenant incluse dans le *Digital Markets Act*.
12. https://www.entreprises.gouv.fr/fr/actualites/numerique/politique-numerique/la-regulation-des-plateformes-numeriques
13. https://www.youtube.com/watch?v=XwvmLTf7m_w
14. https://www.gov.uk/government/news/cma-advises-government-on-new-regulatory-regime-for-tech-giants
15. Cette dénomination rejoint largement la notion de « *gatekeepers* » de la Commission européenne et d'opérateurs de plateformes numériques structurantes pour l'Autorité.

Début 2021, l'Allemagne a également voté une loi permettant à l'autorité de la concurrence allemande, le *Bundeskartellamt*, de désigner une liste d'entreprises considérées comme *« d'une importance capitale pour la concurrence sur les marchés »*. Ces entreprises devront respecter un ensemble de règles, notamment l'interdiction d'accorder un traitement préférentiel à leurs propres services ou d'entraver l'interopérabilité avec d'autres services.

Le BEREC a également publié son avis[16] sur le *Digital Markets Act* en mars 2021 ; l'Arcep a activement participé à ces travaux. Le BEREC supporte fortement l'initiative de la Commission européenne de mettre en place une régulation asymétrique *ex ante*. Cependant, le BEREC estime que la proposition est trop tournée vers le passé en se contentant de se fonder sur une collection de décisions des autorités de concurrence et propose de mettre en place un cadre plus souple en :

- complétant les obligations directement applicables d'un dispositif de remédiation sur mesure prenant en compte les spécificités de chaque acteur ;
- renforçant la coopération avec les autorités nationales indépendantes pour la supervision, la mise en pratique du DMA, et la réduction des fortes asymétries d'information.

Ces réflexions autour de la proposition de la Commission européenne se sont aussi faites au sein du *Center on Regulation in Europe* (CERRE). En novembre 2020, le CERRE a présenté une compilation de l'ensemble de ses travaux sur la régulation du numérique[17]. L'institution a accueilli chaleureusement la proposition de la Commission européenne et poursuit ses travaux pour faire des propositions concrètes d'amélioration notamment pour la mise en œuvre du texte. Le CERRE estime en effet que la régulation proposée devrait être plus flexible et dynamique en permettant par exemple d'individualiser certains remèdes. L'institution propose aussi d'intégrer l'ensemble des parties prenantes dans les processus d'élaboration et de supervision des remèdes, notamment les tiers qui sont censés en bénéficier.

5 Avancée des travaux aux États-Unis

Aux États-Unis, un rapport[18] de l'*Antitrust Subcommittee* de la Chambre des représentants a marqué une nouvelle étape dans le débat sur la modernisation de la politique de la concurrence (antitrust) et un changement progressif de doctrine à l'égard des *Big Tech*. Alors que les États-Unis avaient jusque-là adopté une politique de « laisser-faire », la multiplication des procédures antitrust[19] constitue une offensive inédite à l'encontre des grandes entreprises du secteur numérique qui pourrait aller jusqu'à des séparations, au moins fonctionnelles, de certaines activités.

16. https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/9879-berec-opinion-on-the-european-commissions-proposal-for-a-digital-markets-act
17. https://cerre.eu/events/new-perspectives-on-digital-regulation-and-competition-policy/
18. https://www.reuters.com/article/us-usa-tech-antitrust-idUSKBN26R2V6
19. Google, Apple et Facebook sont notamment visés par des procédures en cours.

RENFORCER LE DMA POUR UN NUMÉRIQUE OUVERT AU SERVICE DES CITOYENS ET ENTREPRISES EN EUROPE

L'Arcep salue la proposition de Règlement « *Digital Markets Act* » portant sur les acteurs structurants de l'internet et invite à le compléter par des propositions visant à renforcer son efficacité, et mieux atteindre l'objectif d'ouverture du numérique au bénéfice des citoyens et entreprises en Europe.

L'internet s'est développé comme un bien commun. Il a été construit comme un réseau ouvert pour tous, sans qu'aucune institution, publique ou privée, ne limite son évolution. Cela a notamment permis l'émergence de services numériques qui ont apporté de réels bénéfices au fonctionnement d'internet et à la société en général. Pour autant, il est désormais établi que certaines grandes plateformes, devenues structurantes pour l'internet (entre autres, certains moteurs de recherche, réseaux sociaux et systèmes d'exploitation) **sont des passerelles incontournables qui contrôlent et décident désormais si et comment les utilisateurs peuvent accéder et partager des contenus et des services en ligne.** Dans certaines conditions, même si elles continuent d'innover, elles peuvent freiner la concurrence et l'innovation de l'ensemble du secteur numérique, et conduire à porter atteinte à la liberté de choix et la liberté d'expression des utilisateurs. Ce possible impact négatif sur l'intérêt des citoyens, et le bien-être des consommateurs ne peut plus être ignoré. Il est ainsi crucial de **s'assurer que les infrastructures numériques se développent en tant que biens communs et de préserver la dimension « générative »[1] originelle de l'internet, c'est-à-dire la capacité de tous les utilisateurs à contribuer sans contrainte à son enrichissement et son foisonnement.** Cette capacité est garantie, notamment, par l'architecture décentralisée de l'internet. Dans ce contexte, la proposition de Règlement **visant à assurer la contestabilité et l'équité des marchés numériques** (le « *Digital Markets Act* », DMA), publiée par la Commission le 15 décembre 2020, était attendue et marque la volonté d'une Europe du numérique fidèle à ses valeurs.

L'Arcep appelle depuis plusieurs années à la mise en place d'un cadre de régulation *ex ante*, agile et asymétrique. À ce titre, le DMA, qui cible **les contrôleurs d'accès (*Gatekeepers*) les plus structurants,** y compris les systèmes d'exploitation[2], constitue une avancée importante à saluer. Cependant, la proposition de la Commission ne sera efficace et ne remplira ses objectifs, en particulier **favoriser et libérer l'innovation,** que si elle est complétée sur plusieurs aspects afin de mieux prendre en compte toutes les dimensions des problèmes potentiels posés par ces acteurs, de pouvoir mieux cibler les réponses, et d'assurer leur effectivité réelle.

À ce titre, il conviendrait de doter le régulateur de nouveaux outils dynamiques qui lui permettraient de mieux anticiper les problèmes et de renforcer les moyens qui lui sont alloués pour une mise en œuvre efficiente de son intervention *ex ante*. Il s'agirait en particulier de renforcer le dispositif **de suivi de ces contrôleurs d'accès afin de réduire l'asymétrie d'information** et de prévoir, en complément des obligations fixées à l'avance et de manière générale, **des remèdes au cas par cas, plus adaptés qu'une solution « *one size fits all* »**. Ces éléments constituent des atouts de la régulation *ex ante* qui a fait ses preuves.

Aussi, une plus grande coopération entre la Commission et les États membres pourrait renforcer l'efficience du dispositif et apporterait des ressources et appuis déterminants.

Enfin, il apparaît nécessaire de mieux considérer la dimension écosystémique de certains acteurs qui peuvent être sources de défaillances de marché, en vue de l'amélioration des conditions concurrentielles, y compris entre les plateformes elles-mêmes. Cette approche permettrait de mieux prendre en compte et favoriser la liberté de choix des utilisateurs finaux, parfois captifs d'un écosystème centralisé, c'est-à-dire d'un ensemble de produits, services[3] ou de matériels numériques interagissant ensemble[4] et conduisant au verrouillage de ses utilisateurs.

01. Certains dispositifs et moyens d'action complémentaires, inspirés de vingt ans d'expérience d'ouverture du secteur des télécoms, rendraient le DMA plus efficace

Les moyens que se donne la Commission seront insuffisants pour garantir l'efficacité du cadre proposé. En effet, bien que la proposition intègre les solutions à nombre de problèmes identifiés à ce stade, elle place la Commission en situation de réaction par rapport aux *gatekeepers*, notamment dans la mesure où le DMA ne prévoit qu'une rectification *a posteriori* du défaut d'application du texte et des problèmes qui continueront d'être constatés : il revient aux *gatekeepers* de décider en premier lieu comment

1. Jonathan L. Zittrain, The Future of the Internet, And How to Stop It, Yale University Press & Penguin UK, 2008, page 70: *"Generativity is a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences"*.
2. Rapport de l'Arcep, « Smartphones, tablettes, assistants vocaux : les terminaux, maillon faible de l'internet ouvert » (Février 2018).
3. Par exemple applications, systèmes d'exploitation, plateformes numériques…
4. Définition inspirée de OCDE (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, Éditions OCDE, Paris, page 22, https://doi.org/10.1787/53e5f593-en

se mettre en conformité avec les obligations générales qui leur incombent. De plus, les acteurs dépendants ou concurrençant les plateformes n'ont aucun moyen de faire entendre leur voix s'ils rencontrent des difficultés dans leur relation avec ces *gatekeepers*.

