N° 1832

———

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 3 avril 2018.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES ÉCONOMIQUES

SUR LA PROPOSITION DE LOI

visant à **préserver** *les* **intérêts** *de la* **défense** *et de la* **sécurité nationale** *de la* **France** *dans le* **cadre** *de l'*__exploitation__ *des* **réseaux radioélectriques mobiles** (n° 1722).

PAR M. ÉRIC BOTHOREL

Député

———

Voir les numéros : 1722 et 1830.

SOMMAIRE

—

Pages

INTRODUCTION

Le déploiement commercial prévu au début de l'année 2020 en France de la cinquième génération standardisée de connectivité des terminaux mobiles, dite « 5G », est présenté comme une véritable rupture technologique. Outre un supplément de services attendu pour les consommateurs finaux, dont les usages numériques requièrent toujours plus de mobilité, la 5G devrait permettre d'accélérer prodigieusement le développement d'usages industriels. L'exemple le plus répandu, mais également le plus pertinent, des promesses de la 5G est sa capacité à supporter le déploiement à grande échelle de véhicules autonomes.

Plus généralement, l'arrivée de la 5G permettra de répondre aux limites de la précédente génération, la 4G, en relevant trois défis principaux que sont : l'engorgement des réseaux de communications électroniques face à la massification des usages mobiles ; la capacité à fournir un accès aux réseaux et un débit suffisant à une grande quantité d'objets connectés (individuels, domotiques ou industriels) ; enfin, de trop longs délais de latence pour des services innovants qui requerront des temps de réaction à l'échelle de la milliseconde [(1)]. Pour toutes ces raisons, il faut accueillir avec enthousiasme l'arrivée à maturité technologique de ce nouveau standard et réunir les conditions nécessaires au déploiement rapide de ce nouveau réseau sur le territoire français.

Toutefois, le développement de la 5G n'est pas exempt de risques et il en va de la responsabilité du législateur de les prévenir avec justesse. Deux types d'enjeux de cybersécurité peuvent aujourd'hui être identifiés et font l'objet de la présente proposition de loi.

Les spécificités techniques propres à la 5G sont, tout d'abord, susceptibles d'accroître les vulnérabilités des réseaux par rapport aux générations précédentes de standards technologiques. Les réseaux 5G offriront notamment une plus grande surface de vulnérabilité à d'éventuelles attaques en raison de leur grande ramification, qui va supposer la multiplication des antennes, des capteurs et des nœuds informationnels par rapport aux réseaux existants. Potentiellement, chaque antenne pourra devenir une partie sensible du réseau, et non pas seulement l'extension passive du cœur de réseau, centralisé et bien protégé, comme c'est le cas des réseaux 3G et 4G actuels.

En outre, la 5G devrait être le vecteur de la généralisation de réseaux virtualisés – dans lesquels les équipements physiques (le *hardware*) sont remplacés par des solutions logicielles (*software*) déployées dans le *cloud* – qui

(1) La latence d'une connexion 5G serait d'environ 5 millisecondes, contre 100 millisecondes pour une connexion 4G. La différence est peu sensible pour une simple connexion à un site internet, mais devient critique pour des mécanismes de freinage automatique

promettent d'être plus véloces et plus résilients, mais qui ne seront pas exempts de failles d'un nouveau genre [(1)]. En corollaire, la 5G étant le terrain de nombreuses innovations technologiques, il y aura beaucoup d'expérimentations et de corrections avant que le réseau ne se stabilise. Ce facteur d'imprévisibilité se traduit nécessairement par un accroissement des risques liés, d'une part, à l'utilisation de technologies non parfaitement matures et, d'autre part, au fait que la protection contre ces risques s'ajustera toujours avec un temps d'adaptation.

En second lieu, certains secteurs critiques, exigeant une sécurité absolue des réseaux utilisés, vont, par ailleurs, être amenés à utiliser la technologie 5G. L'exploitation malveillante ou criminelle d'éventuelles faiblesses des équipements 5G utilisés dans ces domaines pourrait avoir de graves conséquences, aisément imaginables dans le cas d'une voiture connectée ou d'une opération chirurgicale à distance. Plus traditionnellement, ce sont les installations et établissements porteurs d'infrastructures critiques (sites classés SEVESO, sites de production d'énergie, réseaux de communications électroniques eux-mêmes) qui doivent faire l'objet d'une connectivité irréprochable. Dans les périmètres géographiques qui accueillent de telles structures, il existe d'ailleurs des « lignes rouges », non écrites, mais qui impliquent que les opérateurs de communications électroniques manifestent de plus fortes précautions dans leurs modalités de déploiement des réseaux.

Notons, enfin, qu'il est également dans l'intérêt économique à long terme de l'économie française de garantir la sécurité de ses réseaux de communications électroniques. Ces réseaux supposent des investissements colossaux – de l'ordre de plusieurs centaines de millions d'euros – et constituent un actif économique qu'il serait très préjudiciable de dégrader, par exemple en raison de choix techniques inappropriés.

Ces différents arguments, qui font écho à l'existence de risques accrus dans des secteurs jugés critiques, montrent la nécessité d'une adaptation du cadre juridique visant à garantir la sécurité et la résilience des réseaux de communications électroniques déployés en France. La présente proposition de loi prévoit ainsi un régime d'autorisation préalable, fondé sur des motifs de défense et de sécurité nationale, des équipements des réseaux de communications électroniques mobiles qui seront déployés pour diffuser la 5G.

Ce dispositif proposé a été élaboré en concertation étroite avec les acteurs privés directement concernés et avec les autorités de régulation. Il vise à garantir un développement soutenable et sûr de la 5G et de ses usages en France. Votre rapporteur veillera également à ce qu'il demeure suffisamment souple pour ne pas obérer les capacités d'innovation des opérateurs, des équipementiers et des industriels ni gêner un déploiement rapide et efficace sur l'ensemble du territoire.

---

(1) À titre d'exemple, les réseaux étant déployés sur une surface dématérialisée, en cloud*, les serveurs qui soutiennent ce* cloud *et ses applications sont une nouvelle source de vulnérabilité.*

TRAVAUX DE LA COMMISSION

I. DISCUSSION GÉNÉRALE

Au cours de sa séance du mercredi 3 avril 2019, la commission a procédé à l'examen de la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (n° 1722), sur le rapport de M. Éric Bothorel.

M. Mickaël Nogal, président. Mes chers collègues, notre commission est saisie au fond de la proposition de loi de M. Gilles Le Gendre et de plusieurs de ses collègues visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles. Après une présentation d'une dizaine de minutes de notre rapporteur, M. Éric Bothorel, nous entamerons la discussion générale : les orateurs des groupes auront droit à une intervention de quatre minutes, puis les députés qui le souhaitent pourront prendre la parole pour deux minutes. Nous passerons ensuite à l'examen des articles de la proposition de loi. Je vous informe que la commission avait initialement été saisie de 26 amendements, mais que l'un d'eux a été retiré : il en reste donc 25.

M. Éric Bothorel, rapporteur. Monsieur le président, Madame la secrétaire d'État, Monsieur le rapporteur pour avis de la commission de la défense nationale et des forces armées, Mesdames et Messieurs les députés, mes chers collègues, il y a tout juste une semaine, la Commission européenne a officiellement émis des recommandations préalables à l'arrivée de la 5G sur le territoire de l'Union européenne. Elle a souhaité que, dès cette année, chaque État membre renforce ses exigences de sécurité en matière de réseaux radioélectriques. La proposition de loi que j'ai l'honneur de vous présenter aujourd'hui s'inscrit pleinement, et avec un temps d'avance, dans cette perspective.

Le déploiement commercial de la 5G, soit la cinquième génération standardisée de connectivité des terminaux mobiles, est prévu en France pour le début de l'année 2020. Nous allons donc, dans moins d'un an, contribuer à cette grande rupture technologique. La 5G ne fera pas qu'améliorer les services rendus à des utilisateurs toujours plus mobiles : elle accélérera prodigieusement le développement de nouveaux usages. Les exemples ne manquent pas : déploiement à grande échelle des véhicules autonomes, optimisation de la consommation énergétique, ou encore développement de nouveaux services en télémédecine.

Plus généralement, l'arrivée de la 5G permettra de dépasser les limites de la précédente génération, la 4G, en relevant trois défis principaux : désengorger les réseaux de communications électroniques de plus en plus saturés par la massification des usages mobiles ; fournir un accès aux réseaux et un débit

suffisant à une grande quantité d'objets connectés ; enfin, réduire les délais de latence pour des services innovants qui requerront des temps de réaction à l'échelle de la milliseconde. Pour toutes ces raisons, nous devons accueillir avec enthousiasme l'arrivée à maturité technologique de la 5G et réunir les conditions nécessaires au déploiement rapide de ce nouveau réseau sur le territoire français. Cependant, si les réseaux sont devenus une évidence dans nos vies, en particulier pour les plus jeunes générations, ils représentent aussi une menace, et la 5G ne fait pas exception. Son développement n'est pas sans risques et il est de notre responsabilité de les prévenir avec justesse.

Deux enjeux majeurs de cybersécurité peuvent aujourd'hui être identifiés. Le premier est celui des spécificités techniques propres à la 5G. Elles sont susceptibles d'accroître la vulnérabilité des réseaux par rapport aux générations précédentes de standards technologiques. En effet, la 5G n'est pas la 4G + 1 : les réseaux 5G offriront notamment une plus grande surface de vulnérabilité à d'éventuelles attaques en raison de leur grande capillarité, qui va supposer la multiplication des antennes, des capteurs et des nœuds informationnels par rapport aux réseaux existants. Chaque antenne pourra potentiellement devenir une partie sensible du réseau : elle ne sera plus l'extension passive du cœur de réseau, centralisé et bien protégé, comme dans les réseaux 3G et 4G actuels.

Ces spécificités techniques comprennent également le déploiement de « réseaux virtualisés », que la 5G devrait généraliser. Les équipements physiques y seront remplacés par des solutions logicielles déployées dans le *cloud.* Ces réseaux promettent d'être plus véloces et plus résilients, mais ils ne seront pas dépourvus de failles d'un nouveau genre. D'une manière plus générale, la 5G sera le terrain de nombreuses innovations technologiques et il faudra un grand nombre d'expérimentations et de corrections avant que le réseau ne se stabilise. Ce facteur d'imprévisibilité se traduira nécessairement par un accroissement des risques liés, d'une part, à l'utilisation de technologies non parfaitement matures et, d'autre part, au fait que la protection contre ces risques nécessitera toujours un temps d'adaptation.

Le deuxième enjeu est celui des secteurs critiques, qui exigent une sécurité absolue des réseaux et qui vont être amenés à utiliser très prochainement la technologie 5G. L'exploitation malveillante ou criminelle d'éventuelles faiblesses des équipements 5G dans ces domaines pourrait avoir des conséquences désastreuses, comme la perte de contrôle de plusieurs voitures connectées ou l'interruption subite d'une opération chirurgicale à distance. Je pense aussi à l'ensemble de nos installations et établissements porteurs d'infrastructures critiques, comme les sites classés SEVESO, qui doivent faire l'objet d'une connectivité irréprochable. Tout cela démontre la nécessité d'adapter le cadre juridique visant à garantir la sécurité et la résilience des réseaux de communications électroniques.

La proposition de loi que nous allons examiner a pour but de répondre à cet impératif. Elle prévoit un régime d'autorisation préalable, fondé sur des motifs

de défense et de sécurité nationale, des équipements des réseaux de communications électroniques mobiles qui seront déployés pour diffuser la 5G.

Permettez-moi de vous décrire très brièvement le dispositif.

L'article 1er de cette proposition de loi s'inspire directement d'un dispositif du code pénal introduit pour protéger le secret de la correspondance privée. Élargissant cette base juridique relativement étroite au regard des nouveaux impératifs de sécurité, il soumet à une autorisation du Premier ministre l'exploitation, sur le territoire national, « d'appareils, à savoir tous dispositifs matériels ou logiciels » qui permettent la connexion au réseau radioélectrique mobile, c'est-à-dire au réseau sur lequel transitent les communications électroniques des téléphones portables. Les opérateurs visés par cette autorisation sont les opérateurs d'importance vitale (OIV) dans le secteur des télécoms. Leur liste est confidentielle, mais on peut avancer sans trop de risque qu'elle comprend les quatre principaux opérateurs nationaux.

Cette autorisation, destinée à préserver les intérêts de la défense et de la sécurité nationale, sera octroyée pour un ou plusieurs modèles et une ou plusieurs versions des appareils concernés. Cela permettra d'éviter de possibles lourdeurs administratives et de garantir, en conséquence, la liberté et la rapidité de déploiement des réseaux de communications électroniques.

Le Premier ministre pourra aussi refuser l'autorisation s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale, c'est-à-dire que le respect des règles de confidentialité, d'intégrité, de sécurité et de continuité de l'exploitation des réseaux et de la fourniture de services n'est pas garanti. Il disposera enfin d'un pouvoir d'injonction en cas d'exploitation sans autorisation d'un appareil pourtant soumis au régime d'autorisation préalable.

