SYNTHÈSE DES DÉBATS

AROMATES RELATIONS PUBLIQUES
169 Rue d'Aguesseau 92100 Boulogne-Billancourt
Contact : aromates@aromates.fr
Document rédigé par Nicolas Brizé

PROPOS LIMINAIRES

« AGIR POUR QUE NOS INFRASTRUCTURE DU NUMÉRIQUE DEVIENNENT UN LEVIER DE PUISSANCE POUR LA SOUVERAINETÉ DE LA FRANCE »

Jacques MARCEAU, président d'Aromates

Les infrastructures du numérique sont devenues un pilier de la souveraineté nationale – notre économie, notre démocratie, notre sécurité en dépendent – mais ce sont aussi une nouvelle source de fragilité. Les câbles, les satellites, les datacenters, ou encore les réseaux pilotés par l'intelligence artificielle, doivent résister à des cyberattaques ou à des événements climatiques extrêmes. Dans un contexte géopolitique en tension, l'intrication croissante entre numérique, énergie et industrie expose ces infrastructures essentielles à une dépendance commerciale et technologique.

« La présence à ces 19èmes Assises du ministre chargé de l'industrie et de l'énergie témoigne de l'engagement au plus haut niveau de l'Etat pour garantir le déploiement, la maintenance, l'évolution et la protection de cet écosystème techno-industriel d'intérêt vital. »

Pour y parvenir, de nombreuses questions restent en suspens. Qui pense la sécurité des interconnexions entre réseaux énergétiques, infrastructures cloud, câbles sous-marins et satellites ? Qui porte la responsabilité de la résilience de cet écosystème ? Qui pour garantir la gouvernance, la permanence et la sécurité des réseaux nationaux et transcontinentaux terrestres, sous-marins et spatiaux ? Qui pour piloter et réguler les flux critiques à l'ère de l'IA et des ruptures technologiques ?

Ces Assises ont vocation à faire émerger des pistes de solutions concrètes et utiles à l'action publique.

« BÂTIR DES STRATÉGIES DE RÉSILIENCE, INVENTER DES OUTILS DE GOUVERNANCE, REDÉFINIR LA SOUVERAINETÉ À L'HEURE DU CLOUD, DES SATELLITES ET DE L'IA »

Damien MICHALLET, sénateur de l'Isère, président de la Commission Supérieure du Numérique et des Postes

Un « enjeu civilisationnel, » c'est sur ce mot que le sénateur introduit les grands thèmes de ces Assises.

Premier sujet : **sécurité et indépendance.** La guerre, les tensions sur les marchés mondiaux de l'énergie, les ruptures d'approvisionnement en composants électroniques, les épisodes climatiques, les cybermenaces croissantes, font des réseaux télécoms des « infrastructures critiques » : hôpitaux, administrations, opérations de secours, production industrielle, distribution d'énergie, logistique alimentaire, défense... « L'interdépendance entre ces infrastructures vitales et le numérique peut s'avérer dangereuse lorsqu'elle n'est pas cartographiée, planifiée, régulée. » Le sénateur salue les 100 milliards d'euros annoncés lors du Sommet de l'IA (fév.

2025) pour investir dans les datacenters. Mais « les plans de résilience doivent être mieux anticipés, mieux préparés, mieux planifiés. Il faut sécuriser la chaîne industrielle des semi-conducteurs, routeurs, équipements actifs ou datacenters face aux menaces géopolitiques. »

Second sujet : **les réseaux sous-marins et satellitaires**. 99% du trafic mondial transite par les fonds marins. La France, deuxième domaine maritime au monde, a une responsabilité : « avons-nous la maîtrise de nos câbles sous-marins ? » Les constellations privées de satellites offrent quant à elles de nouvelles formes de connectivité (zones blanches, territoires isolés, situation de crise), mais « elles ne nous appartiennent pas ». La France et l'Europe doivent se doter de constellations propres. « La loi de programmation militaire 2024-2030 amorce cette réflexion avec des budgets renforcés pour l'espace et la cyberdéfense. Mais cela ne suffira pas. Ce défi concerne l'économie, l'industrie, l'environnement et la démocratie. »

Troisième sujet : **les ruptures technologiques.** La 5G a ouvert la voie à une segmentation fine des usages, le slicing permet de réserver des capacités réseaux à certains services, l'intelligence artificielle optimise les flux, et tout cela change notre rapport à la neutralité du net, à la régulation et la sécurité. Ne doit-on pas hiérarchiser les usages, protéger en priorité les services d'urgence, l'enseignement, la télémédecine, les administrations, la défense ? Faut-il envisager des régimes d'exception pour certains usages stratégiques, ou au contraire maintenir une neutralité stricte ? Et que dire de la cybersécurité ? Les arbitrages sont complexes, que ce soit pour réguler l'accès aux données, contrôler les équipements ou garantir la sécurité sans tomber dans la surveillance de masse. « Le rapport Draghi [sur le futur de la compétitivité de l'Europe] propose la création d'une infrastructure publique intégrée résiliente. C'est une piste intéressante... »

Le président de la CSMP attend de ces débats des réflexions et des solutions qui nourriront les travaux législatifs afin, dit-il, de « **prendre les bonnes décisions pour construire une stratégie nationale du numérique** ».

« LA RÉSILIENCE, ÇA NE SE DÉCRÈTE PAS, ÇA SE CONSTRUIT AVEC AMBITION, AVEC ANTICIPATION, AVEC LE COLLECTIF. »

Marc FERRACCI, ministre chargé de l'industrie et de l'énergie

92% des Français sont éligibles à la fibre (contre 28% en 2017) ; 99,8% de la population est couverte en 4G (contre 89% en 2018) ; « la France dépasse les standards européens... » Après avoir dressé un bilan très positif du plan France Très Haut Débit et du New Deal Mobile, le ministre veut « aller plus loin » : « Les tempêtes Ciarán et Domingos nous l'ont appris : dans un monde où les crises se multiplient, les infrastructures numériques deviennent la cible, et il faut avoir le courage de les regarder pour ce qu'elles sont, c'est-à-dire **les artères numériques de la nation**. »

« La France ne veut pas dépendre. » Le vrai défi est de « sécuriser, protéger, et résister » face aux événements climatiques et aux attaques. La résilience doit garantir à la fois l'électricité et la connectivité. Cette « priorité absolue » passe par l'anticipation : « identifier les failles, renforcer les infrastructures, c'est le sens des **schémas locaux de résilience** ». Une trentaine de porteurs de projets de réseaux d'initiative publique (RIP) s'en sont saisi. Le ministre attend que « tous les territoires s'y engagent ». Et il a un message aux opérateurs : « **les plans de continuité d'activité et de reprise d'activité à jour sont de votre responsabilité**. Quand la crise frappe, il faut aller vite. Rétablir les réseaux mobiles, puis le réseau fixe, suppose une coordination sans faille entre opérateurs télécoms, acteurs de l'énergie, collectivités et services de l'Etat. »