Pour permettre au régulateur d'intervenir à temps et utilement et de s'adapter aux pratiques d'un secteur en constante évolution, **le DMA devrait être pourvu des outils, dispositifs et moyens d'action nécessaires à une mise en œuvre rapide et efficace de la régulation *ex ante* asymétrique qu'il esquisse** et à la réalisation des objectifs ciblés. La proposition n'offre en effet pas suffisamment de flexibilité et d'individualisation pour permettre au régulateur de prendre en compte les disparités de situations et de modèles d'affaires des différentes entreprises. Le texte tel que proposé ne permet pas non plus de faire face aux moyens des acteurs amenés à être régulés, que ce soit en termes de technicité des problèmes étudiés, de l'exploitation d'avantages informationnels (tirés des importantes asymétries d'information), ou de créativité pour tenter de s'affranchir des contraintes de la régulation. Dès lors, quelques outils complémentaires connus de la régulation *ex ante* peuvent être proposés.

- **Premièrement,** la proposition devrait prévoir, en complément des listes d'obligations établies aux articles 5 et 6, un **dispositif de remédiation sur-mesure** pour définir des remèdes spécifiques à chaque *gatekeeper* ou type de service à l'issue d'une analyse approfondie des effets des mesures envisagées, afin de traiter de façon proportionnée les cas non anticipés dans les deux listes d'obligations (par exemple par des obligations de non-discrimination, d'accès équitable ciblées voire de séparation sur certains services ou données). Le dispositif actuel est en effet rigide et contraint, donc potentiellement aisé à contourner en développant de nouvelles pratiques, en particulier pour certaines mesures à forte dimension technique comme la portabilité des données. Les remèdes sur-mesure permettent au régulateur, en prenant en compte les particularités de l'acteur concerné, de préciser directement la manière dont une obligation peut être appliquée, désincitant ainsi un potentiel contournement par le régulé et réduisant la nécessité d'interventions additionnelles et, *in fine*, de surrégulation.
- **Deuxièmement,** il semble indispensable d'instaurer et de maintenir **un dialogue incluant l'ensemble des parties prenantes,** et non les seuls *gatekeepers* comme actuellement proposé dans le texte. La consultation (formelle, selon la procédure, ou informelle pour un suivi régulier – cf. mécanisme de suivi ci-après)) des acteurs supposés bénéficier de l'imposition de ces obligations (les concurrents de ces plateformes, les utilisateurs professionnels et, dans certains cas consommateurs et société civile…) contribuera en effet à assurer l'élaboration de remèdes efficients, et à anticiper les problèmes émergents.
- **Troisièmement, un suivi (par un mécanisme de « *monitoring* »)** des évolutions de l'environnement numérique, en demandant par exemple à la Commission d'établir une liste d'indicateurs à collecter périodiquement auprès des acteurs, permettrait à la Commission de **gagner en expertise technico-économique et de réduire l'importante asymétrie d'information entre régulateur et régulés.** Ce suivi pourrait utilement alimenter un dispositif de régulation par la donnée qui, lui aussi, réduirait l'asymétrie d'information entre les plateformes et leurs utilisateurs et contribuerait à orienter le marché au bénéfice du plus grand nombre.
- **Quatrièmement,** la mise en place d'un mécanisme **de règlement des différends** pour compléter la boîte à outils du régulateur permettrait à un acteur qui ne parvient pas à trouver un accord avec un *gatekeeper*, ou qui se considère lésé par un *gatekeeper* dans la mise en place d'une des obligations, de saisir le régulateur pour trouver rapidement une solution opérationnelle. Il peut ainsi concerner une grande variété de problématiques (et notamment l'accès aux magasins d'applications comme le fonctionnement opérationnel de remèdes techniques tels que la portabilité) et préciser le cadre de régulation au regard de cas pratiques, hors de toute logique de sanction punitive.

Enfin, le cadre de régulation proposé ne pourra faire l'économie d'importants moyens humains et techniques. La Commission propose d'allouer 80 agents, ce qui semble très insuffisant. À titre de comparaison, les autorités du Royaume-Uni prévoient plus de 300 agents pour une initiative similaire au *Digital Markets Act*.

Ces propositions, inspirées des vingt ans d'expérience de régulation du secteur des communications électroniques, permettraient de renforcer la proposition actuelle. Si transposer simplement le cadre appliqué aux communications électroniques aux *gatekeepers* n'est pas approprié, le *Digital Market Act* gagnerait à puiser dans ce cadre les éléments ou principes qui lui confèrent sa flexibilité, son adaptativité et son efficacité par une intervention rapide, proportionnée et justifiée.

02. Le renforcement du mécanisme de coopération avec les États membres permettrait une plus grande proximité, notamment avec les petits acteurs professionnels, bénéficiaires des nouvelles dispositions

Certaines des dispositions renforçant l'efficacité de la mise en œuvre du règlement bénéficieraient d'une plus **forte coopération entre la Commission et les autorités nationales,** apportant ainsi un appui de l'échelon national. Actuellement, la coopération n'est prévue que par le seul mécanisme instituant la présence des États membres au sein d'un Comité rendant des avis consultatifs en amont de l'adoption d'actes d'exécution par la Commission. Cette procédure donne la possibilité aux États d'exercer un relatif contre-pouvoir institutionnel sur les actes d'exécution de la Commission. Toutefois, bien qu'elle permette certains échanges, son objet n'est pas d'instaurer un véritable mécanisme de coopération, encore moins de permettre des remontées d'informations de terrain.

Si les acteurs régulés ont une dimension internationale, les bénéficiaires des obligations seront en grande partie des petits acteurs professionnels ou utilisateurs actifs au niveau national. Il semble ainsi qu'un rôle pourrait être confié à cet échelon pour suivre l'évolution du secteur, contrôler l'efficacité des mesures mises en place, remonter des alertes, régler certains différends au niveau national et plus généralement servir d'interlocuteur aux petits acteurs, qui sont dans une position très asymétrique par rapport aux *gatekeepers*, et peuvent être réticents à se tourner directement vers la Commission.

Le DMA pourrait prévoir la création d'un groupe indépendant constitué d'Autorités Nationales Indépendantes qui conseillerait la Commission Européenne en lui apportant une expertise technique et une connaissance des situations, contribuant ainsi à une mise en œuvre efficace du règlement au bénéfice des entreprises, des consommateurs et de la société. Ce groupe pourrait coordonner les éventuelles activités des autorités au niveau national.

03. Le périmètre de la proposition est pertinent mais celle-ci ne vise pas suffisamment à ouvrir les écosystèmes au bénéfice des utilisateurs

Le choix de la Commission d'une approche asymétrique, qui focalise l'intervention sur les acteurs les plus structurants, dont les systèmes d'exploitation des terminaux, est opportun et mérite d'être salué et soutenu. Le champ d'application de la proposition apparait globalement pertinent, modulo certains services qui, posant des problèmes similaires, pourraient voir leur inclusion clarifiée, les navigateurs web et assistants vocaux en particulier.

Toutefois, si l'avancée est importante et le type d'acteurs visés correctement identifiés, l'ambition pourrait être plus large pour réellement rendre les marchés numériques contestables et équitables au bénéfice de tous. La proposition se concentre en effet en réalité essentiellement sur les rapports entre les *gatekeepers* et les utilisateurs professionnels qui dépendent de leurs services. Elle pourrait être complétée **en tenant mieux compte de la dimension écosystémique des acteurs visés afin de :**

- Promouvoir la concurrence entre les plateformes elles-mêmes

La proposition actuelle se focalise sur des dispositions visant à garantir que, lorsque des concurrents sont hébergés par une plateforme verticalement intégrée, le marché aval sera bien animé d'un jeu concurrentiel loyal. Bien que certaines obligations visent à réduire les barrières à l'entrée et traiter les effets de verrouillage (*lock-in*), la proposition gagnerait à comporter davantage de mesures visant à remettre en cause les écosystèmes centralisés qui se sont développés et se maintiennent grâce à de puissants effets d'économies d'échelles, effets de réseau et effets de leviers. Il s'agirait de limiter la dépendance des utilisateurs professionnels vis-à-vis des *gatekeepers* en permettant **l'émergence d'acteurs alternatifs.** Par exemple, si on peut se féliciter de la mise en place d'une obligation de portabilité de données susceptible de traiter une partie des problèmes liés aux effets de verrouillage, les obligations prévues ne remettent pas en cause l'extraction de la rente générée par la captation des bénéfices des effets de réseaux, qu'une **véritable interopérabilité « horizontale »**[5] permettrait, dans certaines circonstances, de résoudre.