L'article 2 détermine un régime de sanction pénale en cas d'infraction aux dispositions du nouveau régime de contrôle. Il crée deux infractions : l'exploitation sans autorisation préalable d'appareils permettant la connexion au réseau mobile et la non-exécution, totale ou partielle, des injonctions du Premier ministre. Il prévoit une peine d'un an d'emprisonnement et de 150 000 euros d'amende pour toute personne physique déclarée responsable d'une de ces infractions. Le juge pourra également prononcer la confiscation des matériels ou leur destruction, ainsi qu'une interdiction de trois ans maximum d'établissement de réseaux électroniques.

Les personnes morales déclarées responsables pénalement encourent, quant à elles, une amende dont le taux maximal est égal au quintuple de celui prévu pour les personnes physiques. Comme pour les personnes physiques, des sanctions complémentaires seront applicables aux personnes morales. Le juge pourra prononcer l'interdiction définitive, ou pour une durée de cinq ans,

d'exercer une activité d'exploitation de réseaux radioélectriques mobiles et la diffusion de la décision prononcée.

Enfin, le troisième et dernier article de cette proposition de loi prévoit que ce régime d'autorisation préalable sera applicable à l'exploitation des appareils installés depuis le 1er février 2019. L'application rétroactive de ce dispositif implique que les opérateurs concernés préparent des dossiers de demande d'autorisation dès l'entrée en vigueur de la loi, pour des équipements déjà mis en place. Ils disposeront d'un délai de deux mois à compter de cette entrée en vigueur pour déposer leur demande.

Il va de soi que ce dispositif a été élaboré en concertation étroite avec les acteurs privés directement concernés et avec les autorités de régulation. Il vise à garantir un développement soutenable et sûr de la 5G et de ses usages en France. Il s'agit moins de faire la révolution que de faire évoluer une doctrine à laquelle les acteurs sont accoutumés. Je veillerai personnellement à ce que ce dispositif demeure suffisamment souple pour ne pas brider les capacités d'innovation des opérateurs, des équipementiers et des industriels, ni retarder l'arrivée de la 5G sur l'ensemble de notre territoire.

Mes chers collègues, la réussite du déploiement de la 5G est, vous l'aurez compris, un enjeu stratégique pour la France. En garantissant sa sécurité, nous préparons notre pays aux innovations et aux investissements de demain.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. La sécurité des réseaux de communication est décisive pour la protection de nos données et pour notre souveraineté technologique. Je me félicite que l'Assemblée nationale se soit saisie aussi rapidement de ce sujet stratégique pour notre économie car nous vivons, avec l'avènement de la 5G, un moment de transformation technologique historique. La 5G va offrir des débits dix fois supérieurs à la 4G, diviser par dix les délais de transmission et renforcer la fiabilité de nos communications. Mais surtout, elle va permettre de développer des technologies de rupture, qui vont bouleverser toutes nos industries : la réalité augmentée sera plus facilement utilisée dans les processus de production, la robotique sera plus efficace, l'espérance de vie des batteries des objets connectés pourrait être allongée de dix ans et les communications entre véhicules seront facilitées, ce qui est crucial pour le développement du véhicule autonome.

Nous sommes entrés dans une course au déploiement de la 5G et les premiers États qui en développeront l'usage seront à même de mettre en œuvre les plus grandes avancées technologiques et industrielles. La 5G, c'est moins un enjeu « B2C » (« *Business to Consumer* »), sauf dans les agglomérations extrêmement denses, qu'un enjeu « B2B » (« *Business to Business* »), c'est-à-dire en direction des entreprises. C'est pourquoi nous avons dessiné, dès l'été dernier, une feuille de route ambitieuse pour la 5G, et surtout pour développer le plus rapidement possible ses usages industriels et ceux liés aux infrastructures. Le déploiement à

venir de la 5G constitue donc un événement structurant pour le secteur des télécommunications et, plus largement, pour l'ensemble des entreprises. Les objectifs du Gouvernement sont ambitieux, puisque la feuille de route publiée le 16 juillet 2018 identifie quatre chantiers : libérer et attribuer les fréquences radioélectriques pour les réseaux 5G ; favoriser le développement de nouveaux usages, notamment industriels ; accompagner le déploiement des infrastructures de la 5G ; assurer, enfin, la transparence et le dialogue sur le déploiement de la 5G et l'exposition du public.

Néanmoins, nous ne pouvons pas innover sans maîtriser pleinement la sécurité de nos réseaux. Dans ce contexte de numérisation de la société, la maîtrise de la sécurité des réseaux est absolument essentielle pour protéger les citoyens et les entreprises et pour assurer la souveraineté de la Nation. C'est un enjeu majeur qui ne doit pas être négligé car, au-delà des nouveaux usages dont elle sera le support, la 5G renforcera, du fait de ses spécificités technologiques, les menaces qui pèsent sur la sécurité et l'intégrité des communications électroniques. Cette nouvelle réalité technologique exige des réponses appropriées. C'est pourquoi il est aujourd'hui nécessaire de renforcer et de compléter le cadre juridique applicable, afin de créer les leviers qui permettront de contrôler efficacement les équipements du réseau 5G. Tel est l'objectif de la proposition de loi que nous examinons aujourd'hui.

Ce contrôle renforcé passe par une mesure concrète : soumettre à autorisation préalable du Premier ministre l'exploitation de nouveaux équipements d'antennes mobiles pour les opérateurs de télécommunications qui sont opérateurs d'importance vitale. Ce dispositif de contrôle, fondé sur des motifs de sécurité et de défense nationale, permettra d'assurer le respect de ces principes de précaution dans le déploiement de la 5G. Il complète des dispositifs déjà en place, notamment celui qui repose sur l'article R. 226-3 du code pénal relatif à la protection du secret des correspondances.

J'aimerais néanmoins fixer deux limites à cet impératif de protection des réseaux. Premièrement, « protection » ne peut pas rimer avec « discrimination » : tous les équipementiers, sans distinction, seront soumis aux mêmes règles, car des vulnérabilités ou des failles de sécurité peuvent être constatées chez chacun d'entre eux. J'y insiste, afin de dissiper les fantasmes qui peuvent entourer cette proposition de loi. Deuxièmement, ces nouvelles protections ne doivent pas retarder l'innovation. Ce nouveau régime de contrôle doit être mis en place sans créer de surcharge administrative qui ralentirait le déploiement du « *New Deal* mobile » ou de retarder la réussite de la 5G. Vous savez l'attachement du Gouvernement au déploiement du « *New Deal* mobile » 4G ou 4G + : nous sommes en train de tripler le rythme de déploiement des pylônes. Les opérateurs de télécommunications se sont engagés dans des programmes d'investissement sur plusieurs années pour améliorer la qualité de leurs réseaux fixe et mobile. Si nous voulons permettre à tous les Français et à toutes les entreprises d'avoir accès à un très haut débit de qualité, nous devons établir des règles claires, simples et stables, qui ne limitent pas la capacité d'investissement et de déploiement des opérateurs.

Tels sont les quelques messages que je voulais vous transmettre au moment d'entamer l'examen de cette proposition de loi.

M. Mickaël Nogal, président. Nous allons maintenant entendre les orateurs des groupes.

Mme Christine Hennion. Nous examinons ce matin une proposition de loi singulière qui, à bien des égards, pourrait même sembler paradoxale. Ce texte a été longuement commenté mais, au final, assez peu explicité. C'est un texte purement technique, dans lequel certains ont cherché, en vain, une fin politique. Un texte, enfin, qui introduit un régime d'autorisation, tout en se voulant favorable à l'innovation. Il se veut favorable à l'innovation, car on ne peut décemment envisager le développement du véhicule autonome, de la télémédecine, de l'industrie 4.0 et de nouveaux usages sans assurer la sécurité effective de nos réseaux mobiles du futur.

Le dispositif que nous vous soumettons est le fruit d'une certitude, d'une volonté et d'une méthode.

Une certitude, d'abord : du fait de certaines spécificités techniques, telles que la multiplication des antennes, le déport de l'intelligence du cœur de réseau vers ces antennes ou la généralisation de la virtualisation, le déploiement de la 5G pourrait présenter des risques plus grands que la 3G et la 4G en matière de cybersécurité. En cela, la 5G ne doit pas être appréhendée comme une simple évolution de la 4G, mais bien comme un véritable saut technologique, nécessitant des précautions particulières en matière de sécurité. Il y va à la fois de notre souveraineté et de notre compétitivité économique à long terme.

Une volonté ensuite : celle de concilier ces impératifs de sécurité avec le respect des calendriers de déploiement des réseaux mobiles. Le dispositif vise en effet à garantir un développement soutenable de la 5G sans alourdir de manière disproportionnée les charges administratives pesant sur les opérateurs.

Une méthode, enfin, qui a reposé sur un dialogue étroit avec l'ensemble des acteurs concernés : équipementiers, opérateurs et administrations. Personne n'est pris au dépourvu, puisque chacun a pu faire valoir sa position. Je tiens d'ailleurs à remercier M. Éric Bothorel pour la qualité des auditions qu'il a menées, auxquelles il a associé l'ensemble des députés intéressés.

Nous ne faisons pas cavalier seul et notre démarche, celle de la France, s'inscrit pleinement dans le plan proposé par la Commission européenne à la demande des États membres, qui consiste à se construire, d'ici au mois de juin, un ensemble de règles pour garantir la sécurité des réseaux 5G. Nous devons nous réjouir de cette prise de conscience et saisir l'occasion qui nous est donnée d'assurer la sécurité des réseaux de demain et la confiance dans leurs usages. C'est pourquoi les députés du groupe La République en Marche voteront cette proposition de loi.

M. Jérôme Nury. Cette proposition de loi touche à un sujet majeur et stratégique à plusieurs titres, d'abord parce qu'il y va de notre sécurité nationale et de notre souveraineté, sujets hautement sensibles, ensuite parce que la technologie dont il est question va révolutionner nos usages du numérique.

Sur le premier point, le groupe Les Républicains est évidemment favorable aux mesures relatives à la sécurisation des réseaux et à la protection des données des utilisateurs, qu'ils soient privés, publics ou industriels. Sur tous les réseaux, quels qu'ils soient, transitent de plus en plus d'informations personnelles ou sensibles, dont certaines sont d'une importance vitale pour la sécurité de notre pays, de nos concitoyens et de nos entreprises. Il est essentiel d'avoir des garanties de confidentialité et de non-divulgation à des tiers, à d'autres pays ou à des entreprises concurrentes. Sur le fond, il est donc important de légiférer et de renforcer notre arsenal de contrôle et de répression pour ne pas nous exposer à des intentions malveillantes qui mettraient à mal les intérêts du pays et de ses habitants.

S'agissant de la technologie elle-même, la 5G ne va pas seulement faire évoluer, mais bouleverser nos usages, ceux du nomadisme connecté. Le passage de la 2G à la 3G, puis de la 3G à la 4G, n'a pas été le fruit d'une révolution technologique. Mais la 5G, elle, est une révolution, celle de l'hyper-connectivité et du déploiement à grande échelle de l'intelligence artificielle, des véhicules autonomes et des objets connectés et intelligents. Ce basculement vers un monde totalement immergé dans le numérique, sans limite de puissance ni de réactivité, impose donc la plus grande vigilance quant à la sécurité de ce nouveau réseau.

Avant d'aller plus avant dans l'examen de ce texte, j'aimerais faire deux remarques.

La première porte sur la forme. Le Gouvernement a beaucoup trop tardé à introduire cette notion de sécurité dans la technologie mobile et 5G. Alors que l'on savait depuis longtemps que l'attribution des fréquences devait se faire en 2019, c'est seulement au cours de l'examen du projet de loi relatif à la croissance et la transformation des entreprises (PACTE) que le Gouvernement a réagi, en déposant un amendement constituant un cavalier législatif, qui n'a finalement pas été retenu par le Sénat – ce qui a peut-être évité au texte de passer sous les fourches caudines du Conseil constitutionnel. Cette proposition de loi arrive très tardivement sur le bureau de l'Assemblée nationale, un peu en catastrophe, sans étude d'impact, sans avoir fait l'objet d'une concertation, et dans une rédaction restreinte, qui laisse le législateur à l'écart.

Deuxièmement, ce texte repose sur un principe ultra-discrétionnaire et technocratique. Il faut veiller, tout en sécurisant les réseaux, à ce que cette nouvelle réglementation n'ait pas pour effet de réduire la concurrence entre les équipementiers. Toute complexification à l'excès, toute élimination *de facto* ou *a priori* d'un équipementier, tout délai d'autorisation trop long aura des conséquences qui pourraient être dévastatrices pour notre pays, tant dans le

déploiement complémentaire de la 4G que dans le déploiement futur de la 5G : hausse des prix du déploiement, baisse de la qualité technologique, retard dans le déploiement et dans la mise en œuvre du « *New Deal* », pouvant aller jusqu'au démontage éventuel d'éléments actifs installés sur les pylônes depuis le début de l'année, retard dans l'attribution des licences 5G et donc de la couverture en France.

Compte tenu des risques énumérés dans ce texte, il semblerait judicieux et sécurisant pour le Parlement et les professionnels du secteur – opérateurs, équipementiers et sous-traitants – de mener de front le volet législatif contenu dans cette proposition de loi et le volet réglementaire, pour travailler ensemble sur la liste des équipements concernés et les modalités opérationnelles de dépôt des dossiers. Nous pourrions ainsi concilier efficacité technologique et économique et sécurité nationale. En cela, nous pouvons nous retrouver sur ce texte.

