ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Jeudi
16 avril 2026
Séance de 10 heures 30

Compte rendu n° 28

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à dix heures trente-trois.

M. le président Philippe Latombe. Madame la directrice générale du groupe Orange, je vous souhaite la bienvenue. La France – ses citoyens, ses entreprises, son administration – est dépendante de solutions et d'infrastructures numériques fournies par des opérateurs extra-européens. Quelles sont, selon vous, nos principales dépendances et vulnérabilités ? Quels risques celles-ci font-elles courir à l'État et, plus généralement, à l'économie ? Y a-t-il des remèdes ?

Avant de vous céder la parole, je vous remercie de nous déclarer tout autre intérêt public ou privé de nature à influencer vos déclarations.

Je rappelle que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter le serment de dire la vérité, toute la vérité, rien que la vérité.

(Mme Christel Heydemann prête serment.)

Mme Christel Heydemann, directrice générale du groupe Orange. Je vous remercie d'avoir souhaité entendre le groupe Orange dans le cadre de vos travaux. La question que vous posez, celle de nos dépendances numériques et de la souveraineté de la France dans ce domaine, est l'une des plus importantes qui soient pour notre avenir industriel, économique et stratégique. Je partage pleinement l'ambition qui a présidé à la création de cette commission, et je souhaite y contribuer avec franchise.

Permettez-moi de commencer par une proposition de cadre de lecture qui, je crois, conditionnera l'utilité de notre échange. La souveraineté numérique ne commence pas avec le *cloud* ; elle porte sur l'ensemble des couches technologiques, y compris les réseaux. Un *cloud*, même souverain dans ses statuts juridiques, ne l'est qu'autant que les infrastructures qui le portent le sont également – les fibres, les câbles sous-marins, les interconnexions de données et toute l'intelligence requise pour les opérer. Si ces couches physiques ne sont pas maîtrisées, il n'est pas de souveraineté numérique qui tienne.

C'est précisément sur ce socle, et sur les menaces qui pèsent aujourd'hui sur lui, que je concentrerai mon propos. Je serai évidemment heureuse d'évoquer notre stratégie *cloud* et nos offres de confiance au fil de vos questions, mais je voudrais commencer par établir ce qui, selon moi, mérite aussi d'être au cœur de vos recommandations.

Je vous proposerai d'abord un état des lieux de ce qu'est vraiment Orange : un opérateur d'infrastructures physiques, dont je vous décrirai les différents maillons – les réseaux d'accès mobile, les fibres, les cœurs de réseau, l'intelligence hébergée dans nos *clouds*, les câbles sous-marins, les infrastructures satellitaires. Je serai ensuite transparente sur nos propres dépendances, car sur ce point, la franchise me semble la condition d'une conversation utile. Je terminerai en évoquant les textes réglementaires européens en cours d'élaboration – le Digital Networks Act (DNA), le Cybersecurity Act (CSA) – et les enjeux de l'attribution des fréquences satellites qui, en l'état, menacent de fragiliser encore plus les acteurs qui portent les infrastructures dont dépend la souveraineté que vous cherchez à défendre.

Premier opérateur télécom intégré en France, Orange est également présent dans vingt-six pays, au service de plus de 300 millions de clients, particuliers et entreprises. Nous accompagnons par ailleurs les entreprises multinationales françaises et européennes dans plus de cent pays grâce à notre réseau IP mondial, Orange Global Network, qui irrigue 230 points de présence répartis sur tous les continents. Ce qui nous distingue de beaucoup d'opérateurs en France et en Europe, c'est notre nature d'opérateur d'infrastructures physiques. Alors que la majorité des opérateurs, parfois contraints par des raisons financières, ont cédé leurs infrastructures, notamment à des fonds, rarement français ou européens, nous avons fait le choix stratégique d'en garder le contrôle.

Premier maillon de notre chaîne d'infrastructure : les réseaux d'accès – le cuivre par le passé, désormais la fibre jusque chez l'habitant, nos antennes mobiles. Notre réseau fibre dessert 57 millions de prises en Europe, foyers et entreprises confondus. En France, nous sommes également propriétaires du génie civil – la boucle locale, les fourreaux souterrains, les poteaux aériens – sur lequel repose le déploiement de la fibre de l'ensemble des opérateurs. Cette infrastructure, que nous continuons d'entretenir, présente une valeur stratégique reconnue par tous les acteurs du secteur. Nous possédons enfin Totem, notre société de tours télécoms, propriétaire des 26 900 mâts qui supportent nos antennes mobiles, avec un ratio d'occupation en progression continue. S'y ajoutent nos propres *data centers*, opérés en France et en Europe, qui hébergent les données et les services de nos clients – entreprises et grand public –, ainsi que nos cœurs de réseau, l'intelligence et nos propres systèmes d'information, dans un environnement entièrement sous contrôle. Contrairement à d'autres opérateurs européens, nous n'avons cédé aucun de ces actifs. Ce choix a un coût, mais nous considérons que c'est une force.

Deuxième maillon : l'interconnexion, les réseaux internationaux et les dorsales longue distance. Nous opérons 600 000 kilomètres de fibres terrestres, et nous développons activement ce réseau pour répondre aux besoins croissants en capacité, notamment de la part des acteurs de l'intelligence artificielle (IA). C'est sur ce réseau que repose Open Transit, seul *backbone* IP Tier-1 d'un opérateur français, une dorsale qui relie l'Europe, les États-Unis, l'Afrique et l'Asie à travers 230 points de présence internationaux et sur laquelle les données transitent, sous notre contrôle et sans dépendre d'un tiers.

Troisième maillon : les câbles sous-marins, qui constituent l'épine dorsale des échanges numériques intercontinentaux. Orange exploite 450 000 kilomètres de fibres sous-marines reliant la France à tous les continents, soit plus de onze fois la circonférence de la Terre. Avec Orange Marine, nous disposons d'une flotte de six navires câbliers, auxquels s'ajoute un navire de reconnaissance de tracé, pour assurer en propre la pose et la maintenance de ces câbles. C'est une capacité industrielle quasi unique en Europe.

Quatrième maillon : nos infrastructures satellitaires. Nous n'opérons pas de satellites mais exploitons nos propres téléports et stations sol, qui constituent des points d'ancrage terrestre à la connectivité par satellite. C'est une capacité essentielle pour desservir les zones non couvertes par les réseaux terrestres et assurer la résilience de nos communications internationales. Orange a également engagé des investissements significatifs pour soutenir la filière spatiale européenne souveraine. Nous avons contribué au lancement de satellites de nouvelle génération aux côtés d'Eutelsat, Thales et Arianespace, dans une logique de filière. Dans cette même perspective, le programme Iris², porté par le consortium SpaceRISE, regroupant Eutelsat, SES et Hispasat, vise à doter l'Union européenne d'une constellation souveraine pour sécuriser les communications critiques des États. Orange y contribue en apportant le cœur 5G, la connectivité des stations au sol et une capacité d'hébergement stratégique à La Réunion, participant ainsi directement à l'architecture technique du système.

Mais Orange n'est pas seulement un opérateur de connectivité et d'infrastructures. Avec 700 chercheurs, un budget de recherche et développement supérieur à 600 millions d'euros par an et plus de 11 000 brevets actifs – ce qui fait de nous le premier opérateur européen en matière de propriété intellectuelle –, nous participons activement à la normalisation mondiale de la 5G, de la 6G et de la cryptographie post-quantique au sein du 3GPP (*third generation partnership project*), de l'ETSI (*European Telecommunications Standards Institute*) et de l'ITU (*International Telecommunication Union*). Orange co-construit les standards technologiques de demain. Plus de 2 000 entreprises dans le monde utilisent nos technologies sous licence, et nous avançons résolument vers l'indépendance logicielle pour certains éléments de nos *stacks*. D'ici à 2028, 80 % de nos fonctions réseaux internationaux seront « cloudifiées », contre 50 % aujourd'hui, et 30 % seront développés en *open source* ou en propre, contre 20 % actuellement. Nous construisons une véritable fabrique logicielle réseau pour réduire notre dépendance aux éditeurs de logiciels propriétaires. Nous ne subissons pas les standards américains, nous contribuons à les écrire et nous travaillons à nous en affranchir là où la souveraineté l'exige.

Ces différents maillons d'infrastructures forment une chaîne que peu d'opérateurs en Europe possèdent de bout en bout. Pour nous, la question de la souveraineté numérique se pose aussi s'agissant de ces infrastructures physiques, car sans elles, il n'est pas de *cloud* souverain qui tienne. Et sans opérateurs qui les financent et les maîtrisent, elles n'existent pas.

J'en viens à nos dépendances. Elles sont identifiées, assumées, mais risquent d'être aggravées par le cadre réglementaire. Orange n'est pas sans dépendances. Je veux vous le dire clairement, parce que la transparence sur ce point est la condition d'une conversation utile.

En matière de réseaux, nous dépendons de deux ou trois équipementiers pour notre réseau d'accès radio, dont deux sont européens. Nous surveillons attentivement l'émergence potentielle d'un nouveau fournisseur, mais la réglementation européenne pourrait aggraver encore nos dépendances, du fait du Cybersecurity Act – j'y reviendrai. Nos box grand public embarquent des *chipsets* intégralement fabriqués dans des fonderies taïwanaises, actuellement sous tensions géopolitiques. Nos câbles sous-marins de nouvelle génération sont de plus en plus captés par les investissements des grandes plateformes américaines, lesquelles dominent désormais le financement de nouvelles capacités mondiales. Et sur le marché satellite, la position hégémonique qui se dessine pourrait contraindre nos propres offres.

Mais nos dépendances ne s'arrêtent pas aux réseaux. Comme l'ensemble des grandes entreprises, et comme l'État lui-même, ainsi que vos auditions l'ont amplement documenté, Orange dépend des logiciels et des services *cloud* des grands éditeurs américains – Oracle, Broadcom pour ses licences, VMware, Microsoft, Tibco, RedHat, Atlassian. Ces dépendances sont réelles ; nous les gérons activement, nous négocions avec fermeté les conditions de renouvellement, nous développons des plans de sortie pour certaines, nous diversifions nos sources quand c'est possible, et nous développons des alternatives souveraines pour nos propres opérations réseau, comme notre *telco cloud* natif, que nous proposons aussi à nos clients entreprises. Je tiens à le souligner : les solutions que nous trouvons pour nous-mêmes, nous avons vocation à les mettre à disposition de nos clients.

Nous construisons Cloud Avenue, une solution certifiée SecNumCloud, pour les données les plus sensibles des acteurs publics et des opérateurs d'importance vitale (OIV). Avec Capgemini, vous le savez, nous avons conçu Bleu pour permettre aux entreprises et aux administrations d'accéder aux meilleures technologies du marché tout en étant protégées des lois d'extraterritorialité américaines. Orange Cyberdefense protège plus de

50 000 organisations contre les cybermenaces, avec des équipes et des centres de détection entièrement européens. Ce que nous faisons pour nous, nous essayons de le rendre disponible à l'écosystème.