- Garantir l'intérêt des utilisateurs finaux

La promotion de la concurrence s'exerce au bénéfice des consommateurs, mais la concurrence ne permet pas à elle seule d'assurer l'ensemble des intérêts des utilisateurs finaux. Les objectifs de liberté de choix des citoyens européens ou d'ouverture de l'internet[6] pourraient ainsi être mieux intégrés, élargissant les objectifs du Règlement au-delà de de la protection des intérêts des utilisateurs professionnels même s'ils sont, *indirectement*, au bénéfice des utilisateurs finaux. Certaines obligations bénéficiant *directement* aux utilisateurs finaux[7], notamment de transparence ou d'interopérabilité pourraient ainsi être ajoutées (de manière ciblée et proportionnée, cf. deuxième partie) et le périmètre des cas justifiant l'intervention du régulateur[8] pourrait être élargi. Par exemple, les services n'ayant pas ou peu de clients professionnels au sens de la proposition n'entrent pas dans la régulation prévue par règlement. Or, certains d'entre eux constituent indiscutablement des points de contrôle de l'accès et du partage des informations et contenus en ligne pour les utilisateurs finaux[9]. Enfin, une meilleure prise en compte de la dimension écosystémique de ces acteurs et de leur modèle d'affaire conduisant à maintenir les utilisateurs dans un environnement fermé, ainsi que de leurs effets, semble nécessaire, ce qui serait rendu possible par les propositions de renforcement abordées en deuxième partie.

La proposition de la Commission constitue une avancée majeure pour aller vers une plus grande ouverture des écosystèmes numériques dans l'Union européenne et au-delà. Pour la garantir plus largement et plus efficacement, l'Arcep invite les co-législateurs européens à renforcer cette proposition en lui donnant sa nécessaire flexibilité – meilleure proportionnalité, efficacité et rapidité des remèdes proposés, et adaptabilité face à la variété des situations à traiter, aujourd'hui et demain – et en valorisant un appui des États membres notamment, afin qu'elle intègre mieux les caractéristiques écosystémiques de certains acteurs et permette une plus grande liberté de choix des citoyens européens dans l'accès aux services numériques.

5. Capacité de systèmes concurrents, tels que des réseaux sociaux, à permettre la communication entre leurs utilisateurs finaux.
6. Au-delà de la couche réseau, déjà traitée par le règlement relatif à un internet ouvert.
7. En renforçant notamment leur capacité à « *multi-homer* », c'est-à-dire la capacité des utilisateurs à utiliser plusieurs plateformes concurrentes en même temps.
8. C'est-à-dire de mobiliser les obligations déjà identifiées au service d'objectifs complémentaires, notamment lorsque la Commission précise les conditions d'implémentation des obligations *via* le mécanisme prévu à l'article 7.
9. Par exemple les services de cloud et certains grands services de messageries instantanées dont la clientèle ne serait constituée essentiellement que d'utilisateurs non professionnels.

La parole à



IAN BROWN

Consultant indépendant

DES OBLIGATIONS D'INTEROPÉRABILITÉ POURRAIENT STIMULER LA CONCURRENCE DANS LES RÉSEAUX SOCIAUX ET LES MESSAGERIES INSTANTANÉES

L'interopérabilité et l'interconnexion sont des mesures de régulation bien connues dans le domaine des communications électroniques au sein de l'UE ; afin que les régulateurs nationaux puissent exiger des opérateurs qu'ils connectent leurs réseaux à ceux de leurs concurrents. Cela permet de garantir une concurrence fondée sur les mérites de leurs services plutôt que sur le poids des effets de réseau découlant de bases de clients importantes.

Dans sa récente proposition du *Digital Markets Act*, la Commission européenne a inclus des exigences similaires d'interopérabilité, mais limitées aux services complémentaires, pour les plus grandes plateformes dites *gatekeepers*, qui fournissent des services essentiels tels que les réseaux sociaux et les messageries instantanées. Cette décision fait suite aux recommandations de l'Arcep et d'autres régulateurs européens en faveur de tels pouvoirs, qui sont déjà inclus dans un récent amendement à la loi allemande sur la concurrence. Les petites et moyennes entreprises technologiques européennes ainsi que la société civile ont demandé que ces exigences soient élargies pour couvrir les services essentiels de ces *gatekeepers*.

Des réserves ont été soulevées quant aux effets sur l'innovation. Cependant, la concurrence est un moteur essentiel de l'innovation, et les réseaux sociaux et les messageries sont des services courants depuis maintenant deux décennies. À ce niveau de maturité, les économistes de la concurrence ont fait valoir que des obligations imposées aux plateformes dominantes pour rendre interopérables les fonctions standard du secteur *via* des API ouvertes ou des normes de communication peuvent maximiser le bien-être.

Les mécanismes permettant d'imposer des normes techniques sont un élément-clé de la législation européenne sur le marché intérieur et pourraient être étendus pour permettre aux régulateurs d'imposer la conformité aux normes déjà existantes et bien développées du *World Wide Web Consortium* et de l'*Internet Engineering Task Force*. La Commission européenne pourrait également fournir des fonds de R&D pour l'infrastructure et le développement de nouvelles technologies, ce qui était un mécanisme politique américain clé derrière le développement de l'ARPAnet/internet. Des protections spécifiques pour l'innovation pourraient également être incluses dans le *Digital Markets Act*, comme elles le sont dans le Code européen des communications électroniques.

La parole à



HENRI VERDIER

*Ambassadeur pour le numérique – **ministère de l'Europe et des Affaires étrangères***

L'INITIATIVE *OPEN TERMS ARCHIVE*

Les grandes entreprises du numérique établissent aujourd'hui des normes de fait, *via* leurs conditions générales d'utilisation (CGU). Leur compréhension est nécessaire :

- à chaque usager, pour qu'il puisse identifier ce qu'il a accepté, les données qu'il a partagées, les droits qu'il a cédés aux services et ceux qu'il a conservés ;
- aux autorités pour vérifier la compatibilité de ces cadres contractuels avec le droit national et supranational, notamment lorsque ces derniers évoluent ;
- aux régulateurs pour évaluer les efforts et la redevabilité des plateformes.

Afin d'outiller ces acteurs, l'équipe de l'Ambassadeur pour le numérique a lancé l'initiative ***Open Terms Archive***[1] **(OTA).** Il s'agit d'une solution libre et ouverte de suivi et d'archivage des évolutions des CGU des principaux fournisseurs de services en ligne, en :

- enregistrant en temps réel les mises à jour des documents ;
- affichant spécifiquement les changements appliqués aux documents ;
- disposant d'un corpus documentaire de leur historique.

OTA a vocation à s'enrichir et à devenir un « commun », contributif, sur lequel il sera possible de bâtir notamment des outils pour la recherche en droit comparé, alertes ciblées, analyses linguistiques. À titre de premier usage, a ainsi été codé **Scripta Manent,** un service qui, pour 367 contrats, permet de mesurer toutes les évolutions entre deux dates.

Le choix de développer des outils ouverts et collaboratifs, au service de la transparence, s'inscrit dans deux des lignes de force de la **diplomatie numérique française :** (i) incarner une **souveraineté numérique européenne** c'est-à-dire une réelle autonomie stratégique fondée sur une capacité d'action et de choix ; (ii) construire un **cadre de régulation du numérique fondé sur le dialogue multilatéral et multi-acteurs.**

1. On trouvera en ligne une présentation d'*Open Terms Archive*, de premiers exemples d'expérimentations, l'API, les jeux de données disponibles, ainsi qu'une documentation sur le fonctionnement et les modalités d'usage.

PARTIE 3

Agir face au défi environnemental du numérique

CHAPITRE 6
Encourager un numérique soutenable

CHAPITRE 6

ENCOURAGER UN **NUMÉRIQUE SOUTENABLE**

À retenir

2020 a été l'occasion pour l'Arcep de lancer sa plateforme « Pour un numérique soutenable » :

9 ateliers

127 participants

42 contributions écrites d'acteurs qui ont permis la publication du rapport « Pour un numérique soutenable » le 15 décembre 2020.

La feuille de route du Gouvernement sur le numérique et l'environnement publiée en février 2021 identifie plusieurs chantiers pour l'Arcep, comme la réalisation d'un baromètre environnemental, l'analyse des pratiques de distribution de terminaux et de leur effet sur le renouvellement des terminaux, l'amélioration, conjointement avec l'ADEME, de l'estimation de l'empreinte environnementale du numérique.

La proposition de loi visant à réduire l'empreinte environnementale du numérique en France ainsi que **le projet de loi** de lutte contre le dérèglement climatique et le renforcement de la résilience face à ses effets seront structurants dans la mise en œuvre des propositions identifiées dans les rapports publiés sur le sujet en 2020.

L'impact des réseaux de communications électroniques, des terminaux, des centres de données et des usages du numérique sur l'environnement est un sujet d'attention croissant dont se saisissent peu à peu un nombre grandissant de parties prenantes. La Convention citoyenne pour le climat[1] note d'ailleurs que si le numérique est un levier essentiel pour la transition écologique et la lutte contre le réchauffement climatique, ce dernier ne doit pas contribuer davantage à la hausse des émissions.