Mme Laure de La Raudière. La 5G porte mal son nom : comme vous l'aviez dit, Monsieur le rapporteur, c'est une vraie rupture technologique dans l'organisation et l'architecture des réseaux de téléphonie mobile. Les nouveaux services offerts par la 5G sont proprement enthousiasmants, qu'il s'agisse des voitures connectées et autonomes, de la téléchirurgie ou des nombreux usages qui vont naître dans le domaine de l'industrie et des loisirs. Tous ces services nécessitent à la fois des débits beaucoup plus puissants, mais aussi un temps de transmission beaucoup plus court qu'avec les réseaux 4G actuels. Ils exigent aussi une sécurité absolue des réseaux pour éviter le piratage des données et des systèmes.

Le débat ouvert par cette proposition de loi est non seulement bienvenu, mais nécessaire, avant l'attribution des fréquences 5G aux opérateurs en France. Étant donné l'importance de cet enjeu pour le développement économique de notre pays, il est stratégique d'en débattre dès maintenant afin que la France ne prenne pas de retard.

Je souhaiterais néanmoins, au nom du groupe UDI, Agir et Indépendants, faire quelques remarques au Gouvernement et au rapporteur. Premièrement, par le fait qu'il s'agit d'une proposition de loi, et non d'un projet de loi, nous n'avons pas d'étude d'impact. Or il est probable que cette mesure aura des conséquences importantes sur les opérateurs et sur les constructeurs. Deuxièmement, en agissant de son côté, la France semble faire fi de la communication de l'Union européenne du 26 mars 2019, qui appelle à une approche commune : pourquoi ne pas avoir choisi une approche négociée au niveau européen ?

J'ai également un certain nombre de questions techniques à vous poser. Comment se passe concrètement la transformation d'une antenne 4G en 5G ? Vous nous avez invités à vos auditions, Monsieur le rapporteur, mais elles ont eu lieu pendant le déplacement de la commission des affaires économiques à Bruxelles, si bien qu'un certain nombre d'entre nous n'a pas pu y assister. Comment un opérateur pourra-t-il mettre à jour son réseau si le constructeur qu'il

avait choisi pour la 4G n'est pas retenu pour la 5G ? Comment se fera l'autorisation des mises à jour logicielles, très fréquentes sur ce type d'équipement et qui risquent de l'être encore plus avec la 5G ?

J'entends dire que les opérateurs décideront si ces mises à jour logicielles doivent faire, ou non, l'objet d'une validation par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Si tel n'est pas le cas, qui exercera ce contrôle ? Quelles sanctions spécifiques sont prévues pour les opérateurs qui ne feraient pas le nécessaire en matière de déclaration auprès de l'ANSSI ? Comment l'opérateur sera-t-il tenu informé de ce que contiennent les mises à jour en cas de non-communication du constructeur ? Et quels sont les moyens de recours vis-à-vis du constructeur, si c'est lui qui est en faute ? Ne faut-il pas durcir le régime des sanctions appliquées aux opérateurs pour les mises à jour des logiciels, dès lors que l'obligation de déclaration leur incombe ?

Même si cette proposition de loi est nécessaire, il subsiste de nombreuses zones d'ombre et il aurait été souhaitable de bénéficier d'une réelle étude d'impact.

Mme Marie-Noëlle Battistel. Les équipements qui supporteront les nouveaux réseaux de cinquième génération feront potentiellement courir de nouveaux risques en matière de cybersécurité, du fait de plusieurs facteurs qui ont déjà été relevés par le rapporteur et la secrétaire d'État : leurs caractéristiques intrinsèques et leurs spécificités techniques, d'abord ; l'usage de la 5G dans certains domaines industriels critiques, notamment les véhicules connectés et les réseaux d'énergie, ensuite ; des obligations légales, enfin, qui pourraient contraindre les opérateurs à coopérer avec des États étrangers dans la collecte de renseignement.

L'exploitation des faiblesses des équipements de desserte des réseaux 5G, du fait d'erreurs ou de défauts de conception, volontaires ou non, pourrait porter atteinte à la sécurité nationale. La mise en place de la 5G a pris une dimension politique européenne et internationale, du fait des fortes craintes exprimées par les États-Unis sur la probité de l'opérateur chinois Huawei. Cette crainte s'exprime dans le contexte particulier d'une guerre commerciale larvée entre les deux grandes puissances. Les États-Unis, par le biais de leur ambassadeur à Berlin, ont notamment sommé l'Allemagne d'exclure l'opérateur chinois de l'appel d'offres d'ouverture à la 5G sur son territoire national, sous peine de renoncement à tout échange de renseignement entre les deux pays. L'Allemagne, qui tire une grande partie de ses exportations du commerce avec la Chine, a refusé cet ultimatum, mais a affirmé vouloir prendre toutes les précautions nécessaires au niveau technique.

Avec cette proposition de loi du groupe majoritaire, qui introduit un régime d'autorisation préalable pour certains équipements radioélectriques, la France semble s'engager dans une voie qui lui permettra d'interdire les opérateurs qui ne respecteraient pas les conditions légales d'intégrité et de sécurité des

réseaux. Il faut noter que l'agenda européen percutera probablement l'examen de cette proposition de loi, puisqu'un important sommet de l'Union européenne avec la Chine aura lieu le 9 avril, la veille de son examen en séance publique.

Ce texte prévoit l'obligation de formuler une demande d'autorisation préalable au Premier ministre avant toute exploitation de certains équipements radioélectriques. Ce dernier déterminera « s'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale, en se basant sur les critères définis dans la loi et notamment au regard des garanties que présente l'équipement pour l'intégrité, la sécurité et la continuité de l'exploitation des réseaux ». Devront ainsi être respectées les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service, les conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications et, enfin, les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique. La liste des équipements soumis au régime d'autorisation sera d'ailleurs publiée et régulièrement actualisée. Il sera notamment porté attention au fait que les opérateurs ne soient pas soumis à l'ingérence d'États non membres de l'Union européenne. Cette autorisation sera délivrée pour un ou plusieurs modèles et un périmètre géographique pour une durée maximale de huit ans. La proposition de loi prévoit également, en cas d'infraction à ce dispositif, des peines d'emprisonnement et des amendes.

Madame la secrétaire d'État, Monsieur le rapporteur, le groupe Socialistes et apparentés est *a priori* favorable à cette proposition de loi, mais nous souhaitons faire deux remarques à ce stade des débats. Premièrement, il nous semble nécessaire que la décision du Premier ministre soit pleinement éclairée et rendue après avis de l'ANSSI. Nous proposerons donc un amendement en ce sens. Deuxièmement, les opérateurs craignent que les délais d'instruction prévus par la présente proposition de loi aient pour effet de ralentir le déploiement des réseaux 4G et 5G. Pouvez-vous, Monsieur le rapporteur, nous donner votre avis sur ce point ?

M. Jean-Luc Lagleize. Les réseaux de télécommunications de cinquième génération formeront, d'ici à quelques années, l'épine dorsale de nos sociétés et de nos économies, reliant des milliards d'objets et de systèmes, y compris dans les secteurs critiques comme l'énergie, les transports, les banques, la santé ou l'industrie. Ces réseaux de cinquième génération n'en sont certes qu'à leurs débuts, mais le groupe du Mouvement démocrate et apparentés se réjouit de voir que l'Union européenne et la France se positionnent d'ores et déjà à l'avant-garde de cet essor.

Dès septembre 2016, dans un plan d'action pour la 5G, l'Union européenne s'est fixée comme objectif pour 2025 que les zones urbaines, ainsi que les principaux axes routiers et ferroviaires, disposent d'une couverture 5G. L'Union européenne s'est également fixée comme objectif intermédiaire, dès

2020, que la 5G soit disponible dans au moins une grande ville de chaque État membre. La France a également présenté sa feuille de route pour la 5G en juillet 2018, afin d'accompagner et de faciliter le déploiement de cette innovation de rupture. Depuis lors, les pouvoirs publics se sont pleinement mobilisés pour décliner cette feuille de route, par exemple en octroyant des autorisations d'utilisation de fréquences à des fins d'expérimentation, en créant un guichet pilote 5G ou en évaluant l'impact sanitaire associé au déploiement de la 5G.

Malgré les prouesses à court terme que nous promet cette technologie émergente, qui allie équipements physiques et solutions logicielles, nous devons appliquer le principe de précaution et nous protéger en renforçant nos infrastructures critiques. Dans un futur proche, les réseaux 5G véhiculeront des informations de plus en plus sensibles et leur vulnérabilité pourrait être exploitée pour mettre en péril ces systèmes et ces infrastructures numériques, ou pour voler ou espionner des données à grande échelle. Face à ces risques majeurs, le groupe du Mouvement démocrate et apparentés salue les recommandations opérationnelles émises par la Commission européenne la semaine dernière pour garantir un niveau élevé de cybersécurité des réseaux 5G dans l'ensemble de l'Union européenne. Toute vulnérabilité ou cyberattaque qui ciblerait les futurs réseaux 5G dans un État membre affecterait potentiellement l'Union dans son ensemble. Pour cette raison, ces recommandations comportent précisément des mesures à prendre au niveau national et européen.

Au travers de cette proposition de loi visant à préserver les intérêts de sa défense et de sa sécurité nationale dans le cadre de l'exploitation des réseaux radioélectriques mobiles, la France prend ainsi les devants en ce qui concerne le niveau national. Grâce au régime d'autorisation préalable du Premier ministre et aux sanctions pénales en cas d'infraction, nous minimisons les risques et les incertitudes pesant sur les opérateurs qui souhaitent investir dans ce secteur, tout en maximisant notre stratégie de défense et de sécurité nationale. Cette proposition de loi, que nous espérons voir adopter dans les meilleurs délais, nous paraît donc équilibrée.

Conformément à l'ambition du groupe du Mouvement démocrate et apparentés de renforcer le rôle et les missions du Parlement, nous avons déposé une série d'amendements, qui font écho aux avancées à l'article 55 *bis* du projet de loi PACTE, lequel prévoit la remise d'un rapport au Parlement sur l'action du Gouvernement en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation, ainsi qu'en matière de contrôle des investissements étrangers. Les rapports que nous proposons d'introduire pourraient donner à la Représentation nationale une meilleure lisibilité de l'évolution des investissements directs étrangers dans ce secteur stratégique des équipements de réseaux radioélectriques.

Notre groupe votera cette proposition de loi et restera attentif aux actions menées par la France au niveau européen pour assurer la sécurité des réseaux 5G.

M. François Ruffin. Je souhaite faire deux remarques préalables.

Premièrement, pour les membres du groupe La France insoumise, le progrès ne viendra pas demain du progrès technologique, il ne viendra pas d'une technologie cent fois plus puissante que la 4G, ni de téléphones portables connectés au frigo et au grille-pain, ni même de la croissance ; il viendra de la qualité des relations nouées, au sein de notre société, entre les humains.

Deuxièmement, à l'heure où nous passons à la 5G, il reste encore des centaines, voire des milliers de zones dans notre pays, où l'on n'a encore ni la 2G, ni la 3G, ni la 4G. Le risque, c'est d'avoir demain un réseau de classes avec, d'un côté, une avant-garde qui bénéficiera de la 5G dans les territoires urbains, avec des trucs ultra-puissants, et, de l'autre, les laissés-pour-compte du numérique. Je sais bien qu'un « *New Deal* mobile » est en route, mais il avance à petits pas et il laisse beaucoup de zones grises, voire de zones blanches.

J'en viens à la proposition qui est sur la table. Nous pensons qu'il faut effectivement garantir la souveraineté nationale sur le réseau 5G, ne pas en faire un cheval de Troie au bénéfice des Chinois ; mais nous devons tout autant nous protéger contre le cheval de Troie des États-Unis. Ce pays pratique un espionnage massif, avec IBM, les câbles sous-marins et les données numériques : on l'a vu au moment de l'affaire Snowden. La Chine serait une menace, mais pas les États-Unis ? Nous, nous considérons que la menace pour la souveraineté nationale est tout aussi réelle quand elle est américaine.

Enfin, je ne comprends pas pourquoi la préservation de la souveraineté nationale se limiterait au développement de la 5G. On aurait dû également intervenir à ce titre dans les dossiers Alcatel, Alstom ou Péchiney – M. Emmanuel Macron était alors ministre de l'économie – qui mettaient en jeu des technologies très précieuses, voire stratégiques, pour notre pays. Je mentionnerai une entreprise située dans la commune de Longvic, à côté de Dijon, où je me suis rendu récemment : cette entreprise, Francéole, est la seule en France à fabriquer des mâts d'éoliennes. Ce marché est en pleine croissance. Pourtant, cette entreprise est en train de disparaître parce qu'on n'a pas fait le nécessaire pour favoriser son accès au crédit et lui garantir un minimum de protection – faute de quoi, elle est cuite !

Pour le groupe La France insoumise, notre souveraineté, qu'on invoque pour la 5G à propos du Chinois Huawei, doit également être préservée dans un certain nombre d'autres domaines industriels.