Cette réactivité suppose aussi de « mieux préparer le terrain. Dans l'urgence, l'approximation peut coûter cher ». En lien avec le ministère de l'Intérieur, son ministère s'engage à diffuser dans les prochains mois un **guide pratique aux préfectures.** Par ailleurs, le **guide ORSEC-RETAP-RESEAUX** sera mis a jour début 2026 avec un objectif : « que chacun sache quoi faire, et qui fait quoi. »

Sur la méthode, le ministre entend « capitaliser » sur le plan THD. « Le triptyque Etat - Élus - Opérateurs a fait ses preuves. En période de crise, les informations doivent circuler vite. » Aussi il attend « une organisation de crise renforcée chez les opérateurs d'infrastructures, une mobilisation immédiate des opérateurs commerciaux, une collaboration exemplaire avec Enedis ». « Vous pouvez compter sur mon engagement pour fluidifier et optimiser ces relations. »

Enfin, le ministre pose la question de **l'enfouissement**. Bien que les infrastructures aériennes aient joué « un rôle essentiel pour connecter le pays », elles sont aussi « plus exposées aux aléas climatiques » (chutes d'arbres). Cependant, il reconnaît que « l'enfouissement n'est pas une réponse magique » (risque d'incendie, de glissements de terrain). « Nous avons le devoir d'identifier les vulnérabilités et de nous adapter de manière pragmatique, territoire par territoire. Seul le collectif nous permettra d'aller plus vite, plus fort et plus loin. C'est la condition de notre souveraineté, le socle de notre sécurité, le prix à payer pour que, face aux crises, aux attaques, au chaos, la France reste connectée, unie et debout dans la tempête. »

KEYNOTE QUELLE RÉGULATION POUR CONSTRUIRE NOTRE AUTONOMIE ?

Laure de La Raudière, présidente de l'ARCEP

Du point de vue du régulateur, « la France reste très dépendante des pays étrangers pour les équipements et services numériques devenus indispensables dans tous les instants de nos vie professionnelles et personnelles ». La crise du Covid, la guerre en Ukraine et l'élection de Trump ont fait prendre conscience de « la fragilité de notre économie et de notre société ». Cependant, Laure de la Raudière a une bonne nouvelle : la souveraineté numérique, la résilience et l'indépendance stratégique sont à l'agenda de la nouvelle commission européenne. « Pour construire notre autonomie, il faut créer un cadre de régulation favorable à l'émergence de nouveaux acteurs. Il ne peut y avoir d'autonomie stratégique sans alternative crédible aux géants mondiaux du cloud, les hyperscalers. »

Sur le marché des télécoms, la régulation a apporté stabilité et prévisibilité,

mutualisation et efficacité, innovation et compétitivité des prix. Ce cadre stable a justement permis et favoriser les investissements par des fonds spécialisés. » Craignant les sirènes de la dérégulation pour favoriser les investissements, l'Arcep plaide pour « la création de conditions claires et stables de régulation économique des services cloud et de l'IA afin de favoriser l'investissement et le développement d'acteurs émergents ».

La présidente cite trois actions. Pour « **faciliter le changement de fournisseur cloud** », l'Arcep vient de mettre en consultation publique les « bonnes pratiques », et se dit « très active » sur le Data Act (règlement sur la gouvernance des données). A**u niveau européen**, elle préconise de « **désigner les géants du numérique comme des gatekeepers pour leurs services cloud (dominants) et certains services d'IA (omniprésents) au titre du Digital Markets Act** ». Les capacités d'interaction de leurs nouveaux modèles d'IA avec leurs services numériques traditionnels (moteurs de recherche, services de cartographie, plateformes vidéo...) constituent « un risque majeur de verrouillage de certains services. L'accès aux ressources clés de développement de l'IA que sont la puissance de calcul, l'énergie, et les compétences, devrait être facilité pour les acteurs émergents et ne pas être préempté par les hyperscalers. » Enfin, une troisième condition de souveraineté serait de « **consolider un écosystème d'infrastructure de partage de données entre les entreprises dans un cadre de confiance** ». Depuis mai 2024, la loi SREN permet à l'Arcep de labelliser des intermédiaires de données. « Ce label naissant, valable dans toute l'Europe, constitue un nouveau front d'autonomie stratégique et un levier fort de souveraineté. »

Sur le volet environnemental, le diagnostic est préoccupant : « la consommation d'énergie explose, les ressources en minéraux et matériaux s'épuise ; si rien n'est fait, l'empreinte carbone du numérique aura triplé d'ici 2050. » L'Arcep entend « prendre le problème à la source et s'occuper des services : aujourd'hui c'est un angle mort des politiques publiques européennes ». Publié en 2024, le référentiel général de l'écoconception des services numériques (Arcep – ARCOM - ADEME) vise à réduire l'impact environnemental de ces services. À la clé, si les services sont mieux conçus : « moins de nouveaux datacenters, moins de nouveaux équipements dans les réseaux, et un renouvellement moins rapide des terminaux ». Avec le Forum des parties prenantes de l'écoconception des services numériques (lancé en 2025), l'Arcep et l'Arcom comptent sur la mobilisation de tous pour porter cette ambition au niveau européen.

Avant de conclure, Laure de La Raudière pointe les marchés publics. « Il faut permettre aux acteurs émergents européens d'avoir un accès préférentiel aux marchés publics. Le climat géopolitique nous donne un nouvel espoir pour une entente au niveau européen. » Pour finir, la présidente n'oublie évidemment pas les réseaux télécoms qui restent « au cœur de la stratégie de l'Arcep ». Des infrastructures numériques pour tous, partout, et pour longtemps, c'est « une nécessité qui inclut la soutenabilité, la résilience et la pérennité financière ».

EN SAVOIR PLUS : Référentiel général d'écoconception de services numériques - 2024

KEYNOTE LE SPECTRE DES FRÉQUENCES : L'HEURE DES CHOIX STRATÉGIQUES

Gilles BREGANT, directeur général de l'ANFR

Le spectre électromagnétique est devenu un enjeu majeur d'efficience à l'heure où tout est sans fil. « Brouiller une fréquence, un signal GPS, un mobile, c'est brouiller un service, l'accès au réseau », nous dit Gilles Bregant. Chaque année, entre 1 500 et 1 800 brouillages sont déclarés à l'ANFR. « Ils sont traités et résolus à 99%, mais il y en a probablement dix fois plus non déclarés. » Le rôle de l'ANFR est d'assurer la qualité du spectre critique en France métropolitaine et d'outre-mer, de prévenir les acte de cybermalveillance et les traiter en temps réel. À cet effet, l'ANFR, qui délivre les autorisations des émetteurs, a élaboré un tableau des fréquences prioritaires en cas de crise majeure (attentat, glissement de terrain...). « En cas de délestage électrique, nos études (avec l'Arcep et Enedis) ont identifié la couverture des services d'urgence. Nous accompagnons également la remise en état auprès des préfectures. Les réseaux mobiles ont été les premiers à redémarrer à Saint-Martin, et plus récemment à Mayotte et à La Réunion. »

« Les objectifs de sécurité, de résilience et de souveraineté dépendent étroitement de la manière dont nous allons gérer notre spectre de fréquences d'ici 2030. »