D'après diverses études réalisées ces deux dernières années[2], le numérique représenterait aujourd'hui 3 à 4 % des émissions de gaz à effet de serre[3] (GES) dans le monde et 2 % de l'empreinte au niveau national[4] (phase de production et phase d'utilisation comprises). Si ces études peuvent varier dans leurs évaluations précises, elles concordent toutes dans le diagnostic plus général qu'elles dressent.

Si cette part demeure plus faible que celles d'autres secteurs, la croissance annuelle de la consommation de numérique (volume de données, nombre de terminaux, etc.) doit interroger. En effet, selon le rapport de la mission d'information sur l'empreinte environnementale du numérique du Sénat, l'empreinte GES du numérique pourrait augmenter de manière significative si rien n'est fait pour la limiter (+60 % d'ici à 2040 soit 6,7 % de l'empreinte GES nationale). Si elle se matérialisait, une telle évolution apparaîtrait contraire aux engagements pris dans le cadre de l'Accord de Paris de 2015[5] qui vise à contenir le réchauffement de la planète à un niveau nettement inférieur à 2° C, et implique de la part de l'ensemble des secteurs économiques des efforts rapides et massifs pour la réduction de leur empreinte carbone.

1. La Convention citoyenne pour le climat (CCC) a été constituée en octobre 2019 par une lettre de mission du Premier ministre adressée au Conseil économique, social et environnemental. La CCC regroupe des citoyennes et citoyens tirés au sort et a pour objectif de *« définir les mesures structurantes pour parvenir, dans un esprit de justice sociale, à réduire les émissions de gaz à effet de serre d'au moins 40 % d'ici 2030 par rapport à 1990 »*. Son rapport a été adopté le 21 juin 2020, la proposition 150 s'intitule « Accompagner l'évolution du numérique pour réduire ses impact » https://www.vie-publique.fr/sites/default/files/rapport/pdf/274855.pdf
2. Voir notamment *The Shift Project, Lean ICT : « Pour une sobriété numérique »*, octobre 2018 ; GreenIT.fr, « Empreinte environnementale du numérique mondiale », septembre 2019 ; Arcep, « Réseaux du futur - Empreinte carbone du numérique », octobre 2019 ; CGE, « Réduire la consommation énergétique du numérique », décembre 2019 ou encore Citizing, « Empreinte carbone du numérique en France : des politiques publiques suffisantes pour faire face à l'accroissement des usages ? », juin 2020.
3. Au niveau national, les émissions de GES se décomposent entre émissions directes (soit les émissions directement liées à la fabrication et l'usage d'un produit ou service) et les émissions indirectes (soit les émissions liées, sur le territoire national uniquement, à la consommation d'énergie indirectement source d'émissions de GES ou à d'autres étapes du cycle de vie du produit ou service tel que le transport, le recyclage, etc.). Ces émissions ne prennent pas en compte les sources d'origines étrangères mais uniquement celles situées sur le territoire national. La notion d'empreinte comprend à la fois les émissions directes et indirectes produites sur le territoire national et à l'étranger. Au niveau mondial, les émissions directes et indirectes correspondent donc à l'empreinte.
4. Sénat, Rapport d'information – Pour une transition numérique écologique, juin 2020.
5. Accord de Paris, adopté le 12 décembre 2015 à Paris, signé le 22 avril 2016 au siège des Nations unies à New-York, et entré en vigueur le 4 novembre 2016, https://unfccc.int/files/essential_background/convention/application/pdf/ french_paris_agreement.pdf

L'Arcep a décidé de se saisir pleinement de cet enjeu en s'appuyant sur la mission que lui a confiée la loi en 2010[6] suite au Grenelle de l'environnement, de veiller au respect de l'environnement dans son action en lien avec le Gouvernement.

Dans ce cadre, il faut rappeler que le numérique constitue un puissant facteur d'évolution de la société, tant au plan économique et social que dans la vie quotidienne de nos concitoyens et dans l'évolution des services publics. À cette aune, l'Autorité est attentive à ce que les utilisateurs des réseaux et services numériques restent maîtres de leurs choix et puissent bénéficier des apports des évolutions technologiques. Autrement dit pour l'Autorité, limiter l'impact environnemental du numérique n'est pas forcément synonyme de bridage des usages ou des technologies. Tout l'enjeu est de combiner le développement du numérique selon les besoins de la société et de l'économie avec une nouvelle exigence environnementale.

Ensuite, pour mieux comprendre et appréhender les enjeux liés à l'empreinte environnementale du numérique, et conformément au mode d'action du régulateur, l'Arcep a décidé d'amorcer la construction de ce nouveau chapitre de la régulation en dialoguant avec l'ensemble des parties prenantes. Au moyen de rencontres avec des experts engagés sur la thématique, mais surtout, afin de décloisonner les débats et recueillir la parole d'un plus grand nombre d'acteurs, en développant un espace de dialogue, au sein de la plateforme collaborative « Pour un numérique soutenable ». Le 11 juin 2020, avec le lancement de cette dernière, l'Arcep appelait associations, institutions, opérateurs, entreprises du numérique, personnalités motivées pour y contribuer, dans une série d'ateliers. Dans le cadre de cette plateforme, les participants se sont intéressés aux réseaux télécoms dans leur ensemble (fixes et mobiles), mais aussi aux terminaux et aux usages, véritables moteurs de la consommation numérique et de son empreinte environnementale. Un premier échange, le 9 juillet 2020, avait permis de définir les thèmes de ces ateliers techniques jusqu'à la production d'un premier rapport, annoncé pour la fin de l'année. Tout au long du 2e semestre 2020, une série d'ateliers thématiques et deux grandes discussions, rassemblant 127 participants, ont permis de partager les visions, pratiques, outils et compétences de chacun, afin d'alimenter la réflexion collective.

Un rapport d'étape, fruit de ces échanges, et alimenté par 42 contributions écrites d'acteurs participants, a été publié le 15 décembre 2020.

1 Les propositions du rapport

Dans ce rapport d'étape, l'Arcep formule **11 propositions** pour conjuguer développement des usages et réduction de l'empreinte environnementale du numérique. Suite au constat qu'une prise de conscience est déjà à l'œuvre, les propositions de l'Arcep se donnent pour objectif d'amplifier cette mobilisation, et de s'assurer qu'elle permette effectivement de dépasser le seul registre des bonnes intentions, pour s'inscrire dans une trajectoire ambitieuse de réduction de l'empreinte environnementale. Il s'agit d'inventer une régulation environnementale du numérique, intégrant non seulement les opérateurs de communications électroniques mais aussi les fabricants de terminaux, les fournisseurs de contenus et d'applications en ligne, les exploitants de centres de données… Les consommateurs peuvent aussi jouer un rôle plus actif à condition de disposer des informations utiles, dans une logique de régulation « par la donnée ».

L'analyse de l'Autorité met en lumière la nécessité de disposer de davantage de données pour définir plus finement l'empreinte environnementale du numérique pour toutes les composantes de son écosystème, dépasser l'étape de la prise de conscience et ainsi être à même de prendre les mesures appropriées.

Le rapport souligne la dimension « écosystémique » du numérique qui sollicite des acteurs divers et donc des expertises variées telles que la connaissance d'ingénierie des réseaux et des centres de données, celle des terminaux, mais aussi par exemple de développement des services et applications en ligne, etc, nécessitant chacune des expertises complexes d'origines distinctes. Une analyse de l'empreinte environnementale du numérique exige ainsi une collaboration poussée entre experts de l'environnement et experts du numérique, sur l'ensemble de l'écosystème et pour toutes les phases de la vie des produits en cause (production, usage, fin de vie). En conséquence, le rapport de l'Arcep établit des propositions pour l'ensemble de l'écosystème du numérique.