M. Alain Bruneel. Certes, la proposition de loi qui nous est soumise a pour objet de sécuriser et de protéger nos industries et nos concitoyens. Mais je m'interroge sur notre faiblesse industrielle dans ce nouveau secteur technologique. Rappelons qu'Alcatel, entreprise française, leader dans les télécoms et les réseaux, a été rachetée, en 2015, par Nokia. De surcroît, cette dernière entreprise, qui réalise des bénéfices si considérables qu'elle a distribué 1,8 milliard de dividendes, licencie plus de 2 000 personnes en Europe, dont la moitié sur le

territoire français. Je suis d'autant plus inquiet qu'elle bénéficie d'aides de l'État, au titre du crédit d'impôt recherche – 76 millions d'euros l'an dernier – ou d'exonérations de charges sociales.

La question du groupe de la Gauche démocrate et républicaine (GDR) est donc très simple : quelle est la stratégie industrielle de la puissance publique concernant des entreprises aussi stratégiques que celles des télécommunications ?

M. Thomas Gassilloud, rapporteur pour avis de la commission de la défense. C'est un honneur pour moi de venir vous présenter les travaux de la commission de la défense nationale et des forces armées sur ce texte, dont elle a souhaité se saisir pour avis en raison des enjeux importants pour la défense et la sécurité nationale qui s'y attachent. Il est plaisant, du reste, d'entendre parler de sécurité, de souveraineté et de défense nationale au-delà de l'enceinte de notre commission…

La 5G marque une véritable rupture technologique en ce qu'elle ouvre la voie, beaucoup plus que la 4G, à des applications nouvelles grâce à un débit plus important, à de moindres temps de latence et à des fonctions avancées. Cependant, la commission de la défense est particulièrement sensible au revers de la médaille, c'est-à-dire aux nouvelles vulnérabilités que la 5G créera dans nos réseaux. Ces vulnérabilités résultent, en premier lieu, de la virtualisation croissante des équipements et de l'architecture même des réseaux, qui sera beaucoup plus déconcentrée et maillée que celle des précédentes générations. En effet, il est plus facile de sécuriser un réseau lorsqu'on peut, comme c'est le cas actuellement, concentrer les contrôles sur les corps de réseaux et quelques zones sensibles que lorsque chaque antenne est une porte d'entrée pour des interceptions ou une source de failles. Or les enjeux de sécurité nationale et de défense sont importants, car nos sociétés ont besoin de résilience : les réseaux ont, à cet égard, une « importance vitale », pour reprendre les termes du code de la défense.

Vélocité, résilience, temps de latence de quelques millisecondes : autant d'atouts qui intéressent le monde de la défense, pour des raisons que chacun comprendra. En effet, les forces de sécurité utilisent de plus en plus les réseaux civils dans l'accomplissement de leurs missions, que ce soit les armées, dans le cadre de l'opération Sentinelle, ou la gendarmerie nationale, qui historiquement dispose toujours de son propre réseau, RUBIS, mais qui bascule progressivement vers les réseaux mobiles civils : vous connaissez sans doute tous l'application Néogend, qui permet à nos gendarmes de disposer de terminaux tactiques pour interroger les bases de données.

Pour ces différentes raisons, la commission de la défense soutient pleinement ce texte. Ses débats ont été intenses et, je le crois, productifs. Si je devais en résumer l'esprit, je dirais, au risque de surprendre ceux qui auraient pu craindre de notre part une approche trop sécuritaire, que nous nous sommes attachés à veiller au maintien du bon équilibre entre deux impératifs qu'il nous faut concilier dans ce texte : d'une part, l'impératif de résilience des réseaux et de

sécurité et, d'autre part, l'impératif économique et d'aménagement numérique du territoire, qui suppose de ne pas entraver le déploiement rapide de la 5G.

Soucieux de ne pas saturer votre commission d'amendements susceptibles de rompre cet équilibre, nous nous en sommes tenus à une approche très raisonnable qui nous conduit à vous soumettre un seul amendement, que j'aurai l'occasion de vous présenter lors de la discussion des articles.

M. Éric Bothorel, rapporteur. Merci à toutes et à tous pour vos observations et vos questions, auxquelles je vais tâcher d'apporter des réponses. En tout état de cause, la discussion des articles nous permettra de revenir en détail sur un certain nombre des points que vous avez abordés.

En préambule, puisque nous accueillons, ici, en la personne de son rapporteur pour avis, un représentant de la commission de la défense, permettez-moi d'avoir une pensée pour le militaire tombé hier, au Mali, dans le cadre de l'opération Barkhane.

Monsieur Nury, puisque vous avez employé le mot « bannissement », je veux être tout à fait clair sur la portée et l'ambition de cette proposition de loi. Il ne s'agit pas de bannir quelque acteur que ce soit, mais de soumettre l'ensemble de la filière, industriels et opérateurs, à un régime qu'ils connaissent déjà, puisque nous faisons simplement évoluer la doctrine actuellement appliquée aux réseaux 3G et 4G et qui mobilise les effectifs nombreux d'une agence mondialement reconnue et que nous apprécions tous : l'ANSSI. Du reste, je veux insister sur le fait que, si l'hétérogénéité du parc, la diversité des acteurs, est un facteur de concurrence profitable à la filière, qui réalise des investissements considérables et a besoin de cette concurrence pour déployer les meilleurs services dans les meilleures conditions, notamment au meilleur prix, elle est également consubstantielle à notre sécurité.

À aucun moment, le législateur ne considère que, parmi celles et ceux qui prétendent participer au déploiement des infrastructures 5G, une nationalité serait moins fréquentable qu'une autre. Qu'ils soient européens, chinois ou, pourquoi pas, coréens – puisque plusieurs acteurs coréens frappent à la porte de l'Europe –, l'ensemble des acteurs devront se soumettre à cette doctrine. Le regard qui sera porté sur leur candidature sera technique et technologique dans la mesure où les enjeux de sécurité sont d'abord un sujet technique et technologique.

Monsieur Ruffin, la 5G n'a pas vocation à combler les carences de la couverture mobile dans l'accès aux services de voix ou à internet. Ses usages seront, en priorité, liés au véhicule autonome ou à la médecine connectée, par exemple, qui ont besoin de débits très élevés et de temps de latence très faibles. Mais, puisque vous évoquez la couverture mobile, qu'il me soit permis de rappeler les travaux réalisés au sein de cette commission dans le cadre de l'examen de la loi portant évolution du logement, de l'aménagement et du numérique (ELAN). La réduction des délais d'instruction des dossiers permet, par exemple, de réduire les

zones blanches grâce à la couverture de 600 à 700 sites par an ou de viser l'installation de 4 000 sites en 4G. La situation s'améliore donc, même si je comprends l'impatience de celles et ceux qui ne sont pas encore servis. La filière télécoms a investi, l'an dernier, l'équivalent de 200 rames de TGV. Mais tous les trains n'arrivent pas au même endroit et à la même heure… Néanmoins, je ne doute pas que l'accélération qui est en cours finira par porter ses fruits. Même si nous entendons déployer la 5G, nous ne renonçons en rien à notre ambition de poursuivre l'accélération du déploiement de la 4G et du réseau fixe.

Madame de La Raudière, vous avez raison, la mise à jour vers la 5G n'est pas simple. Actuellement, la compatibilité ascendante ou descendante des systèmes n'est pas forcément parfaite, de sorte qu'il est fort probable que, faute de standardisation, vous deviez faire appel, pour la 5G, au constructeur de la base 3G et 4G de l'antenne. Certains industriels prônent une forme de standardisation, mais elle n'a pas cours et n'est pas défendue par le 3GPP (*3rd Generation Partnership Project*). On assiste donc quasiment à une « propriétisation » des infrastructures. Ainsi, l'hétérogénéité du parc devrait être respectée, car la répartition des parts de marché entre les différents acteurs devrait quasiment se stabiliser. En tout état de cause, ce n'est pas le législateur qui administre les réseaux télécoms en décidant que tel acteur, à tel endroit, se verra attribuer tel service ; c'est la concurrence entre les industriels qui en décidera. Il appartient aux opérateurs qui s'apprêtent à lancer des consultations dans le cadre du déploiement de la 5G de savoir avec qui ils souhaitent contractualiser. Le législateur n'intervient pas en la matière.

Mme Laure de La Raudière. Et si un constructeur n'a pas l'autorisation ?

M. Éric Bothorel, rapporteur. Cela s'est déjà produit, et les opérateurs savent s'adapter ; mais, le but du jeu, vous l'aurez compris, n'est pas de bannir un constructeur. Entendons-nous bien : il nous faut trouver un équilibre entre, d'une part, la sécurité et, d'autre part, la performance de l'innovation. Chaque semaine, le CERT (*Computer Emergency Response Team*) publie un certain nombre de vulnérabilités d'équipements. Or, celles-ci ne concernent pas uniquement des équipementiers asiatiques, elles concernent aussi des équipementiers américains. Nous sommes, dans ce domaine, dans une course contre la montre. Un membre des forces spéciales à qui l'on demandait quel avantage il souhaitait avoir sur son ennemi a répondu : une seconde ou une demi-seconde d'avance… En matière de cybersécurité, il existe, entre ceux qui cherchent à nuire à nos intérêts ou à pénétrer nos systèmes – que ce soit des proto-États, des États ou des organisations criminelles – et ceux qui cherchent à leur résister, avec le secours de la loi, une compétition pour avoir, sur l'autre, un temps d'avance. Parfois, cet avantage se perd parce que ceux qui cherchent à nous nuire finissent par repérer des failles ou des vulnérabilités ; et le risque est d'autant plus grand que ces infrastructures sont de moins en moins matérielles et de plus en plus logicielles. La révolution de la 5G se caractérise précisément par la virtualisation des réseaux.

Quant à la question de l'étude d'impact, elle a été abordée au Sénat lorsque le Gouvernement a présenté ce dispositif. Nous le verrons ultérieurement, nombre d'amendements tendent à imposer l'avis de telle ou telle instance. Il est légitime que l'Autorité de régulation des communications électroniques et des postes (ARCEP) ou l'ANSSI soient consultées. Mais on ne peut pas, d'un côté, affirmer qu'il faut aboutir très rapidement à un dispositif sécurisé et opérationnel parce que l'attribution des fréquences et la libération du marché interviendront en 2020 et, de l'autre, multiplier des consultations qui demandent du temps. De fait, même si l'on réalise une étude d'impact sur la base des quelques villes où la 5G a été déployée à titre expérimental, nous n'aurons un véritable retour d'expérience qu'avec le premier cas d'usage à l'échelle industrielle. Je souhaite moi-même qu'une étude d'impact soit réalisée mais, plutôt que de demander des rapports au Gouvernement, je préférerais que des organismes tels que la Commission supérieure du numérique et des postes, par exemple, s'autosaisissent et produisent, d'ici à quelques mois, leurs propres évaluations.

En ce qui concerne la Commission européenne, vous avez raison, nous sommes plutôt en avance sur le calendrier qu'elle a arrêté la semaine dernière. En effet, il est prévu que chaque État prenne ses dispositions d'ici à l'été et que des rendez-vous soient organisés en septembre ou en octobre pour mettre en commun les différents travaux réalisés autour de la 5G et envisager l'élaboration, à l'échelon européen, d'une doctrine plus générale et partagée de notre approche de cette technologie, notamment en matière de sécurité. La position exprimée par la Commission européenne la semaine dernière ne me paraît donc pas en contradiction avec l'examen de cette proposition de loi.

Telles sont les réponses que je pouvais apporter aux différentes questions qui m'ont été posées, mais je ne doute pas que nous entrerons davantage dans le détail lors de l'examen des articles.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Je commencerai par évoquer l'Europe, puisque M. le rapporteur a conclu sur ce point. Les conditions du déploiement de la 5G relèvent, en effet, d'une compétence nationale exclusive. Ce que demande l'Union européenne à ce stade, ce sont des recommandations pour une approche commune. Elle a fixé le calendrier suivant : l'évaluation des risques doit être faite, au niveau national, avant le 30 juin 2019 et, au niveau de l'Union européenne, avant le 1er octobre ; la convergence doit intervenir avant le 31 décembre, une évaluation étant prévue au 1er octobre 2020. L'Union européenne reconnaît la compétence nationale, mais elle propose que les États échangent des informations, avec le soutien de la Commission et de l'Agence de l'Union européenne pour la cybersécurité. Elle souhaite que chaque État soit conscient des risques et prenne les mesures nécessaires pour y faire face. Nous nous inscrivons donc parfaitement dans le dispositif européen et, comme l'indiquait M. le rapporteur, nous sommes même plutôt en avance sur le calendrier.

Par ailleurs, il va falloir procéder à un rééquipement global : une antenne 4G ne peut pas gérer la 5G, mais une antenne 5G peut éventuellement gérer la 4G. Des appels d'offres seront donc, de toute façon, lancés sur les équipements, qu'il s'agisse des antennes, des cœurs de réseau ou des stations de base. L'important pour les équipementiers est, bien entendu, de connaître le cadre avant de commencer à jouer. L'objectif idéal, à terme – mais il n'est encore évoqué que par une minorité, hélas ! –, est de parvenir à une interopérabilité des équipements. Ce ne sont pas les opérateurs de télécommunications qui en décident, mais il faut faire collectivement pression pour y parvenir, car il y va de la protection de ses parts de marché par chaque entreprise. Cet élément a été évoqué, en février dernier, lors de la conférence télécoms de Barcelone.