Pour organiser le spectre, il faut aussi avoir une vision du futur. Trois sujets sont sur la table. Premièrement, **le choix d'une bande de fréquence pour la 6G d'ici 2030.** Aux États-Unis, le projet de loi de finances massif de Trump (*One Big Beautiful Bill Act*) propose de réserver la bande 800 MHz à la 6G (soit deux fois plus que ce que l'on a en Europe pour la 5G). Cette mesure est inapplicable en Europe, car cette zone sert à l'OTAN et au spatial. « La France doit faire un choix : soit la 6G, soit les RLAN (Wifi). Si on ne fait rien, on n'aura que 500 MHz pour la 6G (soit autant que pour la 5G), donc la 6G ne sera pas un levier en 2030, ce qui est un peu inquiétant. »

Le second choix concerne la **bande autour de 2 GHz** (affectée initialement à des satellites américains), qui va permettre d'interagir directement entre satellites et smartphones (Direct-to-Device). Le choix des titulaires permettra d'assurer une couverture ubiquitaire sur des fréquences de téléphonie mobile terrestre en Europe, y compris dans les zones blanches (ce que fait déjà T-Mobile basé sur Starlink aux États-Unis). « Ce choix va conditionner la souveraineté des réseaux dans toute l'Europe occidentale. »

Troisième choix : **les constellations de satellites en orbite basse**. Ce système très résilient jouit d'une juridiction extra-territoriale. Les États-Unis (Starlink et Kuiper) et demain la Chine sont au-dessus de l'Europe. « L'Europe doit aller vite et décider des usages. » Une constellation consomme énormément de fréquences et cette ressource est rare dans l'espace. IRIS², la constellation européenne souveraine, n'existera que si elle est rapidement mise en orbite et que toutes les constellations respectent les règles internationales. « La loi de la jungle ne doit pas prévaloir à 500 km d'altitude. Il faut sécuriser les règles, s'assurer de leur application au niveau de l'UIT, et agir pour que l'Europe prenne sa place dans les quelque fréquences spatiales qui restent. » Rappelons qu'elles peuvent résoudre les zones blanches non couvertes en Europe.

SESSION 1

INTRODUCTION

Patricia DEMAS, sénatrice des Alpes-Maritimes, membre de la CSNP

Reconnaître la criticité dans notre droit

En préambule, la sénatrice regrette que la transposition de la **directive NIS 2** (*Network and Information Security*), qui vise à renforcer le niveau de cybersécurité des Etats membres, n'ait pas été l'occasion de franchir un pas décisif. « Il est crucial de reconnaître les infrastructures de fibre optique et les antennes relais comme des activités d'importance vitale, et les inscrire comme tels dans le code de la Défense. Cette classification déclencherait l'application d'obligations de sécurité renforcées pour les opérateurs, à la hauteur des enjeux stratégiques. »

Traiter la fragilité structurelle de la fibre dans une approche multidimensionnelle

La sécurité physique contre le vandalisme doit être accrue avec une protection différenciée – un simple boîtier de rue n'a pas la même criticité qu'un NRO ou un pylône – ; la sécurité contre les cyberattaques doit être renforcée par des plans de continuité et de reprise d'activité robustes ; la sécurité environnementale doit protéger des aléas extérieurs les équipements et l'alimentation électrique. « La tempête Alex, la catastrophe de Mayotte, les inondations de Valence, la grande panne de courant de 2025 en Espagne et au Portugal, nous ont appris que sans électricité, une antenne intacte ne sert à rien. »

Déployer un bouclier de connectivité

Suite à la tempête Alex en 2020 dans les Alpes-Maritimes, la Métropole Nice-Côte d'Azur a expérimenté, entre 2021 et 2023, un réseau radio maillé, complémentaire des réseaux opérateurs, autonome en énergie, capable de créer une bulle de communication terrestre pour les services d'intervention de secours et les concitoyens. Des valises tactiques mobiles, activables en 10 minutes, créent des points d'accès Wifi connectés par satellite. En 2025, ce type de réseau va se généraliser en priorisant les 21 communes de la vallée de la Vésubie exposées aux risques de tempêtes.

Les angles morts de la résilience des réseaux

Les raccordements complexes et les poches de basse densité dans les zones très denses sont souvent les grands oubliés des grands plans de déploiement. Le droit au raccordement à la demande, prévu en zone AMII, doit être étendu pour une question d'équité territoriale. Il faut anticiper dès maintenant l'identification des logements qui ne seront jamais raccordés à la fibre pour des raisons techniques ou économiques, et leur garantir une solution alternative performante. De plus, la sénatrice s'interroge sur la robustesse physique du réseau fibre optique. « En zone collinaire et de montagne, l'ajout de câbles fibre exerce une contrainte mécanique sur les infrastructures support existantes (câbles détendus, poteaux inclinés). Le délais de réparation par les opérateurs peut dépasser les six mois. Une surveillance et un audit de l'état des infrastructures doivent être organisés. »

Ne pas créer une cybersécurité à deux vitesses

NIS 2 va étendre les obligations de cybersécurité à de très nombreuses collectivités, y compris les plus petites communautés de communes, lesquelles n'ont ni les moyens, ni l'ingénierie, ni les budgets pour y répondre. La sénatrice suggère de mettre en place **un Fonds de résilience numérique** pour les soutenir dans le déploiement de solutions palliatives, en conformité avec les exigences de cybersécurité. Dès septembre 2025, elle va formuler des propositions législatives pour tendre vers une réactualisation régulière des **Schémas directeurs territoriaux d'aménagement numérique (SDTAN)**, en intégrant un volet résilience pour organiser les solutions palliatives de manière coordonnée et évolutive.

TABLE RONDE 1

INFRASTRUCTURES DU NUMÉRIQUE : NOUVEAUX GARANTS DE L'INDÉPENDANCE ET DE LA SÉCURITÉ DE LA FRANCE

Modération : Roland MONTAGNE, principal Analyst FTTH, Broadband Markets, IDATE

Intervenants :

Zacharia ALAHYANE, membre du Collège, ARCEP
Ilham DJEHAÏCH-MEZOUAR, présidente d'InfraNum
Philippe MOUTHON, CTO Mobile Networks Europe Nokia
Soline OLSZANSKI, directrice stratégie et développement de Ielo
François VERGNET, directeur Marketing et Commercial de Terralpha

Selon l'Idate, les voyants sont au vert en termes de déploiement du FTTH. La France est n°1 en Europe en nombre de foyers raccordables (28 millions) devant l'Angleterre et l'Italie, n°1 en nombre d'abonnés (24 millions), soit la plus forte croissance en un an (+3 millions), et son taux de couverture en fibre optique (90%) est bien au-dessus de la moyenne européenne (69%). Ce « succès commercial » place la France n°3 en Europe, avec un taux d'adoption de 84% (en septembre 2024). Roland Montagne souligne cependant des « points de fragilité » autour des infrastructures numériques : interruptions, aléas climatiques, cyberattaques ou complétude... Comment les rendre plus résilientes ?