6. Loi n° 2010-788 du 12 juillet 2010 portant engagement national pour l'environnement.

11 PROPOSITIONS DU RAPPORT « POUR UN NUMÉRIQUE SOUTENABLE »

Axe 1 : Renforcer la capacité de pilotage de l'empreinte environnementale du numérique par les pouvoirs publics

1. Confier à une entité publique le pouvoir de collecter les informations utiles auprès de l'ensemble de l'écosystème
2. Participer, dans le cadre de ses initiatives avec l'ADEME, à la création d'un référentiel de mesure de référence

Axe 2 : Intégrer l'enjeu environnemental dans les actions de régulation de l'Arcep

Sur le fixe

3. Accompagner la transmission du cuivre vers la fibre
4. Encourager les optimisations des réseaux (mutualisation)
5. Encourager des initiatives visant à la mise en veille automatique des box des opérateurs

Sur le mobile

6. Affiner l'analyse des impacts d'une extinction des réseaux 2G ou 3G pour lever les barrières possibles
7. Étudier en 2021 une évolution des indicateurs de « performance » des réseaux pour y intégrer l'enjeu environnemental
8. Étudier, en lien avec les acteurs, les solutions d'optimisation de l'impact environnemental des réseaux mobiles
9. Développer un suivi plus précis des pratiques de subventionnement de terminaux par les opérateurs et de leurs effets

Axe 3 : Renforcer les incitations des acteurs économiques, acteurs privés, publics et consommateurs

10. Élaborer avec les acteurs concernés des codes de conduites/chartes renforçant la logique d'écoconception et pouvant mener à l'adoption d'engagements juridiquement contraignants
11. Renforcer la capacité d'action et la responsabilité des utilisateurs par une démarche de régulation par la donnée favorisant l'émergence d'outils d'aide à la décision du consommateur (« baromètre environnement »)

2 Les travaux législatifs et gouvernementaux

Certaines des propositions du rapport ont trouvé un écho dans les travaux législatifs en cours, autour de la proposition de loi visant à réduire l'empreinte environnementale du numérique en France[7] et du projet de loi portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets[8].

En parallèle, la feuille de route « Numérique et Environnement » du Gouvernement[9], publiée le 23 février 2021, a repris un certain nombre de propositions l'Arcep[10]. Certaines d'entre elles concernent directement l'Arcep. Notamment :

- **Collecter des données environnementales auprès des acteurs du numérique et construire un « baromètre environnemental »**

La feuille de route du Gouvernement (action 3 : « Construire un baromètre environnemental des acteurs du numérique »), confie à l'Arcep, en association avec l'ADEME, la mise en place d'une collecte annuelle de données environnementales auprès des acteurs du numérique ainsi que la construction et le suivi d'un baromètre environnemental des acteurs du numérique.

À ce jour, l'Arcep a élargi sa décision de collecte auprès des opérateurs et récupère des informations relatives à la consommation électrique et énergétique des réseaux. Les travaux législatifs en cours devraient permettre d'élargir le pouvoir de collecte de données de l'Arcep sur les enjeux environnementaux à l'ensemble des acteurs du numérique (fabricants de terminaux, fournisseurs de contenus et d'applications en ligne, exploitants de centres de données…).

7. La proposition de loi visant à réduire l'empreinte environnementale du numérique en France a été proposée par le sénateur Patrick Chaize et votée au Sénat le 13 janvier 2021. Le texte sera examiné à l'Assemblée nationale fin mai 2021. http://www.senat.fr/dossier-legislatif/ppl20-027.html
8. Le projet de loi portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets a été déposé par le Gouvernement le 10 février 2021 pour tenter de répondre aux propositions de la Convention citoyenne pour le climat. Le texte, très général, propose quelques articles relatifs au numérique. Il a été voté le 4 mai 2021 à l'Assemblée nationale et sera discuté au Sénat en juin. https://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_contre_le_dereglement_climatique
9. https://www.gouvernement.fr/numerique-et-environnement-la-feuille-de-route-du-gouvernement
10. Notamment : 1. Confier à une entité publique le pouvoir de collecter les informations utiles de l'ensemble de l'écosystème numérique et 11. « Baromètre environnemental » / 2. Participer, dans le cadre des initiatives avec l'ADEME, à la création d'un référentiel de mesure de référence / 9. Développer un suivi plus précis des pratiques de subventionnement de terminaux par les opérateurs et leurs effets / 10. Élaborer avec les acteurs concernés des codes de conduite/chartes renforçant la logique d'écoconception.

- **Élaborer une méthodologie de quantification de l'empreinte numérique sur l'environnement**

La feuille de route du Gouvernement (action 1 : « Élaborer une méthodologie de quantification de l'empreinte numérique sur l'environnement ») a confirmé la mission confiée par Barbara Pompili, ministre de la Transition écologique, Bruno Lemaire, ministre de l'Économie, Agnès Pannier-Runacher, ministre chargée de l'Industrie et Cédric O, secrétaire d'État chargé de la Transition numérique et des Communications électroniques, conjointement avec l'ADEME et l'Arcep sur l'évaluation de l'impact environnemental du numérique en France, dont l'un des buts est d'objectiver l'empreinte environnementale des réseaux de télécommunication fixes et mobiles en fonction des usages qu'ils supportent[11].

Cette collaboration entre l'ADEME et l'Arcep s'avère plus large que cette seule mission et permet de développer une approche commune autour de la mesure, de la collecte de données et de la production de méthodologies de mesure de l'empreinte environnementale du numérique et des briques techniques qui la composent. Les deux institutions ont également initié d'autres travaux et des échanges plus réguliers avec les experts de ces questions pour continuer à éclairer ces enjeux.

- **Élaborer une étude sur les modèles de distribution des téléphones mobiles et sur le renouvellement de ces équipements pour le grand public**

La feuille de route du Gouvernement (action 6 : « Prolonger la durée de vie des équipements et lutter contre l'obsolescence logicielle ») a confié à l'Arcep l'élaboration d'une étude sur les différentes pratiques commerciales de distribution des téléphones mobiles et de leurs éventuels impacts sur le taux et la fréquence de renouvellement, notamment au regard des autres modèles de vente. Cette analyse s'inscrit dans la continuité de la demande de la Convention citoyenne pour le climat et afin de permettre au Gouvernement de prendre d'éventuelles mesures en la matière. Une lettre de mission en date du 19 mars 2021 est venue préciser cette mission et l'Arcep a rendu début juin 2021 ses premières analyses à Barbara Pompili et Cédric O.

Travailler sur les voies et moyens de prise en compte des enjeux environnementaux dans les critères d'attribution des prochaines bandes de fréquence 26 Ghz.

La feuille de route du Gouvernement (action 8 : « Accompagner les entreprises du numérique dans l'adoption de l'écoconception et des principes du numérique durable et sobre ») saisit également l'Arcep pour étudier les voies et moyens permettant la prise en compte des enjeux environnementaux dans les critères d'attribution de la potentielle future bande de fréquence 26 GHz, liée à la 5G.

3 Poursuite des travaux

L'Autorité souhaite, comme elle le fait avec les associations de consommateurs ou avec la communauté internet, pérenniser le processus de dialogue, d'écoute et d'enrichissement mutuel qu'elle cherche à construire depuis le lancement de sa démarche, en proposant notamment aux participants de la plateforme et à tout acteur qui souhaiterait rejoindre la démarche, **de se réunir à nouveau en septembre 2021 pour faire un état des lieux sur l'avancée des propositions qu'elle a faites et plus généralement sur l'évolution de l'empreinte environnementale du numérique.**

11. Cette lettre de mission est notamment évoquée dans le cadre de la feuille de route du Gouvernement publiée en février 2021 : https://www.gouvernement.fr/numerique-et-environnement-la-feuille-de-route-du-gouvernement

La parole à



BARBARA POMPILI

Ministre de la Transition écologique



CÉDRIC O

Secrétaire d'État chargé de la Transition numérique et des Communications électroniques

MAÎTRISER L'IMPACT ENVIRONNEMENTAL DU NUMÉRIQUE ET FAIRE DU NUMÉRIQUE UNE CHANCE POUR LA TRANSITION ÉCOLOGIQUE

Le Gouvernement est convaincu que les transitions numérique et écologique sont désormais indissociables. Loin d'être une mode, les concilier est une exigence. Ces deux grandes transformations, qui façonnent, interrogent, parfois bousculent notre quotidien, ont en effet toutes deux connu un saut, notamment avec la crise actuelle ; si le numérique est devenu un pilier de notre société, l'écologie est un fondement indispensable à notre survie et à celle de la nature.

C'est pour se donner tous les moyens d'action utiles que nous avons lancé le 23 février dernier la mise en œuvre d'une feuille de route « Numérique et Environnement ». Déclinée en 3 axes et en 15 actions concrètes, il s'agit de maîtriser l'impact environnemental du numérique, d'abord en favorisant l'allongement de la durée de vie des produits, dont la fabrication représente la grande majorité de l'empreinte carbone du secteur.

Lutte contre l'obsolescence programmée, soutien au développement du réemploi et de la réparation, généralisation de l'éco-conception des équipements et des services : ce sont les priorités que nous nous sommes fixées, et qui se traduisent au travers du plan France Relance, de la commande publique exemplaire, des nouveaux dispositifs réglementaires (disponibilité des pièces détachées, éco-conditionnalité pour les *datacenters*), ou encore de futurs codes de bonne conduite avec les acteurs du numérique.