Comment les opérateurs seront-ils informés des évolutions et quelle sera la responsabilité des équipementiers ? Premièrement – et je réponds ainsi à la question de celui d'entre vous qui souhaitait s'assurer que le Premier ministre sera bien éclairé au moment de prendre sa décision –, c'est l'ANSSI qui réalisera l'expertise des dossiers, sur la base des produits et des logiciels qui lui seront proposés, et non sur la base d'une déclaration. Deuxièmement, l'agence bénéficie toujours de l'application de l'article R. 226-3 du code pénal : les équipementiers ont déjà fait l'objet d'un agrément. Or, l'instruction réalisée en amont est utilisée ensuite pour l'autorisation prévue par cette proposition de loi. Troisièmement, l'ANSSI, les équipementiers et l'opérateur télécoms ont des habitudes de travail, ce qui garantit l'échange d'informations. Lorsque l'ANSSI n'a pas de réponse de la part de l'opérateur de télécommunications, elle se met en relation avec l'équipementier. En tout état de cause, les opérateurs ont l'habitude d'anticiper et de gérer, dans le cadre des appels d'offres, ce dialogue avec l'ANSSI.

Le travail de cette dernière va-t-il augmenter considérablement ? Un certain nombre d'éléments sont traités dans le cadre de l'article R. 226-3, dont le champ d'application inclut, je le rappelle, les cœurs de réseaux mobiles à compter de 2021. En tout état de cause, la capacité d'absorber les autorisations ne pose pas problème, dans la mesure où un gros travail de validation est d'ores et déjà réalisé. Les mises à jour mineures seront immédiatement autorisées ; quant aux mises à jour majeures, elles seront évidemment étudiées de près comme je l'ai rappelé. Il est très important pour le Gouvernement que le déploiement de la 5G ne soit pas freiné.

Monsieur Ruffin, s'agissant des zones blanches, l'objectif du *New Deal* numérique est, je le rappelle, de parvenir à une couverture de 99,5 % de la population en 2020. Il s'agit donc bien de ne pas avoir une France à deux vitesses en matière d'accès aux télécommunications mobiles. Par ailleurs, je me réjouis que vous souligniez l'importance du dispositif de contrôle des investissements étrangers, que nous avons renforcé – je suppose que cela ne vous a pas échappé – dans le cadre de la loi PACTE. Je rappelle, à ce propos, que le rapport de M. Raphaël Gauvain sur la protection des entreprises confrontées à des mesures d'extraterritorialité va dans votre sens. Je me réjouis également de vous voir soutenir implicitement les efforts que nous consentons pour mettre en œuvre une

politique européenne commune dans des domaines comme ceux de la batterie électrique et de la nanoélectronique, en encadrant et en accompagnant, grâce à l'aide d'argent public, le développement de nouvelles technologies stratégiques.

Trois équipementiers sont actuellement présents sur le marché européen : Nokia-Alcatel, Ericsson et Huawei – un quatrième, Samsung, envisage d'y entrer. Je rappelle que, à la suite de la reprise d'Alcatel, Nokia s'est engagé envers l'État à préserver 2 500 emplois dans la R&D. Cet engagement concerne, je tiens à le préciser, les laboratoires 5G situés en France. Quant aux autres emplois, nous en assurons un suivi rapproché afin d'être certains que les reclassements bénéficient du plus haut niveau d'exigence. Ces emplois concernent des fonctions support. Ils ne sont pas moins importants, socialement, qu'un emploi technologique mais, dans le domaine qui nous intéresse ici, à savoir la souveraineté technologique, nous sommes particulièrement attentifs à la partie R & D.

S'agissant de la « probité » de Huawei, la question qui se pose est de deux ordres : premièrement, il faut savoir si certains équipementiers pourraient être légalement contraints de communiquer des données à leur gouvernement – c'est un élément important à prendre en considération dans une décision, mais cela ne concerne pas que les acteurs chinois ; et deuxièmement et surtout, il faut anticiper les possibles failles techniques : cela concerne tous les équipementiers, mais la faille ne se situera pas nécessairement au niveau de l'équipementier ; elle peut être le fait d'un de ses sous-traitants, au niveau des lignes de codage, par exemple. L'enjeu de la souveraineté technologique concerne donc tous les équipementiers, tous les logiciels, toute la sous-traitance. Il s'agit de nous doter d'un dispositif robuste de contrôle pour préserver notre souveraineté technologique – notion qui nous est chère, Monsieur Gassilloud, car elle est au cœur de notre indépendance industrielle.

Enfin, les décisions ne se limitent pas à une autorisation ou à une interdiction ; elles sont plus nuancées. Nous pouvons ainsi demander, au cours de l'instruction, des restrictions d'application géographique, des restrictions d'application d'usage ou formuler des recommandations en vue d'améliorer les dispositifs. Cette proposition de loi a le mérite de nous permettre une approche qui est la plus pragmatique possible afin d'assurer un équilibre entre, d'une part, la qualité de nos réseaux technologiques et, d'autre part, la capacité à maîtriser les risques en matière de souveraineté et de fragilité technique.

M. Éric Straumann. On reproche souvent à l'Europe d'être trop réglementaire, trop tatillonne. Or, s'il est un domaine où elle pourrait exercer une plus grande influence, c'est bien celui de la sécurité des réseaux de télécommunications. En effet, si la réglementation espagnole ou belge est moins rigide que la réglementation française, ne nous exposons-nous pas à l'entrée d'un cheval de Troie ? Il faut donc être attentif à ce qui se fait chez nos voisins.

Par ailleurs, nous avons tous les yeux rivés sur l'opérateur chinois, qui nous inquiète. Mais qu'en est-il d'Ericsson, l'opérateur américain ? On sait que la

National Security Agency (NSA) a surveillé les chefs d'État européens, notamment la Chancelière allemande et le Président français. Je souhaiterais donc savoir si l'on s'intéresse également de près aux liens entre cette agence et Ericsson.

M. Guillaume Kasbarian. L'objet de cette proposition de loi est de sécuriser notre réseau 5G. Il s'agit d'un enjeu vital pour notre économie, de plus en plus connectée. Le bon fonctionnement technique et la sécurité des équipements 5G sont donc une nécessité stratégique. Je ne m'étendrai pas sur les poursuites pour espionnage visant certains acteurs de ce marché, ni sur leurs pratiques commerciales parfois déloyales car subventionnées par des États ; nous avons étudié cette question lors des travaux de la commission d'enquête sur les décisions de l'État en matière de politique industrielle, et ce n'est pas le sujet de ce jour. Je me limiterai à l'aspect purement technique de la question. Or, je rappelle que, par le passé, les composants de certains équipementiers ont été affectés par de graves problèmes, dont les consommateurs ont souffert. C'est notamment pour contrôler ces garanties techniques et sécuritaires que nous renforçons la loi – la confiance et les bons sentiments ne suffisent pas toujours.

Les opérateurs télécoms remplissent leur rôle : développer un réseau de bonne qualité à moindre coût pour leurs clients et développer ainsi leur chiffre d'affaires et leur modèle économique. À ce propos, ils nous ont alertés, lorsque nous les avons reçus, il y a quelques semaines. Si vous limitez la concurrence, nous ont-ils dit, cela nous coûtera cher et nous n'aurons pas les meilleures offres techniques sur le marché. Et si vous nous imposez des contraintes, nous ne pourrons pas remplir les objectifs fixés en matière de déploiement d'antennes sur le réseau mobile.

Notre rôle de législateur n'est pas de freiner le développement des opérateurs télécoms, bien au contraire. Mais il est avant tout d'assurer la sécurité et la souveraineté des Français, grâce à un État fort, régulateur, qui sait imposer des normes et des contrôles pour garantir l'intégrité de la Nation et éviter l'ingérence d'États extérieurs. La proposition de loi que nous examinons nous permet de nous doter d'outils puissants. Il faudra ensuite que l'exécutif ait la volonté et le courage de les utiliser effectivement ; je ne doute pas qu'il les ait, malgré les fortes pressions économiques que j'ai mentionnées.

Pour conclure, je ferai appel au bon sens paysan. Lorsqu'un arbre fruitier est malade, vous avez généralement deux options : ou bien vous ne touchez à rien, en espérant que le reste de l'arbre ne sera pas contaminé et qu'il donnera quelques fruits à la fin de la saison ; ou bien vous assumez vos responsabilités en coupant immédiatement les branches malades, même si cela prend du temps, cela coûte un peu cher et cela amoindrit la récolte, car, si vous ne le faites pas dans l'urgence, c'est l'arbre tout entier, voire l'ensemble de l'exploitation, qui risque de mourir. Je suis certain que tous les acteurs, les opérateurs télécoms et l'État en tête, auront le courage de choisir la seconde option quand la sécurité des Français et la souveraineté nationale seront en jeu.

M. Dino Cinieri. Quels que soient les réseaux, il y transite de plus en plus de données souvent très sensibles, qu'il s'agisse de données personnelles, privées, ou d'informations d'importance vitale pour la sécurité de notre pays, de nos concitoyens et de nos entreprises. Des garanties de confidentialité, de non-divulgation à des tiers, à d'autres pays ou à des entreprises concurrentes sont à l'évidence indispensables. Madame la secrétaire d'État, quelle garantie absolue de sécurité êtes-vous en mesure de proposer ?

M. Éric Bothorel, rapporteur. Nous traitons ici des réseaux, donc des tuyaux qui véhiculent l'information. Pour protéger celle-ci, la doctrine qui a cours chez nous et pour laquelle nous nous battons est le chiffrement de bout en bout. C'est un élément de solidité, de robustesse et de garantie de la protection des données. Se prémunir contre les vulnérabilités que les réseaux pourraient présenter et qui permettraient d'en prendre le contrôle afin d'accéder à l'information, c'est tout l'objet de cette proposition de loi.

Monsieur Straumann, je ne suis ni naïf, ni paranoïaque ; or il faut être tout à la fois un peu naïf et un peu paranoïaque. Ceux qui sont un peu trop naïfs doivent surtout devenir un peu plus paranoïaques car ils risquent de manquer de discernement face à ceux qui cherchent à leur nuire. Vous avez raison de rappeler qu'il n'y a pas qu'un seul pays qui se soit livré à la surveillance d'une chancelière, par exemple, « à l'insu de son plein gré » ; ce peut être également le fait de nos meilleurs amis. En la matière, il s'agit de savoir si l'acteur, quelle que soit sa nationalité, respecte les règles du jeu que l'on a fixées pour préserver notre souveraineté et garantir la sécurité des réseaux : ou bien vous respectez le cahier des charges, et vous avez droit à l'autorisation, ou bien vous ne le respectez pas, et vous n'y avez pas droit, c'est aussi simple que cela ! Peu importe la couleur, la nationalité ou le capital – même si, natif de Paimpol et vivant à proximité de Lannion, je n'ignore pas les efforts consentis, autour de ma circonscription, par des acteurs plutôt européens en faveur de la 5G.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Je n'ai rien à ajouter : tout a été dit. S'agissant de l'Union européenne, j'ai rappelé, tout à l'heure, le calendrier du travail commun que doivent réaliser l'ensemble des États, de manière à se prémunir contre tout cheval de Troie. Enfin, je le répète, l'ensemble des acteurs, quelle que soit leur nationalité, sont évidemment concernés.

M. Philippe Michel-Kleisbauer. Le propos de M. le rapporteur me rappelle cette réflexion de Michel Audiard : dans la vie, mieux vaut être un petit peu paranoïaque qu'un petit peu mort…

II. EXAMEN DES ARTICLES

Article 1er

(art. L. 34-11, L. 34-11-1, L. 34-11-2 et L. 34-11-3 [nouveaux] du code des postes et des communications électroniques)

Régime de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques

A. L'ÉTAT DU DROIT

Il n'existe aujourd'hui qu'un dispositif d'autorisation encadrant la mise sur le marché des équipements de réseaux radioélectriques. Ce dispositif est prévu par l'article 226-3 du code pénal. Néanmoins, **l'autorisation se réfère à un objectif de protection de la vie privée et du secret des correspondances électroniques**, ce qui constitue une base juridique relativement étroite au regard des impératifs de sécurité qui sont au fondement de la présente proposition de loi.

1. L'article 226-3 du code pénal

Le régime d'autorisation préalable proposé par le présent article s'inspire directement d'un dispositif similaire du code pénal, mis en place pour protéger le secret de la correspondance privée.

Plus précisément, l'article 226-3 du code pénal punit de cinq ans d'emprisonnement et de 300 000 euros d'amende la « fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques » qui n'ont pas fait l'objet d'une autorisation du Premier ministre, prévue par l'article R. 226-3 du même code. Le régime d'autorisation est, ainsi, communément appelé « **régime R. 226-3** ». Il s'agit, en pratique, d'une autorisation de mise sur le marché.

Les appareils ou dispositifs concernés sont ceux susceptibles de permettre l'atteinte au secret des correspondances privées (infraction définie à l'article 226-15 du même code) ou à la vie privée (article 226-1 dudit code) soit par détection de conversations à distance, soit par captation de données informatiques. Concrètement, ce sont tous les outils technologiques qui permettent d'écouter des personnes à leur insu, d'enregistrer des conversations téléphoniques, d'intercepter les données transmises sur les réseaux de communications électroniques (réseaux filaires comme le réseau cuivre ou le réseau en fibre optique ; réseaux hertziens) : SMS, courriels, données de connexion aux sites internet fréquentés, images visualisées sur l'écran, etc.