Responsabiliser les exploitants de réseau, les préfectures et les collectivités

Pour l'Arcep, la résilience s'appuie sur trois piliers : la sécurisation du réseau, l'anticipation des risques, et une gestion de crise adaptée. Depuis 2021, la loi Climat et Résilience permet aux préfets des zones de défense et de sécurité d'exiger des exploitants de réseaux un plan de résilience (diagnostic des vulnérabilités, mesures en cas de crise, procédures de remise en état...). Zacharia Alahyane ne saurait dire si un préfet a déjà mobilisé cette disposition. « La multiplicité des acteurs et des schémas complexifie la coordination : plusieurs opérateurs cohabitent en zone très dense, il y a un acteur différent dans chaque zone AMII ou AMEL, et différents schémas en zone RIP (DSP concessive ou d'affermage)... » À cela s'ajoute l'hétérogénéité du risque climatique selon les régions. La Direction générale de la sécurité civile et de la gestion des crises (DGSCGC) a en charge les plans ORSEC-RETAP-RESEAUX en cours d'actualisation. « Charge à chaque préfecture de l'adapter à son territoire. » L'Arcep appelle les collectivités délégantes, les préfectures et les opérateurs à se saisir

du guide « Élaborer son schéma local de résilience » (Banque des Territoires - ANCT).

Sur un plan plus technique, **la sécurisation du réseau** doit garantir une continuité de service. Cela passe par l'architecture (bouclage, redondance), la réduction de l'exposition aux risques (déplacer un NRO), et ponctuellement par de l'enfouissement. Ces choix, qui figurent dans le plan de résilience, ont une dimension politique. Le rétablissement d'un réseau en deux ou dix jours exige des niveaux d'investissement différents. Un réseau bien construit sera plus résilient.

Chez ielo, opérateur télécoms, **la résilience repose sur le design du réseau et les process opérationnels**. « Une boucle locale mutualisée aura plusieurs types de fragilités (armoires de rue, absence de redondance, de garantie de diversification de parcours et de temps de rétablissement...) puisque chacun des opérateurs n'a pas la main sur sa propre infrastructure », explique Soline Olszanski. « Une infrastructure déléguée à un tiers va empêcher la maîtrise totale du réseau. » Le type de raccordement va déterminer le niveau de résilience et les opérations de remédiation. « **Sur la couche physique, les leviers reposent sur des parcours diversifiés, dans des infrastructures maîtrisées, tracées, identifiées, pour pouvoir agir.** » Au niveau du routage, la capacité de diversifier est plus forte. Pour autant, les attaques cyber sont plus faciles à travers la couche IP et certains types d'équipement. Au niveau applicatif, le chiffrement opéré par un tiers offre un niveau de résilience optimal. « **Sur le design, tout dépend de la destination de l'équipement, du réseau et de la fiabilité réelle par construction.** »

La cartographie des risques

Les chiffres inquiètent. En 2024, 50% des banques européennes ont été la cible d'une cyberattaque pour un montant moyen de 6 millions €, indique Soline Olszanski. Le secteur public a été la cible de 19% des attaques, le secteur du transport 10%. Sur la partie opérationnelle (exploitation et gestion des crises et incidents), la cartographie des risques reste la meilleure des protections préventives, à condition qu'elle soit « **hiérarchisée en fonction du type de réseau** ». Qui agit, où, et comment on se coordonne ? Soline Olszanski insiste sur « la nécessité d'un inventaire et d'une traçabilité sur les couches physiques et logique du réseau, y compris sur les parties opérées par un tiers ».

La tarification d'offre de gros FTTH

À la fédération InfraNum, on affirme que les schémas de résilience ont été pris en compte dans la construction des RIP (sécurisation des réseaux, adduction des NRO, continuité électrique...) L'Observatoire de la Transition Numérique des Territoires (InfraNum, Banque des Territoires, Avicca) a recensé les infrastructures dans les zones à risques... Pour aller plus loin, Ilham Djehaïch-Mezouar avance deux propositions. La première concerne la tarification d'offre de gros FTTH : « 80% des territoires ont des surcoûts d'exploitation. Exploiter nos réseaux coûte plus cher parce qu'il faut plus maintenir, plus intervenir, plus auditer, plus rénover. » L'Observatoire de la TNT propose une feuille de route que la Cour des Comptes a confirmée à travers deux recommandations : « **que l'ARCEP objective les coûts dans les RIP, en donne une feuille de route à fin 2025, pour faire évoluer les coûts d'exploitation à la hauteur des investissements.** »

La seconde proposition concerne les datacenters de proximité. « La stratégie d'hébergement des données et des services est extrêmement structurante. La proximité des datacenters auprès des entreprises, des acteurs et des opérateurs est garante de la sécurité et de la souveraineté, et présente un moindre risque de dégradation. Il faut **limiter l'éloignement géographique des datacenters et developer les datacenters de proximité afin d'être moins dépendants des grands datacenters en France.**" À la rentrée, Infranum publiera un guide sur les datacenters de proximité.

Les datacenters face aux cyberattaques

Chez Nokia, on estime que le mouvement vers le cloud va prendre 5 à 10 ans, le temps de servir les usages de cloud et d'IA sur toutes les couches réseau, et de migrer l'accès 5G vers les clouds de proximité. Point important : la cloudification des fonctions réseau fixe et mobile. « Faire tourner des plateformes réseau dans des clouds privés chez les opérateurs suppose une protection contre les cyberattaques », souligne Philippe Mouthon. Nokia y travaille, en partenariat avec les opérateurs et l'ANSSI. Mais tout cela prend du temps. « Lorsqu'on anticipe, c'est très important de travailler dans la stabilité, avec des partenaires de confiance, dans des relations de long terme. »

Des datacenters de plus en plus interconnectés

Avec l'arrivée de la 6G, les smartphones vont embarquer de plus en plus d'IA et vont collaborer avec des datacenters d'IA. Cette « logique d'interconnexion » entre les smartphones et les datacenters, et les datacenters entre eux, appelle un « métier de routage » beaucoup plus sophistiqué, avec des mécanismes de résilience. Nokia opère actuellement cette transformation avec les opérateurs. « Grâce à l'IA, on est déjà capable de détecter des pannes deux jours à l'avance (à partir de signaux faibles) et de les résoudre. »

Au-delà de la maintenance prédictive, l'équipementier a d'autres sujets à traiter. Pour empêcher **l'informatique quantique** de casser des codes de cryptage considérés aujourd'hui comme sûrs, Nokia va intégrer dans la couche de routage IP et optique des algorithmes d'encodage *Quantum Safe*. Par ailleurs, les technologies mobiles du 3GPP se propagent vers des **usages militaires et de sécurité.** Nokia a noué des partenariats très lourds pour fournir des équipements tactiques, en 2024 avec Lockheed Martin (pour équiper le corps des marines et des forces spéciales américaines), en 2025 avec l'italien Leonardo. Dernier point : **le réseau 5G et la gestion des usages stratégiques**. « On sait faire faire des tranches fines de réseau 5G avec des qualités de service dédiées, indique Philippe Mouthon. Nous allons étendre les cas d'usage à la gestion de flux logistiques comme l'acheminement de la nourriture ou de l'eau dans les territoires. » Depuis 5 ans, Nokia a également investi lourdement dans le traitement du signal de routage afin d'accroître les performances et de se protéger contre les cyberattaques. Au début, ses clients n'en voyaient pas l'intérêt, mais « depuis la guerre en Ukraine, cette capacité est utilisée ».