Par ailleurs, cette feuille de route ambitionne, et c'est une conviction profonde, de faire du numérique une chance, un levier pour la transition écologique. Cette dernière ne sera en effet possible qu'avec le numérique, avec des réseaux très performants, une forte connexion des acteurs et une utilisation importante de l'intelligence artificielle. Nous constatons déjà sur le terrain des avancées concrètes très intéressantes : meilleure gestion des ressources agricoles, optimisation des circuits logistiques, réduction de la consommation d'eau, ou encore amélioration de la gestion des déchets. Nous soutenons d'ailleurs fortement ces initiatives portées par des PME et des start-up notamment en mobilisant plus de 300 M€ de soutien à la « *Greentech* ».

Afin de concrétiser ces deux axes, la feuille de route répond également au besoin de données précises, claires, objectives et faisant consensus, sur l'impact réel du numérique sur l'environnement, ceci afin de développer la connaissance et d'outiller les décisions et actions collectives.

C'est dans cette optique que le Gouvernement a missionné l'Arcep sur plusieurs sujets capitaux : étude sur l'impact environnemental des infrastructures et des services numériques co-portée avec l'ADEME, analyse de l'impact environnemental des offres commerciales de téléphonie mobile notamment celles des offres groupées, réflexion sur les voies et moyens pour mieux prendre en compte les enjeux environnementaux dans la potentielle prochaine attribution des fréquences 5G bande 26 Ghz.

L'Arcep est un partenaire-clé pour objectiver mais aussi pour travailler à maîtriser cette empreinte. La publication chaque année de cet état des lieux très complet d'internet, tout comme la parution en décembre dernier du rapport « Pour un numérique soutenable », témoignent de l'exemplarité des travaux du régulateur.

Réussir à faire converger numérique et environnement est un défi collectif. À nous de le relever ensemble.

La parole à



PATRICK CHAIZE

Sénateur de l'Ain, président du groupe d'études Numérique, président de l'Avicca

GARANTIR LE DÉVELOPPEMENT D'UN NUMÉRIQUE SOBRE, RESPONSABLE ET ÉCOLOGIQUEMENT VERTUEUX

Les enjeux environnementaux nous amènent collectivement à nous interroger sur nos outils, pratiques et modes d'organisation, afin de les rendre davantage soutenables. Les réseaux et usages numériques n'échappent pas à la règle.

La crise sanitaire démontre le rôle essentiel des outils numériques. Or si leur généralisation est souhaitable sur le plan sociétal, celle-ci accroît mécaniquement leur impact environnemental. Elle oblige les parties prenantes à reconsidérer leurs actions, afin de rendre positif le solde entre les bénéfices d'un numérique facteur de transition écologique, et l'empreinte environnementale générée par la construction, le fonctionnement et le remplacement des réseaux, serveurs et autres terminaux.

Dans cet esprit, j'ai déposé une proposition de loi cosignée par plus de 130 sénateurs visant à réduire l'empreinte environnementale du numérique en France. Il s'agit d'orienter le comportement de tous les acteurs du numérique pour garantir le développement d'un numérique sobre, responsable et écologiquement vertueux.

Adopté en première lecture au Sénat en janvier 2021 et à l'Assemblée nationale en juin 2021, ce texte qui a été largement conforté dans ses principales orientations par le rapport du Haut Conseil pour le climat (HCC), doit être prochainement inscrit à l'ordre du jour du Sénat pour 2e lecture.

Les missions de l'Avicca s'inscrivent dans cette logique. Elle assure la promotion et la diffusion des bonnes pratiques des collectivités, dont l'exercice des compétences mais également les projets leur confèrent un rôle central dans la convergence des transitions économique, écologique et numérique. Aussi a-t-il été décidé que l'impact environnemental du numérique serait une nouvelle thématique.

L'Avicca prendra toute sa part dans cet exercice, aux côtés de l'Arcep dont elle soutiendra les actions déterminantes visant à responsabiliser l'ensemble des acteurs de la chaîne à l'adoption de pratiques plus vertueuses.



ARNAUD LEROY

*Président - **ADEME***

ADEME-ARCEP, DEUXIÈME ANNÉE DE COLLABORATION

L'année 2020 fut – entre autres – celle du constat d'une nécessité de s'appuyer sur les services et réseaux numériques pour continuer à vivre, travailler, communiquer, enseigner à nos enfants, étudier, nous divertir… Tout en ayant conscience du besoin de connaître et maîtriser les impacts de ces services, bien plus matériels et réels que l'idée qu'ils véhiculent.

L'ADEME a débuté une étroite et fructueuse collaboration avec l'Arcep autour d'un travail sur la connaissance des impacts environnementaux du numérique. Ce travail nous permettra d'apporter une vision objective de ces impacts en France, et d'en proposer une vision prospective à l'horizon 2050. Notre objectif est de pouvoir proposer des pistes et leviers à l'action publique. Ce travail d'étude permettra également de contribuer collectivement à la feuille de route du Gouvernement « Numérique et Environnement », et de donner des clés de lecture et de compréhension aux Français pour une consommation plus responsable.

Notre collaboration s'étend également sur les travaux liés à l'élaboration de méthodologies permettant de développer un socle technique, partagé et utilisé par tous les acteurs déterminés à mesurer l'impact environnemental de leurs produits et services numériques.

Au-delà de la connaissance des impacts, il est nécessaire de travailler à la réduction des impacts environnementaux en développant notamment l'éco-conception, de toutes les briques des services numériques, qu'elles soient logicielles ou matérielles. Des acteurs majeurs du monde numérique, qu'ils soient opérateurs télécoms, distributeurs de contenu ou de services, commencent à s'engager et à montrer la voie d'un numérique plus responsable. Il est nécessaire d'accélérer dans ce sens. La mise en œuvre du Plan de relance nous permet un accompagnement sans précédent des entreprises pour emprunter cette voie vers une innovation qui se doit d'être plus frugale, tout en répondant aux besoins de notre société.

La parole à



MICHEL COMBOT

*Directeur général - **Fédération française des télécoms***

LES INFRASTRUCTURES NUMÉRIQUES ET L'ENVIRONNEMENT

La crise sanitaire et économique que traverse notre pays depuis le début de l'année 2020 a démontré l'importance vitale des infrastructures numériques pour le maintien de l'activité économique et sociétale. Les réseaux numériques ont su absorber un surcroît important de trafic, jusqu'à 30 % sur internet au plus fort du premier confinement de mars 2020.

L'accès de toutes et tous, entreprises et particuliers, à ces infrastructures est donc bien indispensable, d'autant que le développement des réseaux et des usages numériques permet de diminuer, au global, l'émission des gaz à effet de serre (GES), par son impact sur l'ensemble des secteurs industriels et sur la vie quotidienne des citoyens, que ce soit par la réduction des déplacements ou l'automatisation des procédés industriels.

Par exemple, selon une étude réalisée par Arthur D. Little pour la Fédération, un gramme de CO_2 émis en matière de télétravail a conduit à une économie d'émission de 100 g de CO_2.

Pour autant, même si les réseaux numériques, selon une étude de juin 2020 de Citizing et KPMG, ne représentent que 5 % des émissions de gaz à effet de serre du numérique en France, contre 81 % pour les terminaux et 14 % pour les *datacenters*, le secteur des infrastructures numériques investit régulièrement pour optimiser sa consommation énergétique. Ainsi, la fibre consomme 3 fois moins d'énergie que les réseaux cuivre. De plus, chaque nouvelle génération de réseau mobile a permis de réduire d'un facteur de 10 la consommation d'énergie nécessaire pour transmettre un gigaoctet par rapport à la précédente, ce qui sera aussi le cas avec la 5G.

Dans ce contexte, il est indispensable de sensibiliser collectivement le grand public à l'enjeu environnemental : que ce soit en incitant les citoyens à recycler leurs téléphones mobiles – les opérateurs de la Fédération ont collecté 5,5 millions de téléphones depuis 2016, ou en les informant sur l'équivalence entre usages et émissions de GES. Cette information sera mise en œuvre dans les prochains mois par les opérateurs, au travers notamment des travaux avec l'ADEME.

LEXIQUE

Afnic (Association française pour le nommage internet en coopération) : association loi de 1901 qui a pour mission de gérer les domaines internet nationaux de premier niveau de France (.fr), La Réunion (.re), Terres australes et antarctiques françaises (.tf), Mayotte (.yt), Saint-Pierre-et-Miquelon (.pm) et Wallis-et-Futuna (.wf).

Android : système d'exploitation mobile développé par Google, utilisant le noyau Linux.

API (*Application Programming Interface*) : interface de programmation applicative qui permet à deux systèmes de s'interopérer et de communiquer sans qu'ils aient été conçus initialement dans cet objectif. Plus précisément, ensemble normalisé de classes, de méthodes ou de fonctions au travers duquel un logiciel offre des services à d'autres logiciels.

APN (*Access Point Name*) : identifiant qui permet à un utilisateur de téléphonie mobile de se connecter à internet.