Mais les enjeux de souveraineté doivent être pensés à l'échelle européenne. La fragmentation actuelle de l'Europe et l'absence de marché unique du numérique sont un frein réel, qui entraîne une perte de vitesse dans la durée. Plusieurs textes réglementaires européens en cours de finalisation sont par ailleurs susceptibles d'aggraver ces dépendances au lieu de les réduire. Permettez-moi de souligner un paradoxe général, qui pèse sur l'ensemble de nos capacités d'investissement : l'Europe proclame sa souveraineté numérique, mais elle élabore simultanément des textes qui fragilisent les acteurs qui financent les infrastructures dont cette souveraineté dépend.

Avant d'aborder certains textes sectoriels qui nous concernent directement en tant qu'opérateurs, je me dois de mentionner un phénomène transversal, qui touche l'ensemble des entreprises européennes et qui constitue, à mon sens, l'une des formes les plus pernicieuses de dépendance structurelle : l'accumulation des obligations de *reporting* et de conformité. Comme toutes les grandes entreprises françaises et européennes, Orange est soumise à un empilement de réglementations sectorielles, horizontales, verticales, nationales – CSRD (directive relative à la publication d'informations en matière de durabilité par les entreprises), CS3D (directive sur le devoir de vigilance des entreprises en matière de durabilité), Dora (règlement sur la résilience opérationnelle numérique du secteur financier), NIS 2 (directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union), taxonomie verte, Pay Transparency… Tous ces textes prévoient des états de *reporting* d'une granularité et d'un volume croissants.

Si nous partageons complètement leurs objectifs, plusieurs de ces obligations produisent des effets contreproductifs dans leur application actuelle. La directive Pay Transparency, par exemple, impose une publicité des écarts de rémunération. Sa transposition, mal calibrée, crée de la rigidité salariale et de la tension sociale, alors que l'objectif était précisément de les réduire. Or les acteurs américains, qui sont nos vrais concurrents pour les talents, n'y sont pas soumis.

Plus largement, nous sommes contraints de publier avec une précision croissante l'état de nos engagements fournisseurs et de nos politiques de ressources humaines. Ce faisant, nous livrons ces informations à des acteurs extra-européens, qui ne sont soumis à aucune obligation symétrique et profitent donc de cette transparence sans la subir. J'aurai l'occasion de revenir tout à l'heure sur un exemple particulièrement frappant de ce paradoxe, à savoir l'extension aux navires câbliers de l'ETS (*European trading scheme*), le système communautaire d'échange de quotas d'émission. Je le disais, les acteurs extra-européens bénéficient d'une transparence qu'ils n'ont pas à offrir en retour, dans des conditions de compétitivité que les simplifications annoncées dans le cadre du paquet Omnibus n'ont, dans les faits, pas encore substantiellement allégées. Nous subissons des lourdeurs administratives – bilans carbone détaillés fournisseur par fournisseur, audits de chaînes de valeur, rapports ESG (rapports sur les critères environnementaux, sociaux et de gouvernance) d'une complexité croissante – qui absorbent des ressources humaines et financières considérables et constituent autant de handicaps compétitifs au regard d'acteurs qui en sont exemptés.

Je ne demande pas que l'on renonce à ces objectifs, mais que la représentation nationale et le gouvernement portent à Bruxelles un message clair : la simplification réglementaire n'est pas une concession faite aux entreprises, mais une condition de la

compétitivité européenne. La réciprocité des obligations doit être au cœur de toute négociation sur les accords commerciaux et les règles d'accès au marché européen pour les acteurs extra-européens.

J'en viens à quatre textes qui nous concernent plus directement, en tant qu'opérateur de réseaux, et sur lesquels je voudrais formuler des attentes précises.

Le Digital Networks Act promeut une ambition que nous partageons : simplifier, harmoniser, approfondir le marché intérieur – comme l'avait proposé Mario Draghi dans son rapport –, soutenir l'investissement. En Europe, nous faisons face à un enjeu absolu de taille critique : la fragmentation, je l'ai dit, est une faiblesse structurelle. Mais si le DNA comporte des avancées réelles, notamment sur le spectre et les licences de longue durée, il manque sa cible sur l'essentiel : il ne traite pas l'équation économique du secteur et ne prévoit pas de mécanisme contraignant de rééquilibrage dans la chaîne de valeur numérique. Ainsi, les grandes plateformes, qui génèrent 50 % à 70 % du trafic sur nos réseaux, ne sont toujours pas tenues de contribuer à due proportion au financement des infrastructures qu'elles utilisent – une asymétrie qui s'accentue chaque année. Par ailleurs, le DNA ne simplifie pas la régulation télécom, initialement conçue pour des marchés en monopole, alors que nous opérons désormais dans un environnement multi-infrastructures fortement concurrentiel. L'accès *ex ante* généralisé doit céder la place à une régulation fondée sur la réalité des marchés locaux. Sans correction de ces asymétries, les opérateurs européens continueront d'investir sans retours suffisants, et la souveraineté des réseaux restera un vœu pieux.

Le Cybersecurity Act est tout aussi paradoxal. Là encore, l'objectif est complètement partagé. Nous investissons massivement dans la résilience de nos réseaux et Orange Cyberdefense, je l'ai dit, est le premier acteur européen en la matière. Mais la version actuelle du texte nous préoccupe profondément : en réduisant drastiquement le nombre d'équipementiers admissibles sur des segments critiques, sans analyse de matérialité ni de faisabilité, le CSA risque de nous placer entre les mains d'un nombre très limité de fournisseurs. En voulant réduire une dépendance, on pourrait en créer une autre, plus concentrée encore, et demander aux opérateurs d'en financer seuls le coût par des *swaps* d'équipements massifs, sans mécanisme de compensation. Une politique de sécurité qui affaiblit financièrement les opérateurs qu'elle prétend protéger affaiblit *in fine* la sécurité de l'ensemble. Nous demandons un principe de proportionnalité réelle dans les obligations et un mécanisme de compensation pour les coûts de *swap*, qui relèvent de décisions de politique publique et non de défaillances commerciales. La souveraineté ne se construit pas en réduisant l'assiette des équipementiers admissibles à un ou deux acteurs, aussi remarquables soient-ils.

J'en viens aux enjeux satellites. C'est au sujet des services satellites mobiles *direct-to-device* qu'interviendra probablement le test le plus sérieux de la cohérence stratégique européenne dans les dix-huit prochains mois. Starlink, adossé à Deutsche Telekom, annonce une couverture de 140 millions d'abonnés européens d'ici à 2028. Iris², l'alternative européenne, ne sera pas opérationnelle avant 2029 ou 2030 et n'embarque pas, à ce stade, de projet *direct-to-device* qui ne serait, en tout état de cause, pas disponible avant 2031 ou 2032. Dans l'intervalle, un acteur non européen, massivement subventionné, pourrait prendre une avance structurelle et irréversible sur le marché mobile européen en accédant directement aux clients finaux, en contournant les opérateurs de réseaux terrestres et en créant une dépendance dont il sera impossible de se défaire.

Or les signaux que nous recevons de la Commission européenne sur l'attribution de la bande 2 GHz sont préoccupants. La souveraineté est regardée comme un facteur favorable, mais

à la marge : ce n'est pas un critère d'éligibilité. L'accès *wholesale* est considéré comme un plus, mais pas comme une obligation. Ce n'est pas suffisant. Sur le *Mobile Satellite Spectrum* (MSS), le marché se joue *ex ante* : si les conditions d'attribution de la bande 2 GHz n'incluent pas des critères clairs de souveraineté et d'accès indirect pour les opérateurs terrestres, la souveraineté mobile européenne sera compromise avant même qu'Iris² soit opérationnel – et encore, si tant est que le programme embarque du *direct-to-device*…

Je terminerai par un exemple qui peut sembler technique, mais qui illustre mieux que tout autre la contradiction entre les ambitions proclamées et les décisions concrètes. L'extension du système ETS aux navires poseurs et réparateurs de câbles sous-marins créera une distorsion de concurrence dont les victimes seront quasi exclusivement les acteurs européens, à commencer par Orange Marine. Les navires basés dans un port de l'Espace économique européen devront acquitter des quotas d'émission, y compris pour des opérations menées hors d'Europe, tandis que leurs concurrents non européens, opérant sur les mêmes marchés mondiaux, n'y seront pas soumis. Les effets en chaîne sont prévisibles et documentés : relocalisation des stocks de câbles hors des ports européens, recours accru à des navires non européens pour les appels d'offres internationaux, pression contractuelle exercée par les grands donneurs d'ordre – dont les Gafam eux-mêmes – pour imposer des bases de maintenance extra-européennes, affaiblissement progressif d'une filière industrielle stratégique. Orange Marine et Alcatel Submarine Networks (ASN) se retrouveront face à un dilemme : perdre des marchés face à des concurrents dont les navires seront basés en dehors d'Europe, ou délocaliser leurs navires pour garder leurs marchés. En pratique, on ne décarbonera pas l'activité, on la déplacera hors d'Europe.

C'est l'illustration parfaite d'une politique qui, sous couvert d'un objectif environnemental parfaitement louable, manque sa cible et dégrade l'autonomie stratégique de l'Union dans un domaine où elle dispose encore d'atouts industriels réels. Si l'Europe veut rester souveraine sur ses câbles sous-marins, elle doit exclure les navires câbliers du champ de l'ETS, ou au moins adapter le dispositif avant son entrée en vigueur.

Votre commission arrive à un moment charnière. La France investit depuis des années dans une ambition de souveraineté numérique, mais celle-ci ne pourra se réaliser si les acteurs qui portent concrètement les infrastructures voient leur capacité d'investissement érodée par des textes européens qui ne prennent pas la mesure de l'équation économique réelle. Nous avons des demandes précises : que le Digital Network Act devienne un texte restaurant la capacité d'investissement du secteur, avec un mécanisme contraignant de contribution des grandes plateformes et une régulation proportionnée à la réalité des marchés ; que le Cybersecurity Act prévoie un principe de proportionnalité réelle dans les obligations de sécurité et un mécanisme de compensation pour les coûts de *swap* ; que le MSS prévoie des critères contraignants de souveraineté et d'accès *wholesale* dans l'attribution de la bande 2 GHz, car le marché ne se rattrapera pas après coup.

La représentation nationale est aujourd'hui pleinement éclairée sur la façon dont les investissements des opérateurs télécoms dans les réseaux du futur et leur souveraineté sont contraints, paradoxalement, par le cadre réglementaire même qui prétend les soutenir. Nous espérons que votre commission saura adresser au gouvernement et à la Commission européenne un message très clair sur ces sujets, et nous nous tenons à votre disposition pour contribuer à la construction de ces recommandations. Il n'est pas trop tard !