Pour clore cette discussion, François Vergnet présente **Terralpha**, opérateur d'infrastructure télécom de la SNCF depuis 2021. Ce réseau en propre, au tracé optimisé le long des voies ferrées, assure une indépendance et une qualité de service qui placent « la performance, la résilience et la souveraineté au cœur des enjeux ». Au plan de la **sécurité**, la SUGE (surveillance ferroviaire), les drones et la

vidéosurveillance surveillent les 20 000 km de fibre optique en permanence. Au niveau d e **l'architecture**, Terralpha opère un réseau optique DWDM conçu en redondance (boucles) avec des mécanismes de restauration automatiques pour assurer la continuité de service. Enfin, **l'exploitation** est supervisée au NOC interne à Paris 24/7, aidé de la force de frappe des équipes de la SNCF sur le terrain en cas de fibre brûlée (par un incendie) ou arrachée (des pieds nickelés s'imaginent encore que c'est du cuivre !). Des équipements en bordure d'emprise ferroviaire permettent de repérer une coupure réseau « au mètre près ».

De g. à d. : Roland MONTAGNE, François VERGNET, Zacharia ALAHYANE, Ilham DJEHAÏCH-MEZOUAR, Philippe MOUTHON, Soline OLSZANSKI.

SESSION 2

Introduction COMMENT MAÎTRISER LES FONDS MARINS ?

Vice-Amiral Marc-Antoine LEFEBVRE de SAINT-GERMAIN, responsable de la transformation digitale de la Marine

La guerre en Ukraine a fermé une pose stratégique de trente ans durant laquelle les espaces communs tels que les fonds marins, les espaces maritimes et satellitaires étaient peu régulés. Aujourd'hui, ils redeviennent des enjeux de rapports de force entre les Etats, et donc de sécurité. Toute la région indo-pacifique est en train de se réarmer par des flottes sous-marines et de navires militaires. En 2022, le sabotage des gazoducs Nord Stream en mer Baltique a rappelé qu'à moins de cent mètres de profondeur, on peut fragiliser la souveraineté de l'Europe. Après ce bref tableau géopolitique, le Vice-Amiral se concentre sur l'importance stratégique des câbles sous-marins : on en compte 560 systèmes dans le monde ; l'Internet mondial surfe sur 1,3 million km de câbles, dont le débit a été décuplé depuis 2011. Le récent câble transatlantique AMITIE déployé par Orange Marine, d'une longueur totale de 6 800 km, avec 16 paires de fibre, aura une capacité maximale de 400 Tbit/s. C'est colossal ! Les « autoroutes de la donnée » que sont les câbles sous-marins impactent fortement tout l'écosystème Donnée-IA-Datacenters, dont les GAFAM ont le

monopole. Orange Marine va augmenter la pose de câbles parce que les GAFAM ont besoin d'accéder à la donnée, parce que l'IA tire l'accès à la donnée. La dépendance aux opérateurs privés américains est réelle. C'est toute la géopolitique de la donnée Francfort-Londres-Amsterdam-Paris qui est remise en question.

« Pour avoir la maîtrise des fonds marins, nous devons comprendre ce qui se passe sous l'eau, surveiller et intervenir. »

Chaque année, les pertes de câbles sous-marins sont multipliées par deux. Pour se prémunir du sabotage ou de l'arrachage de câbles par des chaluts, la France a opté pour une stratégie de maîtrise des fonds marins. « La France va s'équiper pour descendre jusqu'à 6 000 mètres de fond avec des objets téléopérés ou des drones autonomes. » Comprendre, surveiller et intervenir, telle est la doctrine. Pour s'en convaincre, l'OTAN, après l'entrée de la Finlande et de la Suède, a décidé d'opérer en mer Baltique l'expérimentation TFX en 2025, en déployant 70 drones, dont une trentaine sous-marins, pour contrôler la Baltique. De son côté, le Portugal a décidé de réinvestir dans des câbles sous-marins étatiques avec le Brésil. « Comment reprendre la main sur ces câbles quand on sait que 70% des datacenters sont américains ? Le Cloud Act [qui permet aux autorités judiciaires américaines d'accéder aux données électroniques stockées à l'étranger par des entreprises américaines] n'est pas qu'un bout de papier ! **Une des possibilités serait de ramener les datacenters et les câbles sous-marins dans les outre-mer... »**

TABLE RONDE 2

RÉSEAUX SOUS-MARINS ET SATELLITAIRES : DES ARMES GÉOSTRATÉGIQUES

Modération : Ludovic PROVOST, directeur des affaires publique, Sogetrel
Intervenants :
Valérie ABRELL DUONG, Chief Digital & Operation Officer du Comité International de la Croix-Rouge
Yohann BENARD, directeur des affaires publiques Europe, Digital, Amazon
Sandrine LAFONT, expert en télécommunications par satellite – marchés, services et usages, CNES
Etienne LESOEUR, head of institutional affairs, Eutelsat
Stella MORABITO, déléguée générale de l'AFNUM

Le déclic de la guerre en Ukraine a révélé le besoin d'une connectivité souveraine dans les mers et dans l'espace. Le spectre est une ressource finie, rappelle Etienne Lesoeur. Face à la montée en puissance des constellations américaines (déjà 7000 satellites Starlink et la moitié annoncée par Kuiper) et chinoises (Constellation Mille Voile pour le commerce, Guowang pour le gouvernement), Eutelsat-OneWeb fait figure de résistant en Europe avec 650 satellites exploités en orbite basse à 1200 km d'altitude. « On a besoin de moins de satellites parce qu'on est plus haut », précise Etienne Lesoeur.

La concurrence est rude. Yohann Benard annonce qu'Amazon lance actuellement sa constellation Kuiper qui va regrouper 3200 satellites en orbite basse à environ 600 km de la terre. Contrairement aux satellites géostationnaires (36000 km), il n'y a pas de latence. La communication satellitaire,

« indépendante », apporte de « la résilience en cas d'événement climatique majeur ». L'objectif est d'offrir « des services de communications complémentaires aux particuliers et aux entreprises, mais aussi à la marine ou l'aviation. Nous serons en capacité de sécuriser la connexion en situation de crise, notamment pour des associations humanitaires. »

Contrôler la « boîte noire » en cas de crise

Valérie Abrell Duong confirme la nécessité pour la Croix-Rouge de disposer de plusieurs solutions back-up. « Le CICR est présent dans une centaine de contextes de conflits armés. La connectivité est essentielle. Les satellites en orbite basse sauvent beaucoup de vies, malgré leur interdiction dans certains pays (Myanmar, Soudan). » Elle souligne aussi que c'est une « boîte noire ». « Le CICR, neutre par essence, ne peut pas se permettre d'avoir des backdoors dans ses infrastructures. La fuite de données et le risque de coupures sont réels. » Le CICR est en lien avec un centre de recherche cyber au Luxembourg pour obtenir une autonomie et une confidentialité maximales. Mais selon elle, c'est le déploiement de satellites en orbite basse pour l'Europe qui va « rétablir l'équilibre géopolitique et garantir la neutralité ».