ARN (Autorité de Régulation Nationale) : organisme chargé par un État membre du BEREC de la régulation des communications électroniques.

BEREC (*Body of European Regulators for Electronic Communications*) : instance européenne indépendante créée par le Conseil de l'Union européenne et le Parlement européen qui rassemble les régulateurs des communications électroniques des 27 États membres de l'Union européenne.

Câble ou « réseaux câblés » : réseaux de communications électroniques constitués d'un cœur de réseau en fibre optique et d'une terminaison en câble coaxial. Historiquement conçus pour diffuser des services de télévision, ces réseaux permettent depuis plusieurs années d'offrir également des services de téléphonie et d'accès à internet grâce à l'utilisation de la bande passante non mobilisée par les flux de télévision.

CDN (*Content Delivery Network*) : réseau de diffusion de contenu sur internet.

CDN interne : CDN situé directement dans le réseau des FAI.

CGN (*Carrier-Grade NAT*) : mécanisme de traduction d'adresse réseau (*Network Address Translation* ou NAT) à grande échelle, utilisé notamment par des FAI dans le but de diminuer la quantité d'adresses IPv4 utilisées.

[Adaptateurs] CPL (Courants Porteurs en Ligne) : équipement qui permet de transporter internet par le réseau électrique à l'intérieur d'une habitation à la place d'un câble Ethernet ou du Wi-Fi.

***Cross-traffic* :** le *cross-traffic* fait référence au trafic généré pendant un test de QoS et/ou QoE par une autre application que celle réalisant le test, sur le même terminal ou sur un autre terminal connecté à la même box. Le *cross-traffic* diminue le débit disponible pour le test.

***Crowdsourcing* :** les outils de *crowdsourcing* font référence aux dispositifs qui centralisent des mesures de QoS et/ou QoE réalisées par des utilisateurs réels.

Débit : quantité de données numériques transmises par unité de temps. Le débit s'exprime souvent en bits par seconde (bit/s) et ses multiples Mbit/s, Gbit/s, Tbit/s, etc. Il convient de distinguer la vitesse à laquelle les données peuvent être :

- envoyées depuis un ordinateur, un téléphone ou tout autre équipement terminal connecté à internet, comme pendant l'envoi de photographies vers un site d'impression en ligne : on parle alors de débit montant ;
- reçues depuis un équipement terminal connecté à internet, comme lors du visionnage d'une vidéo en ligne ou du chargement d'une page web : on parle de débit descendant.

DNS (*Domain Name System*) : mécanisme de traduction des noms de domaine internet en adresses IP.

DNSSEC (*Domain Name System Security Extensions*) : extension de sécurité du protocole DNS.

***Dual-stack* (Double pile IP) :** consiste à affecter une adresse IPv4 et une adresse IPv6 à un équipement du réseau.

***ePrivacy* :** directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques). Un projet de règlement « *ePrivacy* » visant à remplacer l'actuelle directive est en cours de discussion et porte notamment sur l'utilisation des cookies et les pratiques associées, ainsi que le recueil du consentement des internautes.

[câble] Ethernet : nom usuel du connecteur RJ45 supportant le protocole de communication de paquets Ethernet.

FAI : Fournisseur d'Accès à Internet.

FCA (Fournisseurs de Contenu et d'Applications) : fournisseurs du contenu (pages web, blogs, vidéos) et/ou des applications (moteurs de recherche, applications VoIP) sur internet.

***Firewall* :** pare-feu, il s'agit d'un dispositif matériel ou logiciel de sécurité qui permet de filtrer et de bloquer les flux en fonction de la politique de sécurité en place.

FttH ou « réseaux fibrés » (*Fiber to the Home*) : réseau de communications électroniques à très haut débit en fibre optique jusqu'à l'abonné, c'est-à-dire pour lequel la fibre optique se termine dans le logement ou le local de l'abonné.

HTTP (*Hypertext Transfer Protocol*) : protocole de communication client-serveur développé pour le *World Wide Web*.

HTTPS (*HTTP Secured*) : protocole HTTP sécurisé par l'usage des protocoles SSL ou TLS.

IAD (*Integrated Access Device*) : passerelle domestique, communément appelée box internet, qui permet de connecter téléphone, ordinateur et box TV.

iOS : système d'exploitation mobile développé par Apple pour ses appareils mobiles.

IoT (*Internet of Things* ou internet des objets) : réseau d'objets intégrant notamment des capteurs et des logiciels leur permettant de se connecter à d'autres terminaux et systèmes sur internet et d'échanger des données avec eux.

IP (*Internet Protocol*) : protocole de communication qui permet un service d'adressage unique pour l'ensemble des terminaux utilisés sur internet. IPv4 (IP version 4) est le protocole utilisé depuis 1983. IPv6 (IP version 6) est son successeur.

IPv6 activé : qui émet et reçoit effectivement du trafic en IPv6, soit grâce à une activation de la part du client, soit grâce ou une activation effectuée par l'opérateur.

IPv6-*ready* : qui est compatible avec le protocole IPv6, mais sur lequel IPv6 n'est pas nécessairement activé par défaut.

IXP (*Internet Exchange Point*) ou GIX (*Global Internet Exchange*) : infrastructure physique permettant aux FAI et FCA qui y sont connectés d'échanger du trafic internet entre leurs réseaux grâce à des accords de *peering* public.

LAN (*Local Area Network*) : réseau local. Pour un particulier, il s'agit du réseau constitué de la box du FAI et de tous les périphériques qui y sont connectés en Ethernet ou en Wi-Fi.

Latence : délai nécessaire à un paquet de données pour passer de la source à la destination *via* un réseau. La latence est exprimée en millisecondes.

Linux : au sens large, désigne tout système d'exploitation fondé sur le noyau Linux. Le noyau Linux est utilisé sur du matériel informatique allant des téléphones portables (exemple : Android) aux super-ordinateurs en passant par les PC (exemple : Ubuntu).

---

macOS : système d'exploitation développé par Apple pour ses ordinateurs.

Mires de test (pour les tests de qualité de service) : un serveur qui ne stocke pas de données, mais qui est en mesure de délivrer des données à très haut débit, afin de permettre de mesurer le débit.

NAS (*Network Attached Storage*) : serveur de stockage de fichiers, autonome et relié à un réseau.

NAT (*Network Adress Translation*) : mécanisme de traduction d'adresses réseau permettant de faire correspondre des adresses IP à d'autres adresses IP, notamment utilisé pour limiter le nombre d'IPv4 publiques utilisées.

OS (*Operating System*) : système d'exploitation. Logiciel qui permet de faire fonctionner un périphérique, comme Windows, macOS, Linux, Android ou iOS.

OTT (*Over-The-Top*) : qualifie les services de communications électroniques fournis par des FCA sur internet.

***Peering* :** désigne l'échange de trafic internet entre deux pairs (ou *peers*). Un lien de peering peut être gratuit ou payant (pour celui qui envoie le plus de trafic vers son pair). Le *peering* peut par ailleurs être public, lorsqu'il est réalisé à un IXP (*Internet Exchange Point*), ou privé, lorsqu'il s'effectue dans le cadre d'un PNI (*Private Network Interconnect*), c'est-à-dire d'une interconnexion directe entre deux opérateurs.

Point de terminaison du réseau : le point physique auquel un utilisateur obtient l'accès à un réseau de communications électroniques public.

POP (*Point of Presence*) : point de présence physique d'un opérateur.

Port logiciel : à chaque connexion sur internet émanant d'une application est associée à une session UDP ou TCP, elle-même identifiée au moyen d'un « numéro de port », c'est-à-dire une adresse codée sur 16 bits.

Puce NFC (*Near-Field Communication*) : technologie de communication sans fil à courte portée et à haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm dans le cas général.

QoE (Qualité d'Expérience) : dans le cadre du chapitre 1, qualité de l'expérience de l'utilisateur sur internet lors d'usages donnés. Elle est mesurée par des indicateurs dits « d'usage » comme le temps de téléchargement de pages web ou la qualité de la lecture de vidéo en *streaming*.

QoS (Qualité de Service) : dans le cadre du chapitre 1, qualité de service du réseau internet mesurée par des indicateurs dits « techniques » comme le débit montant ou descendant, la latence ou la gigue. Il arrive souvent que le terme QoS soit utilisé pour désigner à la fois la qualité de service au sens de la présente définition et la qualité d'expérience.

RFC (*Requests For Comments*) : documents officiels décrivant les aspects et spécifications techniques d'internet ou de différents matériels informatiques.

RGPD (Règlement Général sur la Protection des Données) : règlement n° 2016/679 de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

SDN (*Software-Defined Network*) : modèle d'architecture réseau qui est basé sur un contrôle centralisé des ressources réseau, une orchestration centralisée et une virtualisation des ressources physiques.

Service spécialisé : service(s) de communications électroniques distinct(s) des services d'accès à l'internet qui nécessite(nt) des niveaux de qualité spécifiques.