Nous ambitionnons d'être l'opérateur qui donne à la France et à l'Europe les moyens concrets de leur souveraineté numérique. Nous y investissons chaque année des milliards

d’euros. Ce que nous demandons en retour, c’est que le cadre réglementaire européen cesse de travailler contre ceux qui investissent dans les infrastructures dont dépend cette souveraineté.

M. le président Philippe Latombe. Le président du conseil d’administration d’Orange est aussi le président de la French-American Foundation. Selon un article du *Figaro* de décembre 2023, cette présidence permettrait de propulser Orange dans une autre dimension. Sachant que votre groupe est peu présent aux États-Unis, quel est le sens de cette représentation ? Ces liens influent-ils sur les décisions d’Orange ? Nos travaux portent sur la souveraineté : il est donc normal que je vous pose cette question en préambule.

Mme Christel Heydemann. Le président n’est pas le seul membre du conseil d’administration. Il n’y dispose d’ailleurs que d’une voix !

Vous imaginez bien que notre gouvernance est absolument étanche. Le conseil d’administration valide la stratégie d’Orange, mais son président, qui y siège en tant qu’administrateur indépendant – d’autres membres représentent les différents actionnaires, l’État ou les salariés –, n’intervient en rien dans la direction de l’entreprise.

J’en profite pour préciser que Jacques Aschenbroich, qui préside effectivement la French-American Foundation, ne sera plus président d’Orange à compter de la prochaine assemblée générale, en mai. Il sera renouvelé dans ses fonctions d’administrateur indépendant, mais en raison de la limite d’âge, il sera remplacé au poste de président du conseil d’administration par Frédéric Sanchez.

Mme Cyrielle Chatelain, rapporteure. Votre propos liminaire était très large. Certains sujets que vous avez abordés n’entrent pas directement dans le champ de nos travaux – je pense notamment à vos questionnements sur l’ETS, qui est un système complexe et mériterait un débat spécifique.

Vous avez indiqué qu’Orange co-écrivait les standards. Pourriez-vous nous donner quelques exemples, préciser la forme que prend cette contribution et expliquer les effets de ces standards ?

Au niveau européen, vous demandez la définition d’un objectif contraignant de rééquilibrage s’agissant du financement des infrastructures par les grands acteurs du secteur. J’imagine que vous avez réfléchi à une proposition plus complète. Pourriez-vous nous en dire davantage ?

Vous nous avez également alertés quant à l’attribution des fréquences satellites. Là encore, pourriez-vous être plus précise ? On voit bien l’effet de verrou une fois la dépendance installée.

Mme Christel Heydemann. Orange a largement contribué à écrire les standards des réseaux mobiles jusqu’à la 5G, et il prend activement part aux travaux sur la 6G. On l’a oublié, mais le GSM est né en Europe ; à l’époque, notre continent était leader mondial dans ce domaine. Mais ne nous y trompons pas : aujourd’hui, la Chine est en pointe dans l’écriture des standards de la 6G, et l’administration américaine a mis un point d’honneur à être en avance sur ce pays, tandis qu’en Europe, aucun cadre ni aucun plan n’ont encore été prévus. Les opérateurs européens n’ont, de toute façon, pas la capacité de peser, et les technologies n’existent pas encore – ces enjeux dépassent l’horizon 2030.

En outre, je l'ai dit, nous investissons dans la recherche, en particulier dans le domaine de la cryptographie post-quantique, qui comporte de nombreux enjeux de souveraineté et de sécurité pour toutes nos entreprises, nos administrations et notre société. Là encore, nous menons une bataille technologique contre les deux géants que sont la Chine et les États-Unis. La France a des cartes à jouer, mais la taille critique et les montants investis par ces deux puissances sont sans commune mesure avec ce qui est fait aujourd'hui en France ou en Europe. Nous détenons aussi de nombreux brevets en matière de vidéo sur les réseaux et terminaux mobiles, pour lesquels les numéros 1 et 2 du secteur, Apple et Samsung, nous versent des droits. Nous déposons donc des brevets, et nos investissements dans la recherche continuent de s'inscrire dans cette logique.

L'enjeu de ce que l'on appelle le *fair share*, c'est-à-dire l'équilibre économique entre nous et les grandes plateformes qui consomment 50 % à 70 % du trafic sur nos réseaux, c'est de faire en sorte que le modèle économique de ces dernières tienne compte de leur impact sur nos investissements. Or, aujourd'hui, leur modèle économique repose sur la croissance du trafic ; ce dernier augmente de 20 % par an sur nos réseaux mobiles, ce qui nous oblige évidemment à réaliser des investissements supplémentaires.

Le rapport de force est déséquilibré : ces plateformes sont cinq à l'échelle mondiale, alors qu'on compte déjà quatre opérateurs dans notre seul pays – rien qu'en Europe, on parle d'au moins quatre opérateurs dans chacun des vingt-sept États membres. Même si nous sommes le deuxième opérateur en Europe et en Afrique, nous n'en restons pas moins à la merci des plateformes ; certes, notre poids nous permet de discuter avec certaines d'entre elles, ce qui les a conduites à déployer des technologies qui réduisent le trafic, mais elles n'ont aucune incitation économique à le faire, et nous n'allons évidemment pas priver les consommateurs, les usagers, de nos réseaux. En raison du principe de neutralité du net, nous n'avons même pas le droit de brider ce trafic.

Nous proposons qu'il existe au moins un lieu d'arbitrage pour forcer le dialogue et les accords entre les grandes plateformes et les différents opérateurs. Le débat n'est pas uniquement européen : il existe aussi aux États-Unis, où ces plateformes contribuent à un fonds pour l'aménagement des réseaux télécoms en zone rurale, et en Asie. C'est un sujet mondial, qui dépasse largement notre seul secteur, mais nous regrettons que l'Europe ne l'inclue plus dans ses textes.

J'en viens à votre question sur les satellites. Nous avons la chance, en Europe, d'avoir des réseaux qui couvrent très bien la population, en particulier en France avec les réseaux fibre et mobile. Le marché ciblé par les constellations satellites ne serait que complémentaire, mais nous sommes très proactifs et avons déjà lancé des offres. Nous voulons proposer la connectivité satellite en complément des réseaux terrestres, car c'est la promesse de la connectivité partout.

Pour éviter la dépendance, puisque c'est là tout l'enjeu, il faut que nous disposions de plusieurs solutions, dont une européenne. Alors que nos partenaires historiques, comme Eutelsat, sont géostationnaires et peuvent donc intervenir à l'échelle européenne, les constellations basse orbite marquent une rupture, parce qu'elles sont, par nature, mondiales. Or la capacité à les rentabiliser sur le marché américain est sans commune mesure avec ce qui est possible sur le marché européen. D'une part, le niveau des prix des offres télécoms sur le marché américain est bien plus élevé qu'en Europe ; nous n'allons pas le déplorer, car c'est très bien pour le pouvoir d'achat et la compétitivité européenne, mais cela crée un espace de marché bien plus grand outre-Atlantique. D'autre part, la couverture des réseaux y est bien inférieure à

celle que nous avons en Europe, ce qui signifie que les opérateurs américains – Starlink, mais aussi Amazon, qui est dans la course et vient d'annoncer le rachat de Globalstar – risquent de rentabiliser leurs constellations sur le marché américain avant de couvrir l'intégralité de la planète pour un prix marginal. Il s'agit donc d'un enjeu mondial essentiel.

M. le président Philippe Latombe. Eutelsat vient d'annoncer une augmentation de capital. Pourquoi Orange a-t-il préféré nouer un partenariat commercial au lieu de prendre une participation, ce qui aurait permis de créer des synergies et d'atteindre une masse critique ? Je me pose la même question s'agissant des câbles sous-marins.

Mme Christel Heydemann. Devenir un opérateur satellite ne fait pas partie de la stratégie de l'entreprise. Nous sommes un opérateur de services satellites, et à ce titre, nous sommes un fournisseur d'Eutelsat et d'autres constellations via nos stations terrestres. Pour tous les projets de nouvelles constellations, notamment Iris², la question centrale est celle de notre capacité d'engagement commercial dans la durée. Cela a presque autant de valeur que d'être investisseur en capital, puisque pour faire tourner le *business plan* de tels projets, il faut des débouchés commerciaux. Les discussions que nous menons dans le cadre du projet Iris² portent, d'une part, sur les services que nous pouvons apporter, et d'autre part, sur la mutualisation des infrastructures existantes, essentielle pour aider à rentabiliser les projets.

Notre métier n'est pas de construire des constellations satellites ; nous ne voulons donc pas investir en capital. Mais la commercialisation de ces solutions européennes, que ce soit sur le continent européen ou en Afrique, est essentielle, car l'enjeu, pour Eutelsat, et désormais pour OneWeb, est de générer des revenus commerciaux. Nous sommes donc un partenaire engagé et absolument essentiel pour leur réussite.

M. le président Philippe Latombe. Et vous ne pourriez pas conclure ce type de partenariat avec Starlink, par exemple ?

Mme Christel Heydemann. Starlink est un concurrent. Il nous arrive, très ponctuellement, de l'intégrer dans nos solutions lorsque des clients entreprises ayant besoin d'un *back-up* satellite le réclament. Mais que ce soit en Europe ou en Afrique, notre accord porte sur la distribution de OneWeb et d'Eutelsat, non de Starlink.

Dans le domaine de la connexion des terminaux mobiles par satellite, nous testons la solution Starlink en Espagne, en zone rurale, mais nous n'avons pas vocation à la déployer. En France, nous avons lancé une offre avec Skylo, qui utilise les constellations géostationnaires existantes et le spectre MSS, et conclu un partenariat avec AST SpaceMobile et sa filiale européenne SatCo, qui est une *joint-venture* dans laquelle ont investi de nombreux opérateurs télécoms parmi lesquels deux opérateurs américains, un opérateur saoudien et Vodafone. Il s'agit d'éviter la constitution d'un duopole américain et de nous assurer qu'émerge une solution européenne alternative que nous puissions intégrer lorsqu'elle sera disponible – même si elle ne le sera probablement pas en 2027 ou 2028 pour les attributions de spectres.

M. le président Philippe Latombe. En Espagne, il ne s'agit que d'un test ?

Mme Christel Heydemann. Pour tester la connexion satellite sur mobile, on peut utiliser soit le spectre satellite européen, comme nous le faisons en France avec Skylo, soit une partie de notre spectre d'opérateur mobile, comme nous le faisons en Espagne. Dans ce cas, sur le plan de la souveraineté, le cadre est entièrement contrôlé. L'accord annoncé par Deutsche Telekom vise, quant à lui, à proposer Starlink dans un cadre plus large que son spectre mobile.