IRIS²: 280 nouveaux satellites européens d'ici 2030

Outre ses 650 satellites en orbite, Eutelsat Group est partie prenante du partenariat public-privé IRIS² pour developper 280 satellites. Le budget total de 10,6 Md€ est financé à hauteur de 60% par l'UE et 40% par le consortium SpaceRISE (SES, Eutelsat, Hispasat). Eutelsat participe à hauteur de 2,2 Md€.

Pour Sandrine Lafont, il ne fait aucun doute qu'IRIS² va permettre à l'Europe de disposer d'une « connectivité sécurisée et sous contrôle souverain » pour « servir le secteur commercial et les utilisateurs gouvernementaux autorisés ». Le CNES accompagne ce programme de nouvelle infrastructure satellitaire, ainsi que le programme GovSatCom basé sur des infrastructures existantes. Une partie des capacités sera réservée à des « usages publics (missions de sécurité, interventions de secours, surveillance frontière ou maritime, infrastructures vitales des Etats) ». Tout le système (continuité de service, disponibilité et sécurité des données) sera à la main de l'Europe. « Il n'y aura pas de chantage à la continuité de service, comme l'a fait Starlink en Ukraine. Le trafic des données sera contrôlé depuis le territoire européen continental, avec quelques stations complémentaires en Outre-mer pour le contrôle permanent des satellites. Ce qui n'est pas le cas de Kuiper ou de Starlink, qui ne sont pas sous contrôle européen. »

La résilience industrielle

Yohann Benard réagit. « La souveraineté n'est pas une question de propriété, c'est la capacité de décider. Pour cela, il faut avoir les moyens financiers et les infrastructures disponibles, et faire en sorte que ces infrastructures soient résilientes. » Et de donner l'exemple des câbles sous-marins : « Ils sont privés et toute la data passe par ces câbles, y compris les plus confidentiels qui sont protégés par des systèmes de chiffrement. » Une constellation de satellites contribue à la résilience parce que c'est « une option supplémentaire et donc une capacité de choix supplémentaire », et aussi parce qu'elle participe à la « résilience industrielle ». Dans le cadre du projet Kuiper, « Amazon a contracté avec quatre lanceurs, dont Arianespace pour jusqu'à 18 lancements. C'est le plus grand contrat

de toute son histoire dixit le PDG d'Ariane. Cette entreprise française est présente dans 13 pays européens, avec plus de 600 sous-traitants. Ces lancements vont irriguer toute l'industrie spatiale européenne. »

Quelle souveraineté dans une industrie mondialisée ?

L'AFNUM, qui regroupe des composantiers sur réseaux mobiles, des équipementiers télécoms, des fabricants de flottes de satellites ou d'infrastructures pour les datacenters, a une vision systémique. « Que ce soient les satellites ou les câbles sous-marins, ils sont repris sur des réseaux terrestres fixes (fibre) ou mobiles (5G) », souligne Stella Morabito.

S'il est vrai que 99% du trafic international emprunte les câbles sous-marins, les flottes de satellite apportent une résilience, la possibilité de pallier d'éventuelles pannes. « Cette infrastructure s'articule au niveau terrestre avec des datacenters, dont l'interconnexion est une question cruciale. » La résilience s'établit à la fois par redondance des voies de transmission (câbles sous-marins, satellites) et par des points de transit au niveau terrestre, c'est-à-dire tous les backbones fibre régionaux et les routes alternatives intra-européennes. Il y a aussi la possibilité de faire prendre le relais à des datacenters régionaux ou des datacenters miroirs. Sur la partie mobile, la 5G Standalone permet de créer des tranches (slices) dans les tuyaux de transmission qui peuvent héberger des applications critiques (santé, industrie...) parfaitement sécurisées.

Le message de l'AFNUM est clair : « **Le secteur de l'électronique est globalisé depuis 50 ans ».** Dans le numérique, le partenariat entre Nvidia et Mistral AI annoncé à VivaTech 2025 en dit long. Les 18 000 puces que Nvidia s'engage à fournir à Mistral AI vont permettre au concepteur d'IA générative de « préempter toute la chaîne, en collaboration avec les meilleurs pour son usage et pour le service souverain qu'elle va fournir à toutes les sociétés françaises et européennes. » À l'AFNUM, on se réjouit aussi des 109 Md€ d'investissements annoncés par la France lors du Sommet sur l'IA en 2025 pour la construction de datacenters de toutes tailles. Les Emirats arabes Unis sont le premier financeur (50 Md€), suivi des États-Unis (21 Md€), Canada (20 Md€), Royaume-Uni (10 Md€), etc. « Au niveau financier, la territorialité n'existe pas. »

Bientôt un « emblème digital »

Au CICR, on milite pour « continuer à investir sur nos propres datacenters » et « limiter le Move-to-Cloud pour des données non confidentielles ». La boîte noire encore. « On ne sait pas où sont stockées les données dans le cloud. Il faut réfléchir au maillage des datacenters de manière stratégique », explique Valérie Abrell Duong. Actuellement, le CICR développe un « emblème digital ». Ce standard international (signé par toutes les Big Tech) a été validé en octobre 2024 dans le cadre des convention internationales de la Croix-Rouge avec tous les pays membres. « Nous sommes dans la phase d'implémentation technique. D'ici un ou deux ans, chaque pays aura alloué des codes qui vont protéger les serveurs où opèrent les SI vitaux, comme des hôpitaux par exemple. »

Pour un espace durable

En droit international, que se passe-t-il si un satellite est détruit ?

demande **Ludovic Provost**. Selon le Traité sur l'espace signé en 1967, l'espace n'appartient à personne, rappelle Valérie Abrell Duong. « Il est interdit de détruire militairement des satellites. Ce cadre s'applique aujourd'hui mais il doit évoluer. » Les tirs de missiles ASAT (*anti satellite activities*) par les Russes, les Américains ou les Indiens font dire à Etienne Lesoeur que le droit international ne prend pas en compte la paix dans l'espace. « Plus d'un millions de débris de moins d'un centimètre flottent dans l'espace. Sans surveillance, il y a un risque de collisions. Les constellations sont proches en orbite (Starlink et Amazon), les Chinois seront quasiment à la même hauteur qu'Eutelsat... Tout cela exige de la coordination, sinon les débris entraîneront d'autres débris, jusqu'à épuisement. C'est ce qu'on appelle « le syndrome de Kessler ».

De g. à d. : Stella MORABITO, Yohann BENARD, Valérie ABRELL DUONG, Sandrine LAFONT, Etienne LESOEUR.