Un arrêté [(1)] établit la liste des appareils et dispositifs « espions » qui doivent ainsi être préalablement autorisés. Les évolutions technologiques récentes

(1) Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal

ont cependant **contraint le législateur à élargir le champ des produits concernés**, notamment pour y intégrer des équipements de réseau plus conventionnels.

L'utilisation des IMSI catcher en matière de renseignement

L'article 226-3 du code pénal a fait l'objet de plusieurs modifications de périmètre ces dernières années, pour tenir compte des évolutions technologiques les plus récentes. À titre d'exemple, M. Michel Mercier, rapporteur sur le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (déposé le 3 février 2016), indiquait dans son rapport au nom de la commission des lois du Sénat :

« L'IMSI catcher peut être défini comme une antenne relais mobile factice qui se substitue, dans un périmètre donné, aux antennes relais des opérateurs permettant ainsi aux services spécialisés de renseignement de disposer d'informations sur les terminaux qui s'y sont connectés. L'utilisation de ces appareils par les services de renseignement a été particulièrement débattue lors de l'examen de ce projet de loi dans la mesure où ces dispositifs mobiles permettent de collecter massivement et de manière indifférenciée des données personnelles dans un large périmètre, qu'il s'agisse de données de connexion ou, pour certains de ces appareils, de correspondances ».

Source : Rapport n° 491 de M. Michel Mercier du 23 mars 2016 sur le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale

En effet, certains équipements déployés au niveau des cœurs de réseaux mobiles (3G et 4G) détiennent, aujourd'hui, des fonctions de duplication ou de routage du trafic de données qui sont transmises sur les réseaux de communications électroniques, ce qui permet de les détourner à des fins d'interception.

Afin de **mettre à jour la base juridique applicable**, l'article 23 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale a fait évoluer le champ des appareils ou dispositifs soumis à autorisation préalable : il s'agit non plus uniquement des produits « conçus pour réaliser » des interceptions ou des captations de données mais des produits « de nature à permettre la réalisation » de telles opérations.

Par conséquent, l'arrêté du 4 juillet 2012, susmentionné, a été modifié en août 2016 afin d'ajouter à la liste soumise à l'autorisation préalable « les appareils qui permettent aux opérateurs de communications électroniques de connecter les équipements de leurs clients au cœur de leur réseau radioélectrique mobile ouvert au public, dès lors que ces appareils disposent de fonctionnalités, pouvant être configurées et activées à distance, permettant de dupliquer les correspondances des clients, à l'exclusion des appareils installés chez ceux-ci ». En somme, il s'agit de tous **les équipements « radio » actifs qui composent un réseau mobile**.

Cette modification significative de périmètre entre en vigueur le 1er octobre 2021.

2. Les modalités de délivrance de l'autorisation

L'autorisation mentionnée par l'article 226-3 du code pénal est délivrée par le Premier ministre après avis d'une commission consultative, présidée par le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et composée de représentants de différentes administrations, d'un représentant de la Commission nationale de contrôle des interceptions de sécurité et de deux personnalités qualifiées désignées par le Premier ministre.

L'ANSSI est donc l'agence qui est chargée de l'instruction des dossiers de demande d'autorisation, même si l'autorisation est elle-même signée par le Premier ministre. Il est vraisemblable que l'agence soit également l'interlocuteur principal des opérateurs de communications électroniques qui sont concernés par la présente proposition de loi.

3. Les opérateurs d'importance vitale (OIV)

Définis à l'article L. 1332-1 du code de la défense, les OIV sont des « opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ».

Plus précisément, un OIV « gère ou utilise (…) un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population » (article R. 1332-2 du même code). Il apparaît donc clairement **que les acteurs majeurs des secteurs de l'énergie ou de l'eau, des télécommunications, des transports et des activités de défense** font partie de ces OIV, dont le nombre, confidentiel, est vraisemblablement compris entre 250 et 350 opérateurs, publics ou privés.

La protection des systèmes d'information des OIV a fait l'objet de plusieurs renforcements législatifs, en particulier depuis la publication de loi de programmation militaire n°2013-1168 du 18 décembre 2013, précitée. Le cadre juridique comprend ainsi :

– des obligations en matière de **sécurité de leurs systèmes informatiques**, notamment l'installation de dispositifs de détection des événements susceptibles d'affecter cette sécurité ;

– une obligation de déclaration au Premier ministre de tout incident majeur qui affecterait le fonctionnement ou la sécurité de ces systèmes ;

– une obligation de soumission de leurs systèmes d'information à un **processus de contrôle et d'audit**, à la demande du Premier ministre.

Les contrôles sont le plus souvent réalisés par l'ANSSI, qui dispose alors de moyens d'intervention accrus. En particulier, l'article L. 2321-3 du code de la défense dispose que la sécurité des systèmes d'information des OIV justifie que « les agents de l'Autorité nationale de sécurité des systèmes d'information (…) peuvent obtenir des opérateurs de communications électroniques (…) l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système ».

Les OIV et l'ANSSI entretiennent donc des relations de sécurité particulièrement approfondies : le dispositif de la présente proposition de loi complète ce cadre juridique protecteur.

4. La recommandation de la Commission européenne du 26 mars 2019

Quelques jours après le dépôt de la présente proposition de loi, **la Commission européenne a pris officiellement position** [(1)] sur les risques de sécurité relatifs au déploiement de la 5G sur le territoire de l'Union européenne (UE), « question d'importance stratégique pour l'Union » [(2)].

Cette recommandation se traduit par des mesures opérationnelles au niveau national et au niveau de l'UE. La lecture de cette recommandation montre que **la présente proposition de loi s'inscrit pleinement dans la continuité de la position de la Commission européenne**.

Au niveau national, la Commission recommande que chaque État membre **évalue les risques** liés aux infrastructures des réseaux 5G avant juin 2019, puis mette à jour les exigences de sécurité existantes pour les fournisseurs de réseaux ainsi que les conditions d'octroi des droits d'utilisation des fréquences dans les bandes qui seront ouvertes pour la 5G. **C'est ce que fait – avec un temps d'avance – la présente proposition de loi**, qui crée un régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques sensibles.

Au niveau de l'UE, la Commission et **l'agence de l'Union européenne pour la cybersécurité (ENISA) mèneront une évaluation coordonnée des risques** avant octobre 2019. Les États membres pourront s'appuyer sur les conclusions de l'évaluation pour mettre en œuvre un ensemble coordonné de mesures d'atténuation des risques (par exemple, des exigences de certification, des

---

(1) Commission recommendation of 26.3.2010, "Cybersecurity of 5G networks", 2335 final : https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks.

(2) Considérant n° 3. Les citations sont traduites pour les besoins du présent rapport.

tests, des contrôles ou le recensement des produits ou des fournisseurs jugés potentiellement non sûrs).

La Commission européenne souligne également que les mesures prises par les États membres pour assurer la sécurité des points sensibles des réseaux « devront inclure des obligations renforcées pour les fournisseurs et les opérateurs » (1). Les autorités compétentes à l'échelle nationale pourront demander la communication de toute information leur paraissant nécessaire avant toute modification des réseaux de communications électroniques par un acteur du secteur. Elles pourront également contraindre, pour des raisons de sécurité et d'intégrité des réseaux, les fournisseurs et les opérateurs à utiliser des équipements et des systèmes de traitement de l'information préalablement testés.

La Commission a également précisé qu'au-delà des facteurs techniques le comportement des fournisseurs, et notamment **l'influence qu'un « pays tiers » pourrait exercer sur eux**, devrait être pris en compte dans l'évaluation des risques pesant sur les réseaux 5G. En conséquence, la Commission a affirmé clairement le droit, pour les États membres de l'Union européenne, « d'exclure des prestataires ou des fournisseurs de leurs marchés pour des raisons de sécurité nationale » (2), ce que permet de faire – en ultime recours – la présente proposition de loi.

B. LE DISPOSITIF PROPOSÉ

L'article 1er crée une nouvelle section au sein du chapitre II du titre Ier du livre II du code des postes et des communications électroniques, intitulée « Régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques ». Le présent article s'inscrit **dans la continuité de l'autorisation dite « R. 226-3 »** et ne s'y substitue aucunement. Outre une date d'entrée en vigueur plus proche que celle prévue pour l'autorisation « R. 226-3 », rendue nécessaire par l'évolution du contexte des déploiements de réseaux, l'article 1er devrait également permettre d'asseoir l'intervention du Premier ministre sur une base juridique moins étroite que le seul respect du secret des correspondances et de la vie privée.

L'objet des quatre articles de cette nouvelle section du code des postes et des communications électroniques sera donc de définir ce nouveau régime d'autorisation préalable.

Le nouvel article L. 34-11 (**alinéa 4**) soumet à **une autorisation du Premier ministre** l'exploitation, sur le territoire national, « d'appareils, à savoir tous dispositifs matériels ou logiciels » qui permettent la **connexion au réseau radioélectrique mobile** (le réseau sur lequel transitent les communications électroniques des téléphones portables) dès lors que :

---

(1) Recommandation n° 5.

(2) Considérant n° 10.

(1) leurs fonctions présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation dudit réseau ;

(2) l'exploitation est effectuée par certains opérateurs de télécommunications (voir ci-dessous) ou par l'intermédiaire de leurs fournisseurs ;

(3) ces appareils ne sont pas installés chez les clients (les utilisateurs finaux).

Le même alinéa précise que **cette autorisation est « destinée à préserver les intérêts de la défense et de la sécurité nationale »**.

Les opérateurs visés par cette autorisation sont uniquement ceux mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense, c'est-à-dire les **opérateurs d'importance vitale** (OIV) dans le secteur des télécoms, dont la liste est confidentielle mais qui comprend les quatre principaux opérateurs télécoms nationaux.

Le II de cet article (**alinéa 6**) dispose que l'autorisation du Premier ministre est **octroyée pour « un ou plusieurs modèles » et « une ou plusieurs versions » des appareils concernés**. Il s'agit ici d'éviter que toute mise à jour logicielle ou que toute modification technique d'un équipement déjà contrôlé fasse l'objet d'un nouveau dossier de demande d'autorisation, avec les coûts et les délais de traitement qui en découlent nécessairement et qui seraient autant de contraintes à la liberté de déploiement des réseaux de communications électroniques.

L'autorisation est octroyée pour un périmètre géographique précis (en fonction des plaques de réseaux des opérateurs) et pour une durée d'au plus 8 ans. Cela signifie que, si les services qui instruiront la demande d'autorisation l'estiment nécessaire, l'autorisation ne pourrait être délivrée que pour quelques mois. L'opérateur sera à l'initiative de la demande d'autorisation ; c'est son dossier qui fixera le périmètre géographique concerné ainsi que les versions et modèles des équipements visés par l'autorisation préalable.

L'article L. 34-11-1 (**alinéa 7**) fixe les conditions de renouvellement de l'autorisation. La demande de renouvellement doit intervenir au moins deux mois avant l'expiration de l'autorisation. La composition du dossier d'autorisation ou de renouvellement est fixée par décret simple.

L'article L. 34-11-2 (**alinéa 8**) encadre les conditions de refus d'autorisation. Le Premier ministre motive son refus, qui peut intervenir s'il « existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale », caractérisé par le **manque de garantie de respect des règles suivantes** (fixées par l'article L. 33-1 du même code) :

« – les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service qui incluent des obligations de notification à l'autorité compétente des atteintes à la sécurité ou à l'intégrité des réseaux et services ;

« – les conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications ;

« – les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'Autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense » (les OIV susmentionnés).

L'**alinéa 10** indique que « le Premier ministre peut prendre en considération », dans son appréciation :

– les modalités de déploiement et d'exploitation mises en place par l'opérateur, ce qui permet d'inclure dans la prise en considération des facteurs autres que ceux strictement techniques (personnel employé, zones géographiques considérées, etc.) ;

– le fait que l'opérateur ou ses prestataires soient sous le contrôle ou soumis à l'ingérence d'un État non membre de l'Union européenne.

L'article L. 34-11-3 (**alinéa 11**) crée un **pouvoir d'injonction du Premier ministre** si l'exploitation d'un appareil soumis au régime d'autorisation préalable est effectuée sans cette autorisation. L'injonction peut porter sur le dépôt d'un dossier de demande d'autorisation ou de renouvellement d'autorisation ou, plus directement, sur le rétablissement de la situation antérieure à l'exploitation, dans des délais fixés par l'injonction. L'absence de mise en conformité avec l'injonction est punie par la même peine que l'exploitation sans autorisation (voir le commentaire de l'article 2).

L'**alinéa 12** précise les conditions d'une **procédure contradictoire** préalable à la prise d'effet de l'injonction : mise en demeure et présentation d'observations dans les quinze jours. Cette procédure contradictoire n'est pas appliquée « en cas d'urgence, de circonstances exceptionnelles ou d'atteinte imminente à la sécurité nationale ».

Enfin l'**alinéa 13** dispose que tous les engagements, conventions ou clauses contractuelles qui prévoient l'exploitation d'appareils sans autorisation préalable sont nuls lorsque cette autorisation est requise ou lorsque la mise en conformité exigée n'a pas eu lieu dans les délais.