Nous avons besoin de notre spectre mobile pour faire face à la croissance du trafic ; nous ne souhaitons donc pas l'utiliser pour le trafic satellite. Par ailleurs, l'utilisation du spectre de réseau mobile, qui est géré au niveau national, est limitée par des problèmes d'interférence. Je m'explique. Nous sommes opérateurs en France et en Espagne, où nous utilisons donc deux spectres distincts, qui ne sont pas cohérents entre eux, de sorte que nous ne pourrions pas proposer de services mobiles dans la zone frontalière. Or l'objectif est tout de même de couvrir des zones montagneuses comme les Pyrénées. L'utilisation de notre spectre mobile terrestre n'est donc pas la solution adéquate. Celle-ci passe forcément par les spectres qui seront attribués en 2027.

Dans le domaine de la communication par satellite, les terminaux mobiles sont un des éléments de dépendance numérique. De fait, ces terminaux sont équipés soit de l'environnement d'Apple, iOS, soit de celui de Google, Android, et sont fabriqués par des entreprises américaines – Apple –, coréennes ou chinoises. Or nous devons travailler avec ces fabricants, car l'utilisation de ces bandes de fréquences implique des changements de *firmware*, voire de *chipset*.

Mme Cyrielle Chatelain, rapporteure. Vous avez indiqué que Meta, Microsoft et surtout Google développaient fortement leur activité dans le secteur des câbles sous-marins, notamment transcontinentaux. Quel impact l'intervention de ces acteurs a-t-elle sur le marché et, éventuellement, sur notre souveraineté ? Quels sont les objectifs des partenariats que vous avez conclus avec Google et Meta pour déployer des câbles, notamment vers l'Afrique ? Enfin, envisagez-vous de faire d'Orange Marine un opérateur plus important en le rapprochant d'ASN ?

Mme Christel Heydemann. Les câbles sous-marins sont essentiels dans le métier d'opérateur, particulièrement en France, puisque Marseille est la porte d'entrée de tous les câbles sous-marins qui assurent le trafic entre l'Asie et l'Europe, et la côte atlantique celle des câbles transatlantiques.

Dans certains des pays où nous sommes implantés, notamment en Afrique, la redondance des routes internationales est un enjeu fondamental. Ainsi, il y a un peu plus de deux ans, trois câbles sous-marins ont été sectionnés à la suite d'un tremblement de terre au large de la Côte d'Ivoire, ce qui a plongé dans le noir trois des pays où nous opérons. Nous avons pu utiliser une route terrestre qui nous a permis de rétablir en vingt-quatre heures, depuis le Sénégal, un trafic minimal. Cet incident n'en illustre pas moins l'enjeu que représentent les câbles sous-marins pour la souveraineté des États où nous opérons ou, à tout le moins, pour la continuité de l'activité.

Historiquement, ces câbles étaient installés par des consortiums d'opérateurs télécoms, car aux débuts d'internet, le trafic international passait essentiellement par nos réseaux télécoms. Du fait de l'explosion du *cloud* et de l'IA, les grandes plateformes internationales que vous avez citées sont devenues les premiers pourvoyeurs de trafic ; nous travaillons donc avec ces acteurs sur de grands projets de câblage. Je pense en particulier au projet 2Africa de Meta – il vise à déployer un câble contournant l'Afrique –, dont nous sommes l'un des co-actionnaires, ce qui nous permet de disposer de capacité et de nous assurer de la création de pattes de connexion vers les pays où nous sommes opérateurs. Lorsqu'il s'agit de câbles reliant la Corse au continent, ou l'Hexagone à la Guyane et aux Antilles, nous sommes les seuls à porter le projet. Parfois, nous allons nous-mêmes chercher d'autres opérateurs comme Google et Meta.

Il est clair que certains des grands projets de ces acteurs visent d'abord à assurer une redondance pour favoriser la résilience de leurs propres services. De fait, la mer Rouge et la mer de Chine sont des zones à risques où passe une partie importante du trafic international. Mais il est vrai que la taille de ces projets leur assure une position qui leur permet d'évincer progressivement les opérateurs. Orange Marine est, pour eux, un partenaire de maintenance, sachant que la pose de grands câbles internationaux n'est pas notre métier – c'est celui d'ASN.

La question de savoir si la position occupée par quelques grands acteurs américains pourrait fermer une partie du marché à Orange Marine et ASN peut se poser, mais elle n'est pas d'actualité – elle se pose également, du reste, à propos des grands projets de câbles chinois. Par ailleurs, nous ne produisons pas les équipements de transmission qui sont posés au fond des océans : nous les achetons à ASN. Ce dernier est donc un partenaire et un fournisseur – nous avons également des projets communs.

Le mariage de ces deux activités serait-il pertinent ? Le projet n'existe pas, à l'heure actuelle. La France a deux champions sur ce marché. Ce n'est pas le cas, par exemple, des pays riverains de la mer du Nord, qui sont très conscients de leur dépendance dans le domaine de la maintenance des câbles sous-marins. Notre savoir-faire est donc envié en Europe. Il faut le partager et éviter de créer une position de monopole.

Je précise par ailleurs qu'Orange Marine est une filiale ; ses activités sont gérées de façon indépendante. Mais, dans les pays africains notamment, sa capacité d'offrir des services de connectivité internationale est perçue comme une des forces du groupe Orange.

M. le président Philippe Latombe. La question de la rapporteure est légitime, car la cession d'Orange Marine a été un temps envisagée. La taille critique étant un atout vis-à-vis des acteurs américains, le mariage de ces deux entreprises – qui ont toutes deux pour actionnaire l'Agence des participations de l'État (APE) – ne permettrait-il pas de créer un champion européen à même de discuter avec les Américains et, ce faisant, de rassurer nos partenaires européens quant à notre capacité d'être stratégiquement autonomes dans le secteur de la pose et de la maintenance de câbles sous-marins ?

Mme Christel Heydemann. À ma connaissance, il n'y a jamais eu de projet de cession d'Orange Marine. L'activité est pérenne et profitable – nous avons même annoncé un investissement dans deux nouveaux bateaux, après en avoir inauguré un il y a deux ans. En revanche, Nokia, qui était devenu propriétaire d'ASN à la suite de son acquisition d'Alcatel Lucent, avait le projet de céder cette entreprise, ce qui a conduit l'APE à en reprendre la propriété.

Je rappelle ce que je disais à propos des enjeux liés à l'ETS : il serait dommage que des problèmes de compétitivité mettent en péril l'activité de ces deux champions français ou que ces derniers soient contraints, pour demeurer compétitifs, de délocaliser leurs flottes de bateaux.

M. Éric Bothorel (EPR). Je salue le projet de nouveau campus d'Orange à Lannion, qui concourt à notre autonomie, donc à notre souveraineté.

S'agissant de l'ETS, je n'ai pas compris quelle était la position de la rapporteure, mais je crois que nous nous accordons sur le fait qu'il représente une menace pour la flotte stratégique des deux entreprises que vous venez d'évoquer.

Mme Cyrielle Chatelain, rapporteure. J'ai justement dit que je ne voulais pas ouvrir le débat !

M. Éric Bothorel (EPR). Je crois néanmoins que ce débat est important. Il est primordial qu'un pays comme la France, doté de façades maritimes importantes, de flottes et d'écoles nationales supérieures de la marine marchande, puisse préserver ces outils de souveraineté qui contribuent de manière essentielle aux infrastructures de transmission des données. J'en profite pour saluer les moyens bloqués dans le détroit d'Ormuz ; pendant la crise du covid, certains n'avaient pas pu être relevés.

Madame la directrice générale, j'aurais aimé vous parler de la distribution de clés quantiques sur fibres à cœur creux, qui sera essentielle pour notre autonomie stratégique future. Mais je réagirai plutôt à l'entretien que vous avez récemment accordé à *La Tribune*, dans lequel vous avez déclaré que l'Europe passait à côté de sa puissance industrielle, ajoutant qu'elle ne soutenait pas suffisamment ses champions industriels, à la différence des États-Unis et de la Chine. Pouvez-vous préciser votre analyse ? Thierry Breton disait hier que la régulation, qui reposait hier sur la confiance, repose désormais sur le rapport de force – une expression que vous avez employée dans votre propos liminaire.

Par ailleurs, vous semblez suggérer que les consommateurs seraient mieux protégés que les entrepreneurs. Je ne partage pas entièrement votre position, mais je reconnais qu'elle peut prêter à discussion. Néanmoins, nous nous inquiétons également du fait que les instances européennes puissent hésiter à agir avec fermeté lorsque cela est nécessaire. La demande formulée vise simplement à aligner certains dispositifs sur les standards américains, notamment en matière de MSS : conditions d'accès au capital, gouvernance, présence opérationnelle sur le territoire national ou européen, droit d'audit continu et emploi des salariés basés en Europe. Dans ce contexte, pourriez-vous contribuer à sensibiliser les parlementaires français au fait que légiférer au niveau national dans ces matières revient à accentuer la fragmentation de l'Europe tant sur le plan politique qu'économique ?

Mme Christel Heydemann. Une prise de conscience est nécessaire en Europe. La révolution technologique qu'est l'intelligence artificielle nous offre l'opportunité de rebattre les cartes et de reconquérir une partie de notre souveraineté dans le domaine numérique. Mais pour pouvoir remporter ces batailles, il faut être en mesure de mobiliser suffisamment de capacités d'investissement pour atteindre la taille critique. Encore faut-il que, dans leurs secteurs respectifs, les champions industriels européens ne soient pas empêchés d'intégrer l'IA par la fragmentation des réglementations, différentes d'un État membre à l'autre. En effet, pour atteindre la taille critique, les entreprises innovantes – et elles sont nombreuses, en France et en Europe – doivent non seulement avoir accès aux capitaux de marché, mais aussi bénéficier du Marché unique européen. Ce marché de consommateurs, plus important que le marché américain, suscite la convoitise du monde entier. Or il est paradoxalement presque plus facile pour une entreprise non européenne d'atteindre la taille critique et de servir le marché européen que pour une entreprise européenne qui, du fait des nombreuses régulations locales – j'appelle cela la matrice à trois dimensions de la régulation –, peine à traverser les frontières.

Ainsi, avant l'entrée en vigueur du règlement général sur la protection des données (RGPD), la protection des données était réglementée par la directive 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, dite directive e-Privacy. Non seulement ces deux réglementations sont redondantes, mais le RGPD lui-même est transposé de manière très différente dans chacun des États membres. Il en va de même pour la protection des

consommateurs, la sécurité ou les modes de paiement, qui varient d'un pays à l'autre, si bien qu'Orange, qui est opérateur dans huit pays d'Europe, est incapable d'étendre immédiatement à l'ensemble de l'Union européenne un service qu'il aurait développé avec succès dans un des États membres ! En revanche, les acteurs américains du web, qui ne sont pas soumis aux mêmes obligations que nous, s'installent souvent dans un des États membres, à partir duquel ils commercialisent leurs services. Pour les services de messagerie instantanée, par exemple, la régulation n'est pas la même pour les SMS et WhatsApp, alors que, pour le consommateur, le service est identique.