SESSION 3

Introduction **HYBRIDATION DES RÉSEAUX, DÉMATÉRIALISATION ET RÉGULATION À L'ÉPREUVE DES MUTATIONS NUMÉRIQUES**

Pierre-Jean BENGHOZI, directeur de recherche au CNRS, professeur à l'École polytechnique et à l'Université de Genève, président de la mission d'évaluation du plan France Très Haut Débit

Le Pr Pierre-Jean Benghozi dresse un panorama éclairant des transformations majeures à l'œuvre dans le secteur des communications électroniques. Sa présentation articule les bouleversements technologiques, économiques et réglementaires autour de trois dynamiques clés : la dématérialisation, l'hybridation technologique des réseaux, et la nécessaire refondation des cadres de régulation.

Des réseaux hybrides et flexibles, moteurs d'une transformation systémique

Le marché du numérique est en pleine mutation. L'hybridation des réseaux ne se limite

plus à la seule convergence fixe-mobile. Elle intègre désormais le satellite, les grands câbles sous-marins, les réseaux privés et publics, fixes ou mobiles, dans une approche systémique. La logique n'est plus celle de réseaux cloisonnés, mais d'un système de systèmes, capable d'interopérer à différentes échelles (locale, nationale, continentale).

Cette dynamique accompagne une mobilité accrue des usages (notamment entre postes fixes et terminaux mobiles) et repose sur des technologies multiples : slicing, agrégation de porteuses, MIMO, Cloud RAN, device-to-device, mobile edge computing, etc. — qui permettent d'assurer la flexibilité et le désilotage des applications dans des architectures intégrées. Cette souplesse s'étend à la gestion fine des segments de marché mais le passage à l'échelle reste difficile et l'identification de cas d'usage concrets devient cruciale, dans les secteurs industriels ou grand public, anticipés (ports, usines), émergents (logistique, voitures connectées) ou inédits (réseaux autonomes, désintermédiés).

La 5G, d'abord envisagée comme un levier de désengorgement pour la 4G, trouve ainsi sa réelle valeur dans des applications industrielles (débit élevé, faible latence, densité de connexions). Pour le grand public, l'intégration de l'intelligence artificielle renforce la sensibilité à la latence et déplace les besoins vers des débits ascendants, jusqu'ici peu valorisés.

Dématérialisation et virtualisation : une reconfiguration en profondeur

La montée en puissance de l'intelligence artificielle et la virtualisation des fonctions réseau (NFV) transforment en profondeur la gestion des infrastructures, affecte le cœur des réseaux et redessine la chaîne de valeur des opérateurs. La virtualisation des fonctions de gestion (NFV) permet désormais d'administrer les réseaux sur des matériels informatiques standards, abolissant la nécessité d'équipements dédiés. Cela rend les réseaux plus malléables, polyvalents, reconfigurables et aux modèles économiques plus variés.

Cette virtualisation rebat ainsi les cartes économiques en brouillant les frontières traditionnelles entre segments (grand public / entreprises), entre types de connectivité (fixe vs. mobile) et entre types d'opérateurs (intégrés, MVNO, VNO, opérateurs de proximité…). Elle renforce aussi l'importance du logiciel, désormais stratégique, au détriment des équipements spécifiques (semi-conducteurs génériques). L'intégration croissante entre opérateurs, équipementiers, fournisseurs de services et plateformes OTT rend plus complexe le partage de la valeur et pose de nouveaux défis pour le financement des infrastructures.

Une régulation à réinventer face à la complexité croissante des écosystèmes

La régulation ne peut rester figée face à ces mutations. Si les missions fondamentales des régulateurs demeurent — garantir l'interconnexion et la transmission des données — leur déclinaison devient plus complexe et diversifiée pour s'adapter à des acteurs aux profils très variés (opérateurs, plateformes OTT, développeurs de logiciels, intermédiaires de données…), aux logiques économiques et capacités d'investissement hétérogènes. Le Pr Benghozi souligne, à cet égard, plusieurs axes des transformations à repenser.

Il convient d'abord de repenser la régulation autour de la connectivité et du THD, et non plus des seules infrastructures physiques. Le rapport Draghi sur les infrastructures intégrées illustre ce besoin de coordination transversale. Il s'agit ensuite de l'articulation des niveaux européen, national et local : la résilience et la sécurité des réseaux exigent une coordination continentale, mais aussi une structuration par le local, en lien avec les territoires. Cela suppose de réinterroger les logiques de consolidation et de souveraineté : faut-il porter l'attention sur les opérateurs nationaux, les infrastructures de cœur de réseau, ou les services ? Quel sens a encore la concurrence par les infrastructures dans un univers où fibre, virtualisation et mutualisation sont la norme ? On peut également s'interroger sur les opportunités d'adapter la définition de la neutralité du net, à l'ère des services redondants, du slicing, et des applications BtoBtoC. Comment garantir un équilibre entre les acteurs de la chaîne de valeur d'Internet quand contenus, réseaux et services sont intégrés et hybrides ? Enfin, l'enjeu est de renforcer la gouvernance des données : la virtualisation rend opaque la circulation des données, multiplie les sources de collecte et interroge la sécurité des flux, notamment à l'ère de l'IoT ou des applications critiques. Les métriques, encore trop opaques, constituent un point de vigilance pour les régulateurs (ARCEP, CNIL…), à l'instar de ce que posent les enjeux liés à l'IoT ou à la défense.

La soutenabilité, nouvelle frontière de la régulation

Enfin, la soutenabilité environnementale s'impose comme une priorité et dimension à part entière de la régulation. Le numérique représente entre 2 % et 4 % des émissions mondiales de GES. Il ne s'agit plus seulement d'inciter à la sobriété ou à l'écoconception, mais bien d'intervenir au cœur des dispositifs structurels : encourager la mutualisation des infrastructures et le partage de données, évaluer systématiquement les impacts environnementaux des choix d'équipement, privilégier les réseaux sobres (notamment la fibre), limiter le renouvellement des terminaux, principale source des émissions du secteur.

TABLE RONDE 3

RUPTURES TECHNOLOGIQUES : VERS UNE NOUVELLE APPROCHE DE LA GESTION DES FLUX ET DES PERFORMANCES ?