C. LA POSITION DE LA COMMISSION

Votre rapporteur rappelle que les opérateurs de communications électroniques principalement concernés par les dispositions de cet article (Orange, Bouygues Telecom, SFR-Altice, Free-Iliad) sont eux-mêmes contraints de s'équiper en appareils de réseau sur **un marché très oligopolistique** : Nokia, Ericsson et Huawei sont leurs principaux équipementiers, tandis que Samsung fait office de nouvel entrant, concentré toutefois sur les équipements 5G. Selon les stratégies d'équipement de chaque opérateur, ces industriels fournissent soit l'intégralité des éléments du réseau 2G-3G-4G, soit se partagent des zones géographiques définies par les opérateurs (par exemple, deux plaques de réseaux qui couvrent la partie nord et la partie sud du territoire métropolitain), soit sont sollicités pour des composantes différentes du réseau – les équipements « cœur de réseau » pouvant par exemple être distingués des équipements présents sur les extrémités du réseau.

En outre, votre rapporteur a entendu les réserves liées à **« l'effet de sentier » industriel** qui implique que, lorsqu'un opérateur a choisi un fournisseur pour équiper ses stations de base en 3G, puis en 4G, il est difficile en pratique de se tourner vers un concurrent pour fournir la couche supérieure d'équipement qui autorisera la connectivité 5G. Les équipementiers n'ont pas développé de solutions standardisées ou de solutions techniques permettant une interopérabilité de leurs produits. Par voie de conséquence, le refus d'autorisation d'un équipement, voire (par ricochet) d'un équipementier, se traduirait vraisemblablement par de **lourdes opérations techniques de démontage** d'appareils plus anciens, non remis en cause mais non compatibles avec le recours à un autre équipementier. Cet échange complet de technologies (ce que les professionnels nomment le *swap*) provoque un coût financier et humain et se ferait nécessairement **au détriment de la cadence de déploiement des nouveaux réseaux**. Dès lors, le refus ou le retrait d'une autorisation devrait, en pratique, rester exceptionnel et n'intervenir qu'une fois que les autres moyens d'action dans la main des services de l'État, et notamment de l'ANSSI [(1)], se soient révélés inefficaces ou insuffisants.

Votre rapporteur a, enfin, pris en compte **la situation des réseaux mobiles ultramarins**. L'application en outre-mer des dispositions du présent article ne nécessite pas de dispositions expresses, sauf pour la Nouvelle-Calédonie, la Polynésie française et Wallis-et-Futuna. Toutefois, c'est l'Office des postes et des télécommunications (OPT) qui est en situation de quasi-monopole sur les deux premiers territoires avec son réseau Mobilis. Son statut d'établissement public industriel et commercial garantit que l'État conserve suffisamment la main sur la politique de déploiement de cet opérateur. En ce qui concerne Wallis-et-Futuna, le réseau mobile, Manuia, est déployé sur les trois îles par le service des postes et des

(1) L'ANSSI dispose de moyens d'intervention efficaces dès lors que ses interlocuteurs, sur un tel sujet, sont des opérateurs d'importance vitale soumis à une réglementation spécifique protectrice des intérêts de la Nation et qui dépasse largement le cadre de la présente proposition de loi.

télécommunications (SPT), qui est un service déconcentré de l'État et du Territoire.

Votre commission a adopté cet article modifié par quatre amendements rédactionnels et trois amendements de précision juridique proposés par votre rapporteur. Deux amendements présentés par Mme Christine Hennion et les membres du groupe La République en Marche ont également été adoptés.

Le premier de ces amendements, sous-amendé par votre rapporteur au titre d'une précision juridique, prévoit explicitement que **l'Autorité de régulation des communications électroniques et des postes (ARCEP) sera consultée** préalablement à la publication initiale de la liste des dispositifs soumis au régime d'autorisation. Il institue par ailleurs un délai de deux mois après la promulgation de la loi pour la publication de ladite liste afin d'assurer visibilité et sécurité pour les opérateurs dans le cadre de leurs programmes d'achats pour le déploiement de la 5G.

Le deuxième amendement présenté par les mêmes auteurs prévoit que le décret définissant les modalités d'autorisation, la composition du dossier de demande d'autorisation et de demande de renouvellement soit pris, **après avis de l'ARCEP et de la Commission supérieure du numérique et des postes (CSNP)**. Le sous-amendement que votre rapporteur a souhaité lui adjoindre précise qu'afin de ne pas allonger les délais administratifs qui nuisent au bon déploiement des réseaux, l'ARCEP et la CSNP auront à se prononcer sur le décret susmentionné dans un délai d'un mois.

*

* *

La commission examine l'amendement CE9 de Mme Marie-Noëlle Battistel.

Mme Marie-Noëlle Battistel. Par cet amendement, nous proposons que l'autorisation du Premier ministre soit donnée après avis de l'ANSSI, dont les missions correspondent au cœur de cette proposition de loi. Madame la secrétaire d'État, vous nous avez donné des éléments de réponse, mais je souhaiterais que vous confirmiez que cet avis sera officiellement rendu. J'ai bien compris que des habitudes de travail existaient entre les différents acteurs et que leurs relations étaient très fluides, mais nous souhaitons que cela soit inscrit officiellement dans la loi.

M. Éric Bothorel, rapporteur. Je demande le retrait de cet amendement, dans la mesure où il est déjà satisfait en pratique.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Demande de retrait, également. De même que le ministre de l'économie et des finances prend ses décisions sur la base de l'instruction de ses services, le Premier ministre se reposera sur l'ANSSI, qui est

un service à compétence nationale placée sous son autorité, sans personnalité morale.

M. Dominique Potier. Nous sommes heureux d'apprendre que l'amendement est satisfait. Je pense que ma collègue va le retirer…

Mme Marie-Noëlle Battistel. Mais non ! *(Sourires.)*

M. Dominique Potier. Elle choisira bien sûr ce qu'elle fera !

Madame la secrétaire d'État, alors que nous sommes en train d'évoquer la sécurité et la souveraineté françaises et européennes, sachez que, depuis quelques semaines, les Lorrains sont très inquiets et se demandent si l'Europe pourra conserver sa souveraineté dans la production de ses canalisations d'eau potable et d'assainissement, dont la moitié est fabriquée par Saint-Gobain Pont-à-Mousson. Or une menace plane : la France et l'Europe risqueraient de perdre le contrôle sur cette production au profit de l'Asie. Si nous devons nous préoccuper de l'évolution des canaux du numérique, ne méprisons jamais l'économie primaire et veillons à préserver la souveraineté de notre appareil industriel traditionnel.

Mme Marie-Noëlle Battistel. Avant de retirer mon amendement, je tenais à préciser qu'un avis peut être rendu public, ce qui n'est pas forcément le cas d'une instruction des services. Mais si Mme la secrétaire d'État confirme que toutes les décisions seront précédées d'un avis de l'ANSSI, je pourrai retirer l'amendement.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. L'ANSSI n'ayant pas de personnalité morale, du point de vue juridique, elle ne peut pas donner d'avis en tant que tel au Premier ministre – elle lui est simplement rattachée.

L'amendement est ***retiré****.*

La commission ***adopte*** *successivement l'amendement rédactionnel CE11 et l'amendement de précision CE23 du rapporteur.*

Puis elle examine, en discussion commune, l'amendement CE21 du rapporteur, faisant l'objet d'un sous-amendement CE24 du rapporteur pour avis de la commission de la défense, ainsi que l'amendement CE20 du rapporteur pour avis de la commission de la défense.

M. Éric Bothorel, rapporteur. En plus des quatre opérateurs télécoms nationaux dont nous avons parlé ce matin, d'autres acteurs pourront accéder à la 5G pour déployer du réseau. L'amendement CE21 vise à soumettre au régime prévu par la proposition de loi tous les acteurs d'importance vitale qui utiliseraient les bandes de fréquence de la 5G à condition qu'ils ouvrent leurs réseaux au public.

M. Thomas Gassilloud, rapporteur pour avis de la commission de la défense. Le sous-amendement CE24 reprend le dispositif de l'amendement CE20, lui-même issu d'un amendement adopté à l'unanimité par la commission de la défense, afin de le rendre compatible avec l'amendement CE21 du rapporteur.

La commission de la défense a jugé utile et prudent d'étendre le dispositif présenté aux opérateurs dits « verticaux ». Jusqu'à présent, on pouvait estimer que les risques pesant sur les réseaux privés ne présentaient pas le même caractère systémique que ceux qui pèsent sur les opérateurs de télécommunications. Mais, compte tenu des vastes possibilités d'application et d'usage de cette technologie – internet des objets, véhicules autonomes, *smart cities*, etc. –, la 5G modifiera très certainement les équilibres actuels. Il est tout à fait possible que les opérateurs verticaux cherchent bientôt à offrir à leurs clients des services nouveaux reposant sur la 5G. En Allemagne, par exemple, des industriels extérieurs au secteur des télécommunications se portent candidats à l'attribution de bandes de fréquence 5G. Un spectre de 100 mégahertz leur a même été réservé, avons-nous appris lors de l'audition de l'Agence nationale des fréquences (ANFR).

En France, il est probable que ces fréquences intéressent des opérateurs tels que la SNCF, de grands aéroports, des sociétés d'autoroutes, des industriels de l'automobile ou encore EDF. Nous devons prendre en compte trois arguments. Premièrement, ces activités sont très sensibles aux aspects de sécurité, qu'il s'agisse d'aéroports ou d'alimentation électrique ; deuxièmement, ces opérateurs sont souvent en situation de monopole ou presque ; du coup, l'hétérogénéité du parc qui garantissait la résilience des opérateurs de télécommunications pourrait disparaître ; enfin, les réseaux des opérateurs verticaux pourraient être étendus rapidement à du service télécom – si la SNCF utilisait la 5G pour ses usages internes, il y aurait fort à parier qu'elle serait tentée de l'utiliser pour fournir un service télécom. Pour éviter des blocages techniques ou de grands coups de bascule, autant proposer d'emblée des règles applicables à tout le monde. Nous pensons qu'avec la 5G la frontière entre réseaux télécoms et réseaux privés est appelée à s'estomper ; par conséquent, le risque systémique s'étendra probablement au-delà des réseaux des quatre grands opérateurs actuels de téléphonie mobile.

Pour sécuriser de telles opérations, la seule possibilité consisterait à requalifier ces opérateurs verticaux en opérateurs de réseaux ouverts au public, même si cette voie présente trois inconvénients : elle n'interviendrait qu'*a posteriori*, après l'ouverture du réseau ; les décrets et arrêtés relatifs aux OIV étant classifiés, le contrôle parlementaire s'en trouverait réduit ; enfin, elle priverait les opérateurs verticaux de la visibilité dont ils ont tant besoin pour optimiser leurs investissements.

Pour toutes ces raisons, intégrer d'emblée les OIV verticaux dans le dispositif leur offre à notre sens davantage de sécurité juridique ainsi que de la visibilité aux entreprises et de la clarté aux parlementaires.

L'amendement CE20 est ***retiré****.*

M. Éric Bothorel, rapporteur. Même si je comprends totalement votre préoccupation, à la veille d'une libération des fréquences et dans le souci de rendre l'innovation attractive, il me semble raisonnable de ne soumettre au régime de la proposition de loi les acteurs non encore opérateurs de télécommunications qu'une fois leurs réseaux ouverts au public. Votre dispositif serait dissuasif, même si nous partageons votre préoccupation : au sein de la commission des affaires économiques, nous débattons souvent du développement des régimes expérimentaux, des « bacs à sable » (*sandboxes*), pour soutenir l'innovation. Votre cadre est, au contraire, trop contraignant. La définition proposée dans mon amendement – « exploitant d'un réseau de communications électroniques ouvert au public » – permet de couvrir un champ suffisamment large pour nous assurer que nous pourrons intégrer les acteurs auxquels vous pensez et dont nous ne connaissons pas exactement le nombre dans le régime de la proposition de loi. Je crains que votre sous-amendement n'ait un effet de dissuasion, pour utiliser un langage militaire… Retrait, sinon avis défavorable.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Avis favorable sur l'amendement CE21. Pour ce qui est du sous-amendement CE24, je suggère également de le retirer. Il me semble que le dispositif est satisfait. De deux choses l'une : ou bien vous êtes un opérateur d'importance vitale non télécom, et le fait de vous soumettre à la loi pour des réseaux secondaires n'a pas de sens ; ou bien vous êtes un des opérateurs verticaux qui se voient attribuer la 5G – possibilité qui n'a été retenue pour l'instant que par l'Allemagne – et vous devenez un opérateur de réseau télécoms, auquel cas, votre appellation d'OIV doit évoluer : vous devenez OIV non seulement au titre de l'infrastructure que vous gérez, mais aussi du service télécom, ce qui vous fait, par conséquent, tomber dans le champ de la loi. Faute de quoi, vous risquez d'imposer à des OIV un contrôle sur une partie de leurs télécommunications, sans rapport avec l'objectif de la proposition de loi.

Mme Laure de La Raudière. Quelle incidence peut avoir le remplacement de l'appellation « clients » par « utilisateurs finaux » sur le champ d'application de la proposition de loi ?