Cette fragmentation législative liée à la transposition de la réglementation européenne par chacun des États membres s'apparente, pour les entreprises, à un puzzle de vingt-sept réalités opérationnelles. Un opérateur comme Orange peut y faire face, au prix de certains investissements. Mais pour de plus petites entreprises qui, grâce à l'IA, peuvent devenir les champions numériques de demain, il est plus facile de développer leur activité dans un pays européen puis de partir aux États-Unis que d'atteindre la taille critique en Europe. Le projet de création d'un vingt-huitième régime européen est, à cet égard, une bonne mesure, car il faut absolument permettre à ces entreprises de bénéficier de la taille critique du marché européen.

Pour ce qui est du marché des télécoms, on peut le dire comme on veut, mais la concentration du secteur est essentielle. Il y a actuellement plus de quatre opérateurs dans chaque pays européen. Lorsque vous êtes numéro 1 sur un marché, comme nous le sommes en France, vous avez beaucoup plus de capacité à investir que si vous êtes le numéro 3 ou 4. Par conséquent, si vous n'êtes pas le premier – c'était notre cas en Espagne –, vous êtes condamné, pour pouvoir continuer à investir, par exemple dans la 5G, soit à fusionner avec un autre opérateur – comme nous l'avons fait en Espagne avec MásMóvil –, soit à vendre vos infrastructures pour vous désendetter. C'est ainsi qu'en Italie, Telecom Italia a cédé son réseau fixe à KKR – je n'ose imaginer les débats qu'aurait suscités en France la cession d'une partie d'Orange !

Le fait est que beaucoup d'opérateurs européens ne peuvent plus investir en raison de leur important endettement lié aux investissements colossaux imposés par le déploiement de la fibre et de la 5G. Or il est crucial d'investir dans la sécurité et la résilience des réseaux, ainsi que dans l'adaptation à l'intelligence artificielle. Il est donc nécessaire, pour un opérateur, d'atteindre la taille critique. C'est pourquoi il faut simplifier la régulation, fixer un cadre qui permet les investissements et autoriser une forme de concentration. Il ne s'agit pas de négliger le consommateur, car les enjeux en matière de pouvoir d'achat et de compétitivité sont essentiels, mais nous avons épuisé le modèle qui avait été pensé pour favoriser la multiplication du nombre d'opérateurs. Une forme de rationalisation est nécessaire, faute de quoi certains jetteront l'éponge.

Mme Cyrielle Chatelain, rapporteure. Vous avez peu évoqué la question des *data centers*. Orange développe-t-il ses propres infrastructures pour stocker ses données ? S'il externalise, quel opérateur a-t-il choisi ?

Par ailleurs, en matière de protection des données à caractère personnel, il nous a été indiqué que les contentieux liés au RGPD – modèle qui s'est d'ailleurs largement diffusé au niveau mondial – sont jugés dans le pays où l'entreprise est implantée, de sorte qu'en pratique, le régulateur européen est l'autorité irlandaise. En l'espèce, la fragmentation me semble donc assez faible.

Enfin, quelle est la différence entre les réglementations applicables aux SMS et à WhatsApp ? Il me semble que le problème n'est pas tant lié à une différence de régime entre les acteurs européens et américains qu'au fait que le développement des services de messagerie instantanée, qui ont pris une énorme place dans notre vie quotidienne, n'avait pas été anticipé. Quelle réglementation pourrait être appliquée à ces services ?

Mme Christel Heydemann. Les *data centers*, qui sont au cœur du développement de l'intelligence artificielle, sont l'une des briques de nos infrastructures physiques. Du fait de la croissance de l'IA, leur consommation énergétique est en train d'exploser au point qu'aux États-Unis, la fourniture d'électricité fait l'objet d'arbitrages entre, d'un côté, les *data centers*, et de l'autre, les industries ou la population.

Nous sommes propriétaires de *data centers* dans chacun des pays où nous sommes opérateurs. Ils hébergent nos cœurs de réseau – lesquels sont de plus en plus souvent « cloudifiés » à l'aide de technologies que nous maîtrisons, en intégrant de l'*open source* – ainsi que les données du trafic. En France, nous possédons principalement trois *data centers* – deux en Normandie, un troisième près de Chartres ; ces infrastructures, dans lesquelles nous avons l'intention d'investir, constituent un socle sécurisé qui nous permet d'envisager l'avenir. Nous en avons également de plus petits qu'il est prévu soit de mettre à niveau, soit de faire migrer vers les trois principaux sites.

Ces *data centers* hébergent les données de l'opérateur, certaines plateformes de services – telles que la messagerie électronique d'Orange, la deuxième la plus utilisée par les Français, que nous avons renforcée et sécurisée, et qui constitue une solution alternative aux solutions américaines –, ainsi que des services que nous proposons à nos clients entreprises, qu'il s'agisse d'hébergement pur ou de *cloud* sécurisé – je pense en particulier à Cloud Avenue.

Par ailleurs, comme je l'ai indiqué, nous sommes investisseurs dans Bleu. Il n'est pas hébergé dans nos *data centers*, mais il n'est pas exclu qu'il le soit à l'avenir.

Cela ne signifie pas que nous n'utilisons pas de solutions de *cloud* public pour une partie de nos données et de nos applications. Nous travaillons en particulier avec Google et Microsoft, toujours dans une logique de diversification, malgré des négociations commerciales souvent complexes. S'il est difficile de se passer de ces plateformes, c'est moins pour l'hébergement lui-même que pour tous les services et les applications qu'elles proposent, et qui permettent en particulier d'appliquer l'IA à certaines données. Les directions des systèmes d'information (DSI) que vous avez auditionnées vous ont sans doute confirmé que renoncer à leur palette d'outils soulevait des problèmes de coûts ou de vitesse d'exécution. Comme la plupart des entreprises, nous utilisons donc à la fois nos propres solutions et celles de ces grands acteurs, essentiellement américains.

Vous avez raison de dire que le RGPD est une règle européenne et que c'est en Irlande que l'Autorité intervient. Cependant, je constate que les modalités d'application retenues par la Commission nationale de l'informatique et des libertés (Cnil) lors de ses contrôles en France sont très différentes de celles qui ont cours dans d'autres pays d'Europe. La jurisprudence française est plus stricte et va plus loin que ce qui est prévu dans les textes européens – nous pourrons vous transmettre des exemples concrets. Pour avoir comparé la jurisprudence dans les différents pays où nous opérons, je ne peux que vous dire que la lecture de la Cnil est parfois beaucoup plus restrictive que celles des agences qui mettent en œuvre le RGPD dans d'autres pays européens ; c'est une interprétation des textes qui n'est pas la même.

La différence principale entre les SMS et WhatsApp réside dans la réglementation. Nous sommes soumis à la directive e-Privacy, une régulation qui s'impose aux opérateurs télécoms mais ne s'applique pas du tout aux acteurs du web. Dans le cadre d'une enquête judiciaire, par exemple, les plateformes n'ont pas l'obligation de transmettre les clés de cryptage au juge qui souhaiterait accéder à certains documents, alors que cette obligation s'appliquait historiquement à tous les services développés par les opérateurs télécoms. Je ne dis évidemment pas que les opérateurs doivent prendre le contrôle de toutes les messageries – je citais WhatsApp, mais il y en a beaucoup d'autres.

La même chose s'est produite lors de la mise en place du standard RCS (*rich communication services*), qui prévoit l'interopérabilité entre des plateformes qui avaient initialement construit des écosystèmes propriétaires fermés – c'est vrai de WhatsApp, mais aussi d'Apple, qui propose des services à ses clients dans l'environnement iOS. Cela n'a pas été sans frein de la part de certaines de ces plateformes, qui voulaient garder un environnement fermé. Avec le déploiement de ce nouveau standard, on nous demande, à nous, opérateurs, d'être le garant de certaines obligations nationales que les États ne sont pas en mesure d'imposer à ces acteurs extra-européens qui ne sont pas soumis à ces obligations dans tous les pays où ils opèrent. Nous vous transmettrons des exemples plus précis, que vous pourrez insérer dans vos conclusions.

M. Éric Bothorel (EPR). Si je suis sous sanctions américaines, comme le juge Guillou, que nous avons récemment auditionné, m'est-il possible de souscrire un abonnement Orange, fixe ou mobile, et de l'acquitter ? Y a-t-il un système de paiement par l'intermédiaire duquel je serais privé de ma capacité de m'abonner ?

Mme Christel Heydemann. Nous découvrons avec ce cas – et il y en a d'autres – notre intense dépendance à ces différentes technologies dans nos gestes du quotidien. Aujourd'hui, si vous allez en boutique pour souscrire un forfait Orange, on vous demandera votre identité, puisque nous en avons l'obligation. C'est d'ailleurs un autre point de différence avec les grandes plateformes : lorsque vous activez un service de communication web, vous ne déclinez pas formellement votre identité – il vous suffit en général de donner un numéro de téléphone, lui-même authentifié par les opérateurs télécoms. Il nous faudra ensuite numériser votre papier d'identité. Si vous avez sur vous votre carte d'identité, les choses sont simples ; s'il faut se connecter à un site internet pour récupérer un justificatif de domicile et que vous n'avez pas accès au web, comme M. Guillou, nous pouvons le faire pour vous en boutique. Enfin, si vous venez avec un RIB papier, nous pourrons le saisir dans notre système. Nous sommes donc capables d'activer le service sans vous demander de passer par une carte de paiement qui, en l'espèce, serait bloquée.

Mme Cyrielle Chatelain, rapporteure. La réponse est claire : les sanctions ne s'appliqueraient pas pour l'offre Orange, qui est une offre française et européenne.

Mme Christel Heydemann. Absolument.

Mme Cyrielle Chatelain, rapporteure. Vous êtes dépendants pour certaines étapes qui permettent de rendre ce service, mais le service pourrait être rendu.

Vous avez dit posséder des *data centers* en propre. Vous travaillez néanmoins avec Google et Microsoft pour bénéficier des services des *hyperscalers*. Pouvez-vous nous préciser le pourcentage et le type de données stockées sur ces *hyperscalers* ?

Dans la même veine, Orange a signé plusieurs partenariats avec Google Cloud et AWS pour des services que vous proposez à vos clients. Quels sont les objectifs de ces partenariats ? Alertez-vous les clients sur les risques que présentent ces options en termes de droit extraterritorial ?