SI (Système d'Information) : ensemble organisé de ressources qui permet de collecter, stocker, traiter et diffuser de l'information.

Sonde matérielle : outil de mesure de QoS et/ou QoE qui prend souvent la forme d'un boîtier à connecter à la box du FAI *via* un câble Ethernet. La sonde matérielle teste généralement de manière passive et automatique la ligne internet.

TCP (*Transmission Control Protocol*) : protocole de transport fiable, en mode connecté, développé en 1973. En 2018, la majeure partie du trafic sur internet utilise le protocole TCP, au-dessus du protocole IPv4 ou IPv6.

Test de débit mono-connexion (*monothread*) : test mesurant le débit *via* une seule connexion, ce qui permet de remonter un débit représentatif d'une utilisation d'internet.

Test de débit multi-connexions (*multithread*) : test mesurant le débit en additionnant les débits de multiples connexions simultanées, ce qui permet d'estimer la capacité du lien.

Testeur web : outil de mesure de QoS et/ou QoE accessible depuis un site internet.

Tier 1 : réseau capable de joindre tous les réseaux internet par une interconnexion directe (*peering*) sans avoir de transitaire. En 2019, 18 opérateurs sont Tier 1 : AT&T, CenturyLink/Level 3, Cogent Communications, Deutsche Telekom AG, Global Telecom & Technology, Hurricane Electric, KPN International, Liberty Global, NTT Communications, Orange, PCCW Global, Sprint, Tata Communications, Telecom Italia Sparkle, Telxius/Telefónica, Telia Carrier, Verizon Enterprise Solutions, Zayo Group.

TLS (*Transport Layer Security*) : permet de chiffrer les échanges sur internet et d'authentifier le serveur.

Transitaire : opérateur de transit.

Transit : bande passante vendue par un opérateur à un opérateur client, qui permet d'accéder à la totalité de l'internet dans le cadre d'un service contractuel et payant.

UDP (*User Datagram Protocol*) : protocole de transport simple, sans connexion (aucune communication préalable n'est requise) qui permet de transmettre rapidement de petites quantités de données. Le protocole UDP s'utilise au-dessus du protocole IPv4 ou IPv6.

VoD (*Video on Demand ou vidéo à la demande*) : technique de diffusion de contenus vidéo numériques interactive *via* réseaux câblés (internet) ou non câblés. La SVoD désigne un service de vidéo à la demande par abonnement (SVoD).

VoIP (voix sur IP ou *Voice over IP*) : technologie qui permet de transmettre la voix sur des réseaux compatibles IP *via* internet.

VPN (*Virtual Private Network*) : connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel.

WAN (*Wide Area Network*) : dans le présent rapport, le réseau WAN désigne le réseau internet par opposition au réseau LAN.

Wehe : application Android et iOS, développée par la Northeastern University en partenariat avec l'Arcep pour détecter des pratiques de gestion de trafic contraires au principe de neutralité du net.

Wi-Fi : protocoles de communication sans fil régis par les normes du groupe IEEE 802.11.

Windows : système d'exploitation propriétaire, développé par Microsoft, qui équipe la majorité des ordinateurs en France.

---

xDSL (*Digital Subscriber Line*) : technologies de communications électroniques utilisées sur les réseaux en cuivre qui permettent aux opérateurs de fournir un accès internet à haut ou très haut débit. Les normes ADSL2+ et VDSL2 sont les normes xDSL les plus utilisées en France pour les accès grand public.

***Zero-rating* :** pratique tarifaire consistant à ne pas décompter du forfait *data* du client final le volume de données consommé par une ou plusieurs applications particulières.

4G : quatrième génération des standards pour la téléphonie mobile. Elle est définie par les normes *Release* 8 du 3GPP.

5G : cinquième génération des standards pour la téléphonie mobile. Elle est définie par les normes *Release* 15 du 3GPP.

Ce document a été réalisé par l'Arcep

Cécile Dubarry, directrice générale
Virginie Mathot, conseillère de la Présidente

DIRECTION « INTERNET, PRESSE, POSTES ET UTILISATEURS »

Loïc Duflot, *directeur*

Unité « Internet ouvert »

Aurore Tual, *cheffe de l'unité*
Samih Souissi, *adjoint à la cheffe d'unité*
Vivien Guéant et Emmanuel Leroux, *chargés de mission*

Unité « Régulation par la donnée »

Pierre Dubreuil, *chef de l'unité*

DIRECTION « ÉCONOMIE, MARCHÉS ET NUMÉRIQUE »

Anne Yvrande-Billon, *directrice*
Laurent Toustou, *conseiller auprès de la directrice*

Unité « Analyse économique et intelligence numérique »

Anaïs Le Gouguec, *cheffe de l'unité*
Anaïs Aubert, *adjointe à la cheffe d'unité*
Arthur Dozias, *chargé de mission*
Estelle Patat, *stagiaire*

DIRECTION « MOBILE ET INNOVATION »

Anne Laurent, *directrice*
Maxime Forest, *directeur adjoint*

Unité « Couverture et Investissements mobiles »

Guillaume Decorzent, *chef de l'unité*

DIRECTION « COMMUNICATION ET PARTENARIATS »

Clémentine Beaumont, *directrice*
Anne-Lise Lucas et Charlotte Victoria, *chargées de mission*

DIRECTION « AFFAIRES JURIDIQUES »

Elisabeth Suel, *directrice*

Unité « Infrastructures et Réseaux ouverts »

Agate Rossetti, *cheffe de l'unité*
Paul Pastor, *chargé de mission*

Un grand merci à...

Toutes les personnes consultées, auditionnées ou ayant participé à la démarche de co-construction de l'Arcep sur la qualité de service d'internet ou à la task-force IPv6 pour leur dynamisme et leur contribution précieuse au présent rapport.

Ce contenu est mis à disposition selon les termes de la Licence Creative Commons Attribution - Partage dans les mêmes conditions 4.0 International

Publication
Arcep
14, rue Gerty-Archimède - 75012 Paris
Direction de la Communication
et Partenariats : com@arcep.fr

Design
Agence Luciole

Crédits photos
p. 6, 7, 8 et 9 : Adobe Stock
p. 39 : DC3

Illustrations
p. 73, 74 et 75 : Simon Giraudot

Juillet 2021

LE MANIFESTE
L'ARCEP, LES RÉSEAUX COMME BIEN COMMUN

Les réseaux d'échanges internet, télécoms fixes, mobiles et postaux, constituent une « infrastructure de libertés ». Liberté d'expression et de communication, liberté d'accès au savoir et de partage, mais aussi liberté d'entreprise et d'innovation, enjeu clé pour la compétitivité du pays, la croissance et l'emploi.

Parce que le plein exercice de ces libertés est essentiel dans une société ouverte, innovante et démocratique, les institutions nationales et européennes veillent à ce que les réseaux d'échanges se développent comme un **« bien commun »,** quel que soit leur régime de propriété, c'est-à-dire qu'ils répondent à des exigences fortes en termes d'accessibilité, d'universalité, de performance, de neutralité, de confiance et de loyauté.

À cette fin, les institutions démocratiques ont jugé qu'une intervention étatique indépendante était nécessaire pour veiller à ce qu'aucune force, qu'elle soit économique ou politique, ne soit en situation de contrôler ou de brider la capacité d'échange des utilisateurs (consommateurs, entreprises, associations, etc.).

L'Autorité de régulation des communications électroniques et des postes (Arcep), arbitre expert et neutre au statut d'autorité administrative indépendante, est **l'architecte** et le **gardien** des réseaux d'échanges en France.

Architecte des réseaux, l'Arcep crée les conditions d'une organisation plurielle et décentralisée des réseaux. Elle garantit l'ouverture du marché à de nouveaux acteurs et à toutes les formes d'innovation, et veille à la compétitivité du secteur à travers une concurrence favorable à l'investissement. L'Arcep organise le cadre d'interopérabilité des réseaux, afin qu'ils apparaissent comme un seul aux yeux des utilisateurs malgré leur diversité, simples d'accès et non cloisonnés. Elle coordonne la bonne articulation public/privé dans le cadre de l'intervention des collectivités territoriales.

Gardien des réseaux, l'Arcep s'assure du respect des principes essentiels pour garantir la capacité d'échange des utilisateurs. Elle veille à la fourniture du service universel, et accompagne les pouvoirs publics pour étendre la connectivité sur l'ensemble du territoire. Elle assure la liberté de choix et la bonne information des utilisateurs, et protège contre les atteintes possibles à la neutralité de l'internet.

L'Autorité lutte plus généralement contre toutes les formes de silos qui pourraient menacer la liberté d'échanger sur les réseaux, et s'intéresse à ce titre aux nouveaux intermédiaires que sont les grandes plateformes internet.