Modération : Jean-Benoît ARVIS, membre du conseil scientifique de la Fondation Concorde
Intervenants :

Viktor ARVIDSSON, Head of Government Affairs, Innovation and Strategy, Ericsson France
Marie-Claude CHARLES, directrice des Investissements Data, confiance numérique & IA, Banque des Territoires · Groupe Caisse des Dépôts
Anne YVRANDE-BILLON, directrice économie, marché et numérique, ARCEP

Face à l'émergence de ce que Jean-Benoît Arvis qualifie de « marché du gros de la connectivité vendu comme une commodité d'ensemble », la doctrine de l'Arcep est de garantir le bon fonctionnement concurrentiel dans un esprit d'ouverture des marchés numériques et des systèmes d'IA, c'est-à-dire dans « **le respect de la neutralité du net, la contribution à la régulation des plateformes numériques et du marché des opérateurs de services cloud, et le contrôle des intermédiaires de données** », affirme Anne Yvrande-Billon. Au niveau du réseau des régulateurs européen (BEREC), l'Arcep a une

implication très forte dans la mise en œuvre de trois règlements : sur les grandes plateformes (DMA), sur les données (Data Act) et sur la gouvernance des données (DGA). Au sein de groupes d'experts, l'Arcep réfléchit au partage des données, en particulier à la « normalisation de l'interopérabilité ». Dans le cadre de la loi SREN de 2024, l'Arcep a de nouvelles compétences visant à sécuriser et à réguler l'espace numérique, notamment sur l'économie de la donnée et du cloud, en particulier sur « les services d'intermédiation de données ». L'objectif est de créer « un cadre de confiance pour faciliter les échanges de données ». Dernier volet : le cloud. Dans un contexte de forte concentration des opérateurs de cloud, l'Arcep cherche à « renforcer la concurrence ». Le but est « **d'éliminer certaines barrières tarifaires ou techniques d'interopérabilité ou de portabilité** ».

L'IA, catalyseur des besoins

« Dans une économie de la donnée, la gestion des flux et des performances doit répondre de plus en plus aux besoins de l'IA », estime Marie-Claude Charles. En tant qu'investisseur, la Banque des Territoires accompagne les collectivités et le secteur privé dans « une approche intégrée de la connectivité ». Son slogan : « **Pas d'IA sans infra ni data** ». Bien connue pour le déploiement des RIP 1ère et 2ème génération, la Banque des Territoires est en train de basculer dans les RIP 3ème génération qui prennent en compte les besoins en matière d'usages. Datacenters de proximité, réseaux bas débit de l'internet des objets, vidéoprotection, réseaux 5G privés pour l'industrie, couverture indoor... « Nous adressons à la fois tous les enjeux de connectivité des territoires – puisque les besoins s'accélèrent – et des enjeux plus globaux liés à la souveraineté », résume Marie-Claude Charles, qui donne l'exemple d'une expérimentation de réseau 5G dans un groupe hospitalier en lien avec la « criticité de la santé ».

Couverture mobile : le poids de la donnée

Du point de vue de l'équipementier Ericsson, les bénéfices de la 5G ont été progressifs. Depuis 2018, le trafic a été multiplié par 10 ; un tiers des utilisateurs mondiaux l'utilisent. En Chine et en Amérique du nord, plus de 90% de la population est couverte ; en Europe environ 50%. « La France est en avance, notamment grâce à l'Arcep qui impose des objectifs de déploiement dans ses licences. » Sur la chaîne de valeur, « l'évolution technologique permet de virtualiser, de cloudifier, d'automatiser la gestion des réseaux, ce qui interroge la place des opérateurs sur la mutualisation ou les TowerCo ». Viktor Arvidsson se dit « frappé » par « le poids de la connectivité ». Rappelant les mots du ministre – « la couverture est bonne » –, il ajoute que « la cible est mouvante ». Les besoins augmentent et la qualité de service n'est pas au rendez-vous. « On n'atteint pas les 30 Mb/s dans 50% des zones rurales et dans 20% des zones intermédiaires. »

Quel avenir pour la neutralité du net ?

« Grâce au slicing, on sait mieux prioriser les flux, mais comment le monétiser ? demande **Jean-Benoît Arvis**. La notion de neutralité du net ou d'égalité de traitement entre les différents flux ne doit-elle pas évoluer ? Aux États-Unis, elle n'existe plus depuis 2018. »

Pour l'Arcep, la neutralité du net est un principe fondamental qui n'est pas antinomique avec un contrôle et le slicing. « L'organisation concrète des slices et les éventuels effets sur la disponibilité ou la qualité doivent être examinés au cas par cas, précise Anne Yvrande-Billon, sous réserve que ces services n'affectent pas la qualité générale des services d'accès à Internet, ni ne soient proposés en remplacement de ces derniers. » La revue stratégique de l'Arcep continue à partager des éléments de doctrine pour « **concilier l'Internet ouvert et la fourniture de services spécialisés innovants** ».

Pas si simple. Dans ce jeu d'équilibriste, Pierre-Jean Benghozi considère que les services spécialisés, y compris la télévision sur Internet, passent sur la fibre mais sont traités différemment de l'accès général Internet. De même avec la vidéo, la publicité va arriver plus vite que le contenu parce que les opérateurs les gèrent différemment. « Avec des services et des réseaux de plus en plus complémentaires et intégrés, l'applicabilité de la neutralité du net a besoin d'être redéfinie dans ses fondamentaux. »

Viktor Arvidsson cite d'autres cas d'usage à équilibrer : les services régaliens de sécurité ou de défense, ou même de l'OTAN (qui ont vocation à se développer sur des tranches sécurisées des réseaux publics), l'accès fixe sans fil (il faut éviter qu'il étouffe l'usage mobile classique), et puis les cas d'usages grand public qui exigent une fiabilité de latence (achat de billets en ligne, transaction bancaire...). « **Sur la neutralité du net, il faudrait préciser la définition d'un service spécialisé, et à partir de quand je considère que je n'impacte pas la qualité de service sur l'accès internet ?** »

Comment garantir la résilience des réseaux ?

L'accès à la donnée induit un système complexe de multiples réseaux connectés aux datacenters et à l'IA pour fournir une seule commodité. Jean-Benoît Arvis s'interroge : « Comment s'assurer de la résilience de ces réseaux convergents ? »

Pour l'équipementier, **la résilience repose sur la redondance des réseaux**, à l'instar du GSM-Rail pour les trains par exemple. La question se pose avec acuité dans le cadre de la mutualisation. Certes, « on va réduire les coûts et l'empreinte carbone, mais quid de la redondance en cas de destruction d'un pylône ? » Viktor Arvidsson préconise « au moins deux réseaux distincts. Un réseau unique peut être aussi un frein pour l'innovation et la différenciation. »

Marie-Claude Charles croit beaucoup à « **la complémentarité et à la convergence** ». La Banque des Territoires accompagne l'ensemble des acteurs dans le financement des schémas locaux de résilience pour s'adapter aux spécificités.

Pour Anne Yvrande-Billon, il faut favoriser un marché concurrentiel sur tous les marchés d'intrants liés à l'accès aux données et à la connectivité, c'est-à-dire les capacités de calcul, les composants utilisés pour les serveurs, ou les ressources telles que les opérateurs de cloud. « **En assurant l'ouverture de ces marchés à la concurrence, on contribue à la résilience de l'accès aux données et de la connectivité.** »

En conclusion, Pierre-Jean Benghozi fait une adresse au régulateur : comment opérationnaliser les enjeux de

résilience, de soutenabilité ou d'empreinte carbone dans la régulation ? Soit on laisse agir la main invisible de la technologie et du marché dans un cadre de jeu fixé par la régulation, soit le régulateur agit de manière plus volontariste en privilégiant une technologie au détriment d'une autre...

De g. à d. : Pierre-Jean BENGHOZI, Anne YVRANDE-BILLON, Marie-Claude CHARLES.