Mme Christel Heydemann. Il faut distinguer la question des données hébergées dans le *cloud* de celle des applications que l'on porte ensuite dans des environnements « cloudifiés ». Un exemple de données hébergées dans un *cloud* public est celui des données liées à notre politique commerciale, c'est-à-dire à la myriade d'offres que nous proposons à nos clients, pour voir combien de clients utilisent ces offres. Ces données marketing sont hébergées dans des environnements *cloud* pour des raisons de simplification ; il ne s'agit typiquement pas de données personnelles. Nous ne mettons évidemment pas sur ce type de *cloud* les jumeaux numériques de nos réseaux, qui sont des données essentielles à la sécurité de ceux-ci, car nous travaillons en France dans des environnements SecNumCloud.

Je ne saurais pas vous donner de chiffres, sachant que le pourcentage diffère beaucoup d'un pays à l'autre. Dans certains pays d'Afrique, les données sont hébergées à 100 % dans nos *data centers*, car il n'existe pas de *cloud* public disponible ; dans certains pays d'Europe de l'Est, celui-ci est beaucoup plus avancé. La France est à mi-chemin. Ce n'est pas en France que nous sommes les plus avancés dans la migration des données vers du *cloud* public, pour la simple et bonne raison que nous avons des *data centers* de qualité et des *clouds* sécurisés qui n'existent pas forcément dans d'autres pays.

Orange Business propose à ses clients un service de migration de leur environnement IT. C'est un service plus limité que celui des grands intégrateurs IT – vous avez auditionné Capgemini, dont c'est le cœur de métier –, car notre activité principale demeure la connectivité et la cybersécurité, mais nous faisons aussi de l'hébergement *cloud*. Nous avons donc noué des partenariats avec les grands acteurs technologiques pour bénéficier de leurs compétences, pour nous former et pour être reconnus comme partenaires. C'est un service à vocation commerciale à la portée assez limitée. AWS est le leader du *cloud* public, mais, paradoxalement, nous collaborons plus avec Microsoft, qui est le leader des outils de collaboration en entreprise ; en effet, les enjeux de téléphonie d'entreprise sont très liés aux enjeux de collaboration.

M. le président Philippe Latombe. Comme vous l'avez dit, il y a des solutions américaines dont on ne sait pas se passer ; c'est le cas de Salesforce. Avez-vous une idée du volume d'activité d'Orange Business lié à ces solutions ? L'association avec des acteurs américains génère-t-elle plus de profit qu'avec des acteurs européens ?

Par ailleurs, Orange Business a noué un partenariat avec Mahindra, en Inde, pour faire du développement. Pourriez-vous nous indiquer combien de salariés et quelle part de l'activité d'Orange Business sont concernés ? J'ai l'impression que cela occupe plusieurs centaines, voire plus d'un millier de personnes. Quelles sont les potentielles dépendances vis-à-vis de l'Inde ? Nous avions posé la question aux établissements bancaires à l'occasion de l'examen du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, à un moment de conflit indo-pakistanais ; plusieurs banques qui faisaient du développement en Inde, et même du *run*, étaient sorties du pays. Avez-vous réfléchi à l'éventualité d'un retour ?

Mme Christel Heydemann. Concernant l'activité d'Orange Business, on constate, de façon un peu paradoxale, que nos plus grandes dépendances n'impliquent pas les grands acteurs du *cloud*, mais plutôt des acteurs comme Cisco. En effet, nous travaillons dans une logique de serveurs en entreprise : pour répondre aux besoins de connectivité, nous avons noué de grands

partenariats avec Cisco et HP. Nous travaillons également avec Bull, quoique dans une moindre mesure. Pendant longtemps, l'activité de Bull était totalement intégrée à Atos ; maintenant que Bull a été repris par l'APE, les discussions ont repris.

L'essentiel des activités d'Orange Business est concentré sur les enjeux de connectivité sécurisée pour les entreprises – je vous communiquerai ultérieurement les chiffres exacts. Dans ce contexte, nous sommes propriétaires de nos réseaux. Certes, comme je l'ai rappelé, ces réseaux comportent des dépendances technologiques, mais les dépendances se situent surtout au niveau des équipements placés chez le client : il s'agit des serveurs nécessaires à la mise en œuvre des solutions de connectivité, qui sont de plus en plus logicielles.

Je précise à ce sujet que nous investissons massivement dans notre *backbone* international. Nous avons créé une plateforme qui héberge un certain nombre de solutions, comme Fortinet ou Cisco, que nous proposons en mode « cloudifié » à nos clients pour permettre leur déploiement plus rapide et être beaucoup plus compétitifs. Nous sommes l'un des rares opérateurs à le faire à l'échelle internationale : nous maîtrisons de bout en bout le service pour nos clients, sur un *backbone* totalement opéré par Orange.

M. le président Philippe Latombe. Cela veut-il dire que vous avez une solution pour la virtualisation, en dehors de Broadcom ?

Mme Christel Heydemann. Nous avons, comme beaucoup d'entreprises, des dépendances à VMware – car le sujet, avec Broadcom, est essentiellement VMware. Comme beaucoup d'entreprises, donc, nous avons eu avec Broadcom des discussions, qui n'étaient pas des négociations, sur sa politique commerciale, et nous avons lancé des plans de réversibilité pour réduire notre dépendance à VMware. Pour certains de nos clients qui ont de grosses dépendances et qui ont eu la même expérience douloureuse d'absence de négociations sur l'évolution tarifaire de VMware, nous avons conçu la solution Cloud Avenue, qui leur permet de migrer dans notre environnement *cloud* sécurisé sans gros investissements de réécriture d'applications. Nous avons également développé d'autres solutions en interne afin de réduire le montant de l'addition, à défaut de pouvoir éliminer complètement la dépendance.

Le partenariat que nous sommes en train de finaliser avec Tech Mahindra concerne près de 3 000 collaborateurs, essentiellement en Inde et en Égypte. L'Inde est un pays dans lequel nous comptons de nombreux collaborateurs, que ce soit pour Orange Business, pour notre réseau international ou pour certaines de nos activités groupe, en particulier celles liées à la recherche et à l'innovation.

Ce partenariat avec Tech Mahindra est important à double titre. Il vise, d'une part, à accélérer la transformation de nos services *back office* et l'automatisation – c'est le volet d'externalisation que je mentionnais –, et, d'autre part, à renforcer notre présence à l'international. Tech Mahindra a pris des engagements fermes de commercialisation, auprès de ses propres clients, de notre produit Evolution Platform, dans lequel nous utilisons notre *backbone* et nos solutions. Tech Mahindra a donc un intérêt à apporter du chiffre d'affaires à Orange Business, et il s'est engagé à le faire. Sur ce périmètre hors Europe, les enjeux de compétitivité sont essentiels, et nous voulons que les grands intégrateurs IT puissent s'appuyer sur notre *backbone* pour distribuer leurs solutions plutôt que de travailler avec d'autres. Cela n'affecte pas notre activité et notre capacité à servir nos clients en France.

Mme Cyrielle Chatelain, rapporteure. Vous avez dit que les données hébergées chez Google et Microsoft étaient à la fois des données propres et celles des applications

développées sur le *cloud*. Pouvez-vous nous expliquer ce que cela signifie exactement ? En clair, Orange développe-t-il des applications dont les données sont finalement hébergées sur les *clouds* de Microsoft et de Google ? Cela veut-il dire que les données partagées par une personne qui téléchargerait ces applications sont stockées sur ces *clouds* ? Pouvez-vous nous donner des exemples d'applications concernées par cette pratique ?

Mme Christel Heydemann. Nous sortons d'un monde de l'IT où il y avait une application, un serveur, un *rack*. Tout cela est désormais virtualisé : nous partageons les infrastructures et choisissons quelle application sera migrée vers quel environnement *cloud*. Ce sont parfois des environnements que nous développons pour nous-mêmes, notamment pour la virtualisation de nos cœurs de réseau ; dans ces cas-là, nous utilisons au maximum l'*open source*. Nous avons reçu des financements européens pour développer, avec Deutsche Telekom, un *telco cloud* que nous maîtrisons nous-mêmes – il n'est évidemment pas envisageable d'héberger des jumeaux numériques dans des environnements *cloud* Azure, AWS ou Google. Il s'agit donc d'applicatifs ou d'applications que l'on migre vers le *cloud*, soit dans un environnement privé, soit dans un environnement public.

Un exemple : si vous interrogez les grands distributeurs vidéo ou les chaînes de télévision, tout le monde vous dira qu'AWS fournit les meilleurs services de diffusion de vidéo en temps réel pour les acteurs *online*. Nous avons donc quelques applicatifs qui peuvent tourner dans un environnement AWS. C'est en général l'un des éléments de la chaîne ; nous construisons au-dessus quelque chose que nous maîtrisons. De ce point de vue, l'IA agentique va nous permettre de développer nous-mêmes des éléments pour lesquels nous avons actuellement des dépendances.

Nous sommes de grands promoteurs de l'*open source*, et nous investissons le plus possible dans l'agrégation de solutions *open source*. Actuellement, nous nous efforçons de maîtriser les applicatifs qui touchent notre cœur de métier. Pour des applicatifs comme le CRM (gestion de la relation client), nous travaillons avec Salesforce dans certains pays. Pour des applicatifs au service de nos techniciens réseau, nous avons recours à des logiciels non-propriétaires qui sont utilisés par toutes les entreprises de logistique qui emploient des techniciens. Nous avons toute une palette de solutions. Je vous le disais, nous travaillons notamment avec des éditeurs comme Salesforce ou ServiceNow dans nos *stacks* logiciels.

L'arrivée de l'IA agentique pose beaucoup de questions à ces acteurs, qui veulent autant que possible conserver des environnements propriétaires et garder les clients. Des discussions sont en cours pour ouvrir les connecteurs et reprendre la maîtrise de certains éléments. Orange a la taille critique pour engager de telles discussions, mais ce n'est pas toujours facile. Notre but est de développer de l'IA, au-delà des dépendances que nous avons envers ces éditeurs. La maîtrise de l'IA agentique est la bataille de l'avenir ; c'est d'elle que dépendra l'indépendance numérique, ou pas, de l'Europe. Nous ne devons pas rater la marche. Il faut surtout éviter que les entreprises créent plus de dépendance. Tout cela va très vite, et il faut mettre à profit la taille critique de certains acteurs en Europe pour influencer les politiques commerciales qui sont en train d'être définies. Nous avons réussi à le faire avec certains acteurs américains ; des négociations sont en cours avec d'autres. Nous favorisons toujours ceux qui ont une approche *open source* pour ne pas nous enfermer dans des environnements sans réversibilité.

M. le président Philippe Latombe. Nous n'avons pas encore parlé d'Orange Cyberdefense. Cette filiale est très connue et incarne une certaine fierté française. Comment voyez-vous la concentration du marché de la cybersécurité depuis le rachat de Vade par Hornet,

puis d'Hornet par Proofpoint ? Est-ce une difficulté pour le groupe Orange ? Comment comptez-vous participer à la capacité de cet écosystème à rester le plus européen possible ?

L'arrivée de l'IA agentique, et notamment de Mythos, est-elle selon vous un *game changer* ? Avez-vous commencé à vous pencher sur le sujet ?

Mme Christel Heydemann. La question de la cybersécurité se pose à deux niveaux : celui des briques technologiques, et celui du service apporté aux entreprises. Orange Cyberdefense propose à ses clients des services pour lesquels nous sommes très dépendants de technologies qui sont essentiellement américaines, et parfois israéliennes : Palo Alto Networks, Zscaler, Microsoft, Fortinet, SentinelOne… Orange Cyberdefense a besoin de ces technologies embarquées pour se protéger et pour protéger les entreprises. Nous avons le choix du fournisseur, mais il y en a très peu d'européens. Nous avons donc lancé un travail pour augmenter notre surface de partenariats européens. Nous avons également recruté Guillaume Poupard, qui m'est directement rattaché, et qui travaille avec Orange Cyberdefense et Orange Business à muscler notre *roadmap* de solutions de confiance.

Le marché de la cybersécurité reste très fragmenté sur les services ; c'est vrai dans chaque pays d'Europe. Orange Cyberdefense est leader en France, en Belgique et en Suède. Nous sommes également en train d'investir en Espagne et dans tous les pays où nous sommes opérateur, d'abord parce que nous avons besoin de ces capacités pour nous protéger, mais aussi parce que nos réseaux sont des infrastructures critiques qui sont attaquées en permanence car ils sont le moyen d'affaiblir nos clients ou de les espionner. Nous sommes dans un environnement géopolitique où les cyberattaques sont devenues un moyen de manipulation. Parmi les partenaires européens avec lesquels Orange Cyberdefense travaille, je peux citer Sekoia, HarfangLab, une solution 100 % française de protection de nos postes de travail, ou encore Qevlar AI, une société de la French Tech que nous utilisons pour automatiser la détection des menaces.

Nous intégrons désormais l'IA agentique dans nos SOC (*security operations centers*) pour augmenter leur capacité d'analyse. C'est absolument indispensable pour automatiser et accélérer notre capacité de défense dans un environnement où les interconnexions et la dépendance à quelques solutions logicielles créent des fragilités économiques mondiales. Quand, quelques jours avant l'ouverture des Jeux olympiques, CrowdStrike a eu un bug lié à une mise à jour de Windows, on a d'abord cru qu'il s'agissait d'une attaque cyber ; l'épisode a montré la grande vulnérabilité des systèmes économiques à quelques logiciels. Dans cet environnement, l'enjeu, c'est à la fois la vitesse de détection des vulnérabilités et celle à laquelle nous sommes capables de les « patcher ». C'est là que l'IA, en particulier Mythos, est redoutable : la moindre vulnérabilité identifiée est immédiatement exploitée par des attaquants. Nous avons des plans pour « patcher » en permanence les vulnérabilités, mais ces dernières viennent malheureusement des logiciels que nous embarquons : il faut donc du temps pour que nous en soyons informés, et du temps pour que nous puissions les « patcher ». Ainsi, lors d'une crise de cybersécurité – nous n'en avons pas tous les jours, contrairement aux cyberattaques, pour lesquelles nous accompagnons également nos grands clients –, tout réside dans notre capacité à « patcher », à monitorer, à voir s'il y a une intrusion et des fuites de données.

Mythos et OpenClaw sont vertigineux de menaces et de risques pour l'écosystème. Faut-il nous-mêmes les utiliser pour découvrir nos vulnérabilités, au risque de ne pas savoir les « patcher » suffisamment vite ? C'est une question qui dépasse Orange et que se posent toutes les entreprises. Si les grands groupes du CAC40 ont les compétences pour y répondre, il n'en est pas de même au niveau du tissu industriel de nos fournisseurs, de nos partenaires et de nos

prestataires, qui sont souvent des PME et qui n'ont ni le savoir-faire, ni les compétences, ni la bande passante qui leur permettent de maîtriser ces sujets. C'est le marché sur lequel Orange Cyberdefense déploie en priorité ses solutions automatisées de gestion à distance, qui sont l'un de ses relais de croissance.

M. le président Philippe Latombe. Avez-vous aujourd'hui les moyens de vos investissements ? Vous distribuez un taux de dividende relativement important par rapport à vos bénéfices : est-ce une demande de l'APE, en tant qu'actionnaire principal d'Orange ? D'ailleurs, l'APE vous a-t-elle donné une feuille de route en matière de souveraineté ? Y a-t-il des discussions de cette nature au sein du conseil d'administration ?

Mme Christel Heydemann. La gouvernance de l'entreprise est solidaire. L'APE, qui s'exprime au conseil d'administration d'Orange, est donc solidaire des décisions qui sont prises par celui-ci en matière de rémunération des actionnaires. Je vous laisse donc interroger l'APE sur sa politique en tant qu'investisseur.

La principale idée que nous avons en tête, c'est que nous sommes, en Europe, sur des marchés matures en forte transformation. Quand on est l'opérateur numéro 1 dans un pays, on a une plus grande capacité à investir dans la durée. Nos investissements ont été historiquement tournés vers les réseaux d'accès que sont la couverture mobile et la fibre. Nous sommes même l'opérateur qui a le plus développé la fibre en Europe : plus de 100 millions de foyers ont été raccordés par Orange. Cela fait d'Orange le champion incontesté de la fibre en Europe. Maintenant que ces investissements sont derrière nous, la pression a baissé : de ce fait, nous avons moins d'investissements en France, et c'est une chance, car nous avons désormais besoin d'investir dans la capacité de nos réseaux mobiles et dans la résilience de nos réseaux au sens large, y compris par la redondance. Au-delà des attaques cyber, le changement climatique fait peser des risques accrus sur nos infrastructures physiques – tempêtes, inondations, incendies, éboulements –, et paradoxalement, un opérateur comme Orange, qui a fait le choix d'être un opérateur d'infrastructures, a une surface de risques plus large.

La vraie question est celle de notre capacité à investir dans des secteurs adjacents comme l'IA, le *cloud* et le développement de solutions *open source*, et à aider l'écosystème d'innovation à « scaler » en Europe. Pour ce faire, nous devons libérer des marges d'investissement dans la durée. Nous sommes l'un des rares opérateurs à avoir maintenu un effort de 600 millions d'euros d'investissements dans la recherche. Cela ne nous empêche pas de rémunérer nos actionnaires. De ce point de vue, les demandes de rendement de l'APE ne sont pas différentes de celles de nos salariés retraités, mais ce n'est pas en ces termes que se posent les débats au conseil d'administration.

Nous venons de mener la plus grosse opération de consolidation en Espagne en fusionnant avec MásMóvil ; nous sommes en train d'obtenir les autorisations pour reprendre le contrôle de cet opérateur, qui est le deuxième d'Espagne, avec 10 millions de clients de plus que Telefónica. C'est un investissement de plus de 4 milliards d'euros que notre bilan nous permet. Comme vous le savez, des discussions sont en cours sur l'avenir de SFR, et nos marges de manœuvre nous permettent également d'investir dans des opérations de consolidation sur notre premier marché.

L'enjeu de l'innovation dans des technologies adjacentes réside avant tout dans notre capacité à devenir une plateforme qui permette à l'écosystème d'innovation de passer à l'échelle. Les innovations technologiques ne viendront pas toutes d'Orange ; au contraire, nous sommes dans un environnement où l'*open source* et la capacité à agréger des technologies sont

essentiels. Il faut donc faire bénéficier les entreprises de notre taille critique, de nos environnements sécurisés et de nos investissements dans les infrastructures – je parlais de notre *backbone* international, mais il y a également les *data centers*… Nous devons promouvoir ces atouts. C'est tout l'enjeu du Digital Networks Act que de permettre aux grands opérateurs télécoms de contribuer à la souveraineté numérique. Nous en discutons avec Deutsche Telekom en Allemagne, avec Telefónica en Espagne, avec Vodafone en Angleterre et avec l'ensemble des opérateurs européens.

Mme Cyrielle Chatelain, rapporteure. Vous avez beaucoup parlé de votre offre Cloud Avenue, certifiée SecNumCloud. Pourquoi avoir développé Bleu ? Quelles sont les différences ? Quel est le rôle d'Orange dans ce partenariat avec Capgemini et Microsoft ?

Mme Christel Heydemann. Vous le savez, Bleu date d'avant mon arrivée à la tête d'Orange – je n'étais alors qu'administratrice. Cette offre répond à une problématique d'entreprise importante. La norme SecNumCloud s'impose aux entreprises comme Orange, qui opèrent des applications dans de nombreux pays d'Europe. Ces solutions tournent dans des environnements Azure, mais en France, les mêmes applicatifs doivent être opérés dans un environnement SecNumCloud. D'où la création de Bleu, dont tout l'intérêt est de garantir l'immunité extraterritoriale dans des environnements Azure.

Il n'y a pas d'indépendance technologique, puisque les briques restent celles fournies par Microsoft. Mais celui-ci investit massivement pour créer un environnement Azure déconnecté de son *cloud* mondial, et il le fait pour deux pays européens : la France, avec Bleu, et l'Allemagne, avec SAP Delos Cloud. Nous avons absolument besoin de cette offre pour sécuriser certaines applications et les migrer dans un *cloud* dans un environnement SecNumCloud, ce qui permet à certaines entreprises de se « dérisquer » au regard de l'extraterritorialité américaine – c'est d'ailleurs tout le sens de cette norme.

Orange est investisseur de Bleu, à hauteur de 50 %, avec Capgemini, mais c'est aussi l'un de ses clients, dans certaines de nos activités, et l'un de ses partenaires, pour ce qui concerne Orange Business. Reste que Bleu est autonome : il y a un directeur général, une équipe. Il travaille avec tous les intégrateurs et démarche les clients qui sont dans sa cible. Cela ne nous empêche pas, je l'ai dit, de développer des solutions en propre. Cela étant, en matière de *cloud* public certifié SecNumCloud, Bleu est une solution et le concurrent, d'une certaine façon, du S3NS de Google. Ce sont les deux solutions en France.

Je précise qu'il s'agit d'un environnement français. Dans de nombreux autres pays d'Europe, la norme SecNumCloud n'existe pas, et l'EUCS, la certification européenne de cybersécurité pour les services *cloud* promue par le Cybersecurity Act, est bien moins protectrice. Nous sommes d'ailleurs les premiers à promouvoir, à Bruxelles, un EUCS+. Il faut prendre conscience du monde dans lequel on vit !

En somme, Bleu est une des solutions. Ce n'est pas la seule – ni la seule que nous utilisons, ni la seule à répondre aux exigences. D'ailleurs, avec nos clients entreprises, nous travaillons aussi bien avec Bleu qu'avec OVHCloud ou nos solutions *cloud*. Ce sont les clients qui choisissent leur environnement.

M. le président Philippe Latombe. Je note que votre réponse est plus allante que celle de votre co-investisseur, qui ne nous a pas dit tout l'intérêt de Bleu pour Capgemini comme vous venez de le faire pour Orange.

Mme Cyrielle Chatelain, rapporteure. SecNumCloud est effectivement une norme française, et nous plaidons pour son déploiement au niveau européen afin de renforcer notre souveraineté. Si j'ai bien compris, vous disposiez déjà d'une offre SecNumCloud, mais l'intérêt de Bleu est, grâce à une capitalisation d'acteurs français, d'offrir une protection à l'endroit des lois d'extraterritorialité, et de vous permettre d'utiliser les mêmes applicatifs Azure que dans d'autres pays tout en répondant aux exigences de souveraineté imposées par la France.

Concrètement, comment l'étanchéité des données est-elle garantie au sein de Bleu ? Quid des mises à jour d'Azure ? Sont-elles assurées par des opérateurs situés en France ou doivent-elles être réalisées à distance ? Quelles garanties avez-vous que Bleu ne repose pas sur la solution Azure de base, celle qui serait utilisée ailleurs ?

Mme Christel Heydemann. Comme je l'ai dit, Orange n'est qu'investisseur dans Bleu. Celui-ci a un directeur général et un conseil d'administration, où Orange et Capgemini ont chacun trois représentants. Je ne fais pas d'ingérence.

Ce que nous savons, c'est que Bleu est une société française, avec des salariés français, qui n'a pas d'activité en dehors de l'Union européenne. Ses centres de données sont situés en France, et ses serveurs opérés exclusivement en France, par des collaborateurs de Bleu. Les données sont hébergées en France et ne peuvent pas quitter le territoire – c'est l'essence même de la technologie *air gap* développée par Microsoft. Bleu a été conçu dès le départ pour répondre aux exigences SecNumCloud 3.2. Le processus de certification par l'Agence nationale de la sécurité des systèmes d'information (Anssi), lancé au milieu de l'année dernière, est en cours. L'agence est en train d'éplucher les modes opératoires, et vous pouvez lui faire confiance pour ne pas passer à côté de quelque chose !

Les applications que nous hébergeons, ou que nous portons, et qui opèrent dans des environnements Azure ne sont pas physiquement hébergées dans les mêmes *data centers*. Dans certains pays, l'environnement Azure n'est pas lié à une notion de localisation puisque, par nature, c'est un *cloud* mondial, même s'il peut y avoir des formes d'européanisation. Pour Bleu, c'est très différent : Microsoft n'accède pas à la technologie, et l'offre, encore une fois, est totalement étanche au Cloud Act, puisqu'elle est assurée par des collaborateurs en propre et que les deux actionnaires sont Orange et Capgemini.

Mme Cyrielle Chatelain, rapporteure. Effectivement, l'Anssi travaille sur le sujet. Nous l'interrogerons sur cette technologie *air gap* pour mieux comprendre comment elle fonctionne.

La question des mises à jour est essentielle. D'après les déclarations publiques de l'Anssi, Bleu semble effectivement offrir une protection à l'égard des lois extraterritoriales, ce qui confirmerait qu'il n'est pas possible d'accéder aux données à distance. Mais vous savez comme moi que cette question n'est pas liée à la localisation des données, mais à l'opérateur de la capacité où elles sont stockées.

Il semblerait, toujours selon l'Anssi, que Bleu repose sur une technologie Microsoft ; cela signifie, en termes de *kill switch*, que l'absence de mises à jour engendrerait à terme des failles de sécurité susceptibles de rendre la technologie obsolète. Comment s'organise la collaboration entre Bleu et Microsoft sur cette question cruciale ? Nous avons du mal à savoir jusqu'où Microsoft opère dans la technologie et ce à quoi il a accès.

Mme Christel Heydemann. Ce qui est sûr, c'est que Bleu n'aura jamais les dernières fonctionnalités d'Azure, puisqu'il faudra du temps pour les porter dans sa *roadmap*.

Dans l'hypothèse où l'on empêcherait Bleu de bénéficier de mises à jour logicielles, on serait dans une forme d'arrêt de maintenance dans la durée qui conduirait à l'obsolescence technique. Mais, paradoxalement, les environnements « cloudifiés » permettent beaucoup plus facilement les mises à jour qu'un certain nombre d'autres solutions logicielles qui ne sont plus maintenues par leur fournisseur. Nous avons beaucoup de telles solutions chez Orange, et ce risque m'inquiète bien davantage, car il faut alors être capable d'investir pour mettre à niveau les environnements. Si vous n'êtes pas dans un environnement *cloud*, il est quasiment impossible de mettre à jour manuellement des solutions qui ne sont plus maintenues.

Nous parlions tout à l'heure d'attaques cyber dans un monde fait d'IA. Bleu travaille avec Orange Cyberdefense ; nous avons donc des capacités de protection. On peut toujours imaginer un scénario catastrophe qui mettrait le monde à l'arrêt, mais le problème dépasserait largement Bleu : il y aurait bien d'autres enjeux !

En revanche, j'insiste sur le nombre de solutions éditeur qui ne sont pas maintenues ou arrivent en fin de maintenance, et sur le risque que cela représente pour les entreprises, y compris pour Orange. Nous avons de nombreux projets de migration, d'extinction… La dette technique est un enjeu essentiel pour toutes les DSI, et elle est d'autant plus importante que l'entreprise est ancienne.

M. le président Philippe Latombe. Au-delà de la dette technique, nous ne pouvons pas négliger le contexte géopolitique. Qui aurait imaginé, il y a deux mois, que les Américains organiseraient le blocus maritime du golfe d'Aden ? La situation du juge Guillou nous le montre : il faut se préparer à tout. C'est pourquoi je vous ai interrogé sur la cybersécurité. Comment sécuriser Microsoft 365 quand la seule entreprise européenne qui en était capable, Vade, est rachetée par Hornet, qui est à son tour rachetée par Proofpoint ? Dans le contexte actuel, il est tout de même gênant de devoir s'en remettre aux Américains.

Mme Christel Heydemann. Tous les conseils d'administration s'interrogent sur leurs plans de continuité d'activité dans le contexte géopolitique actuel. Mais la migration intégrale des environnements d'une entreprise, qu'ils soient hébergés sur Azure ou fournis par Microsoft, prend plusieurs mois. Si vous en avez le temps, vous pouvez l'envisager. Mais si vous avez besoin de plans de continuité, mieux vaut recourir à des solutions comme celle de Bleu, qui garantit la pérennité de votre activité. Pour notre part, nous utilisons, outre l'environnement Microsoft, des solutions de collaboration *open source*, que nous proposons également aux clients d'Orange Business. Je pense à la solution Live Collaboration, qui agrège des briques *open source* et nous permet d'être indépendants. Mais encore une fois, la migration de l'ensemble des postes, dans tous les pays où le groupe est implanté, vers cette solution prendrait trois ans. Compte tenu de la vitesse à laquelle surviennent les crises géopolitiques, ce n'est pas envisageable.

Qui plus est, une telle migration aurait un coût qu'en raison de l'environnement de compétitivité et de pouvoir d'achat européen, beaucoup d'entreprises ne peuvent pas se permettre. Pour celles qui évoluent dans un environnement critique ou régulé, la question du coût d'un environnement sécurisé ne se pose pas, mais d'autres n'ont pas d'autre choix que d'utiliser ce type de technologies. Pour celles-là, la véritable question qui se pose est celle de leur plan de continuité d'activité. Elles doivent faire des choix par défaut, je vous l'accorde ; mais c'est la réalité des dirigeants d'entreprise.

M. le président Philippe Latombe. La dépendance commence aussi à coûter cher du fait de l'augmentation du prix des licences, notamment celles de Microsoft. Mais je note que Bleu est une solution intermédiaire, et cela me convient.

M. Éric Bothorel (EPR). Cela me convient également.

Quels enseignements tirez-vous du bombardement de *data centers* en Ukraine ou, plus récemment, à Bahreïn et aux Émirats arabes unis ? Serions-nous plus résilients si nous concentrions moins ces infrastructures sur notre sol ou si nous recourions à des systèmes interconnectés permettant des *back-up* internationaux ? La menace n'est certes pas immédiate, mais elle se rapproche.

Mme Christel Heydemann. Il est parfaitement utopique de penser les *data centers* sans prévoir leur connectivité et les réseaux de communication à même de les relier. Sans aller jusqu'à imaginer un bombardement, que se passe-t-il en cas d'*outage*, comme c'est arrivé récemment en Espagne ? En général, les *data centers* bénéficient de systèmes de secours qui leur permettent de continuer à être alimentés en énergie. Mais si une panne survient, la résilience est assurée par la technologie *cloud*, qui permet de basculer vers le reste de l'infrastructure. La performance peut être affectée, car la puissance de calcul est moindre, mais cela tient. C'est la démonstration que des environnements non « cloudifiés » hébergés dans un *data center* présentent davantage de risques que des environnements « cloudifiés ». Maintenant, si un *data center* tombe, que vous êtes privé d'environnements redondants et de réseaux de communication ou que ceux-ci sont également coupés, cela fait mal !

Nous vivons dans un monde très dangereux. Nous avons d'ailleurs lancé des solutions de protection contre les drones, que nous utilisons dans nos propres *data centers* en France. Nous sommes donc conscients du niveau de la menace. Je ne pense pas que les professionnels qui travaillent sur ces questions aient été totalement surpris par les événements récents. C'est plutôt la diversité des scénarios et la vitesse à laquelle ils sont mis en œuvre qui en surprend beaucoup ! Je précise qu'en tant qu'opérateur en Pologne, en Roumanie, en Slovaquie et en Moldavie, nous sommes, depuis quelques années déjà, aux premières loges du conflit entre la Russie et l'Ukraine. En Pologne et en Roumanie, où Orange est l'opérateur historique, nos équipes ont évidemment avec les autorités un dialogue permanent sur la sécurité des infrastructures numériques, des réseaux et des *data centers*.

M. le président Philippe Latombe. Merci beaucoup, madame la directrice générale. C'est avec plaisir que nous lirons vos réponses écrites au questionnaire que nous vous avons envoyé, ainsi que d'autres éléments que vous voudrez bien nous transmettre sur les divers sujets que nous avons évoqués.

La séance s'achève à douze heures trente.

Membres présents ou excusés

Présents. – M. Éric Bothorel, Mme Cyrielle Chatelain, M. Philippe Latombe.