Mme Christine Hennion. Je partage l'avis de Mme la secrétaire d'État. D'autres textes nous permettent de contrôler la sécurité des réseaux, notamment tous ceux qui sont dérivés de la directive NIS (*Network and Information Security*) à laquelle sont soumis la plupart des opérateurs verticaux.

M. Thomas Gassilloud, rapporteur pour avis de la commission de la défense. Le niveau d'exigence fixé aux opérateurs verticaux concernant la nature de leurs équipements doit être le même pour les services télécoms. J'ai bien noté la possibilité de requalifier ces opérateurs *a posteriori*, mais cela ne me semble pas de nature à offrir aux entreprises un cadre sécurisé sur le plan juridique ni de la visibilité. Quant au risque de freiner l'innovation, il ne me convainc pas :

l'innovation sera essentiellement soutenue par l'achat de bandes passantes par les quatre opérateurs de télécom. Le club de ceux qui candidateront à des fréquences 5G restera très fermé, le coût des licences étant estimé à plusieurs milliards d'euros. Par ailleurs, nous précisons bien que la disposition ne concernerait que les OIV, soit une centaine d'entreprises en France. Enfin, l'ANSSI nous avait laissé entendre que la charge de travail pour appliquer cette disposition serait tout à fait raisonnable. Je me dois, au nom de la commission de la défense, de maintenir ce sous-amendement.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. L'ANSSI pourrait absorber cette charge de travail. La vraie question concerne les opérateurs : les soumettre à un régime d'autorisation, alors qu'ils n'opèrent pas un réseau télécom stratégique ouvert au public, leur ferait supporter une charge qu'ils ne sauraient pas gérer, ce qui risquerait de les bloquer, même pour des applications d'exploitation assez basiques. Cela ne veut pas dire qu'un opérateur vertical qui deviendrait un opérateur 5G ouvert au public dans une application sensible ne basculerait pas dans ce régime – sa qualification d'OIV serait ajustée en conséquence.

Enfin, Madame de La Raudière, la notion d'« utilisateurs finaux » est un peu plus large que celle de « clients », ce qui permet de couvrir le champ des utilisateurs non payants, autrement dit tout le monde. C'est donc une amélioration rédactionnelle.

*La commission **rejette** le sous-amendement CE24.*

*Puis elle **adopte** l'amendement CE21.*

Elle passe ensuite à l'examen de l'amendement CE1 de M. François Ruffin.

Mme Bénédicte Taurine. Cet amendement vise à étendre le principe d'autorisation du Premier ministre au choix d'un prestataire de logiciels dans un appel d'offres public. De fait, l'utilisation de logiciels étrangers peut poser des problèmes en matière de sécurité nationale. L'entreprise Palantir, par exemple, a remporté, en mai 2016, un appel d'offres de 10 millions d'euros auprès du renseignement intérieur français et travaille aussi pour Airbus. Or cette entreprise, basée en Californie, travaille pour les services de renseignement américains.

M. Éric Bothorel, rapporteur. Si votre amendement répond au souci légitime de protéger les intérêts de la Nation contre l'exploitation malveillante de logiciels, il vise un champ beaucoup trop large, en englobant tous les logiciels et tous les marchés publics. Je ne suis pas certain qu'il soit pertinent que le Premier ministre donne son autorisation à chaque fois qu'une collectivité locale souhaite s'équiper d'un logiciel de gestion en ressources humaines. Quant aux marchés publics, la plupart d'entre eux sont encadrés par le droit de l'Union européenne, qui a pour principe cardinal la libre concurrence. D'où mon avis défavorable.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Lorsqu'il s'agit de contrôler l'attribution d'un logiciel, qui pourrait toucher à la souveraineté nationale, les personnes en charge des marchés publics au sein de l'État sont responsables de la définition des critères de sécurité à satisfaire et sont assistées, le cas échéant, par les services compétents en matière de sécurité nationale. Votre amendement est donc d'ores et déjà satisfait. Faisons confiance aux services de renseignement français pour avoir pris leur décision en toute connaissance de cause.

Mme Bénédicte Taurine. Je maintiens mon amendement : l'exemple que j'ai cité montre qu'il y a quand même un problème.

*La commission **rejette** l'amendement.*

Elle examine, en discussion commune, l'amendement CE8 de Mme Christine Hennion, faisant l'objet d'un sous-amendement CE18 du rapporteur, ainsi que l'amendement CE10 de M. Jérôme Nury.

Mme Christine Hennion. L'amendement CE8 vise à ce que l'Autorité de régulation des communications électroniques et des postes (ARCEP) et la Commission supérieure du numérique et des postes (CSNP) émettent un avis sur le décret et l'arrêté relatifs à cette loi, le plus rapidement possible. Cela permettra d'opérer un contrôle parlementaire, dans la mesure où la CSNP est une commission transpartisane composée de sénateurs et de députés.

M. Éric Bothorel, rapporteur. Le sous-amendement CE18 vise à préciser que la mise à jour des mesures réglementaires peut être effectuée à tout moment par le Premier ministre, sans que la loi n'ait à l'expliciter.

M. Jérôme Nury. L'amendement CE10 vise à ne pas remettre en cause le principe de l'autorisation préalable, mais à mieux l'encadrer par la consultation de l'ARCEP et de la CSNP. Il m'avait semblé que l'amendement CE8 de Mme Hennion ne mentionnait pas l'avis de la CSNP. Qu'en est-il ?

Mme Christine Hennion. Vous avez raison : en fait, j'ai défendu les amendements CE8 et CE7 en même temps. L'amendement CE8 vise à soumettre la liste des dispositifs à l'avis de l'ARCEP seule, les parlementaires ne disposant pas de suffisamment de connaissances techniques pour la juger finement ; le CE7 vise à prévoir que le décret définissant les modalités d'autorisation, la composition du dossier de demande d'autorisation et de demande de renouvellement soit pris après consultation de l'ARCEP et de la CSNP.

M. Jérôme Nury. Je vous remercie, Madame Hennion, pour ces précisions. Il me semblerait intéressant de concilier les deux niveaux pour le décret : technique avec l'ARCEP et transpartisan avec la CSNP, afin de permettre au Parlement de contrôler l'action du Gouvernement.

Mme Christine Hennion. C'est l'objet de mon amendement CE7, qui arrive un peu plus loin.

M. Éric Bothorel, rapporteur. Avis favorable à l'amendement CE8 sous-amendé. Quant à l'amendement CE10, il sera satisfait par l'amendement CE7.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Avis favorable à l'amendement CE8 sous-amendé.

La commission ***adopte*** *le sous-amendement.*

Puis elle ***adopte*** *l'amendement CE8* ***sous-amendé****.*

En conséquence, l'amendement CE10 ***tombe****.*

La commission examine l'amendement CE12 du rapporteur.

M. Éric Bothorel, rapporteur. Cet amendement simplifie la rédaction proposée pour les modalités d'autorisation des appareils sensibles exploités par les opérateurs : la création d'un nouvel article L. 34-11-1 est supprimée au bénéfice d'un II consolidé ; il est superflu de préciser que l'autorisation peut être refusée dès lors que l'article L. 34-11-2 s'applique ; la procédure d'autorisation est décrite de façon plus précise, à droit constant ; enfin, le dossier de demande de renouvellement est remis au regard de l'autorisation en vigueur, et non initiale, en cas de double renouvellement.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Avis favorable.

La commission ***adopte*** *l'amendement.*

Elle est ensuite saisie de l'amendement CE7 de Mme Christine Hennion, qui fait l'objet d'un sous-amendement CE25 du rapporteur.

Mme Christine Hennion. C'est l'amendement dont je parlais à l'instant : il prévoit que le décret définissant les modalités d'autorisation, la composition du dossier de demande d'autorisation et de demande de renouvellement soit pris, après avis de l'Autorité de régulation des communications électroniques et des postes et de la Commission supérieure du numérique et des postes.

M. Éric Bothorel, rapporteur. Le sous-amendement CE25 vise à préciser que l'ARCEP et la CSNP se prononceront dans un délai d'un mois après leur saisine.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Avis favorable à l'amendement CE7 sous-amendé. Il sera toujours possible, bien entendu, de commencer à travailler en temps masqué, autrement dit sans attendre la présentation formelle du décret.

*La commission **adopte** le sous-amendement.*

*Puis elle **adopte** l'amendement CE7 **sous-amendé**.*

*Elle **adopte** l'amendement de précision CE13 du rapporteur.*

Elle examine ensuite l'amendement CE22 du rapporteur.

M. Éric Bothorel, rapporteur. Dans un but de simplification, par parallélisme avec le droit proposé, le manque de garantie de respect des règles qui motivent le refus d'autorisation porte également sur les règles applicables à l'intégrité, à la sécurité et à la continuité de la fourniture de services.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Avis favorable.

*La commission **adopte** l'amendement.*

*Elle **adopte** l'amendement rédactionnel CE19 du rapporteur.*

*Puis elle **adopte** l'article 1er **modifié**.*

Article 2

(art. L. 39-1-1 [nouveau], L. 39-6 et L. 39-10 du code des postes et des communications électroniques)

Sanctions pénales en cas d'infraction au régime d'autorisation préalable

A. L'ÉTAT DU DROIT

Deux catégories de sanctions sont prévues par le code des postes et des communications électroniques.

Des **sanctions administratives** – notamment d'ordre pécuniaire – peuvent être prises par l'Autorité de régulation des communications électroniques et des postes (ARCEP) aux termes de l'article L. 36-11 du code des postes et des communications électroniques. Il s'agit du pouvoir de sanction de l'ARCEP agissant en qualité de régulateur du secteur des télécommunications. Ces sanctions peuvent porter sur des sujets aussi divers que les atteintes à la concurrence dans le secteur, sur le manque de neutralité des réseaux, sur l'irrespect de missions de service public (pour l'opérateur en charge du service public universel) ou de clauses contractuelles de déploiement des réseaux.

Des **sanctions pénales** sont également prévues par ce même code. En matière de régulation des réseaux radioélectriques publics, l'article L. 39 de ce même code punit, par exemple, d'**un an d'emprisonnement et de 75 000 euros d'amende** le fait d'établir ou de faire établir un réseau ouvert au public sans que la déclaration prévue à l'article L. 33-1 de ce même code ait été faite ; l'article

L. 39-1 réprime le fait d'utiliser des fréquences ou de brouiller des communications sans autorisation.

B. LE DISPOSITIF PROPOSÉ

L'article 2 modifie le chapitre V du titre I[er] du livre II du code des postes et des communications électroniques en déterminant un **régime de sanction pénale en cas d'infraction aux dispositions du nouveau régime de contrôle**.

Le nouvel article L. 39-1-1 (**alinéa 2**) du code des postes et des communications électroniques **crée deux infractions** mentionnées respectivement aux **alinéas 4 et 5** :

– **l'exploitation sans autorisation préalable** des appareils visés par le nouvel article L. 34-11 de ce même code ;

– **la non-exécution – totale ou partielle – des injonctions** prises sur le fondement du I du nouvel article L. 34-11-3 de ce même code (voir le commentaire de l'article 1[er]).

Il prévoit **une peine d'un an d'emprisonnement et de 150 000 euros d'amende** pour toute personne physique déclarée responsable d'une de ces infractions.

L'article L. 39-6 du code des postes et des communications électroniques prévoit des sanctions pénales complémentaires en cas de condamnation pour l'une des infractions prévues aux articles L. 39 et L. 39-1 de ce même code. **L'alinéa 6** précise que lesdites sanctions seront également applicables aux infractions prévues par le nouvel article L. 39-1-1.

Ainsi, en cas de condamnation pour l'une des infractions prévues à l'article susmentionné, le tribunal peut **prononcer la confiscation des matériels et installations** constituant le réseau ou permettant la fourniture du service. Il lui est également loisible d'ordonner **la destruction de ces matériels et installations** aux frais du condamné, et **l'interdiction d'établir un réseau radioélectrique mobile** pour une durée d'au plus trois ans.

En outre, les personnes morales déclarées responsables pénalement des infractions définies à l'article L. 39-1-1 encourent une amende dont le taux maximum est égal au **quintuple de celui prévu pour les personnes physiques**. L'article L. 39-10, complété par l'**alinéa 7**, précise qu'à l'instar des personnes physiques, des sanctions complémentaires sont applicables aux personnes morales condamnées pour l'une des infractions prévues au nouvel article L. 39-1-1. Elles encourent ainsi deux autres peines :

– **l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales**, peine mentionnée au 2° de l'article 131-39 du code

pénal. En l'espèce, l'activité professionnelle concernée est l'exploitation de réseaux mobiles radioélectriques publics.

– **l'affichage ou la diffusion de la décision prononcée** par la presse écrite ou par voie électronique, peines mentionnées au 9° de l'article 131-39 du code pénal.

C. LA POSITION DE LA COMMISSION

Votre commission a estimé que **le montant de la sanction était proportionné** et a donc conservé l'équilibre initial de la proposition de loi.

Votre rapporteur a proposé une mesure de précision juridique ainsi qu'une mesure de coordination juridique, qui ont toutes deux été adoptées.

*

* *

*La commission **adopte** successivement l'amendement de précision CE14 et l'amendement de coordination CE15 du rapporteur.*

*Elle **adopte** l'article 2 **modifié**.*

Article 3

Dispositions d'entrée en vigueur du régime d'autorisation préalable

A. LE DISPOSITIF PROPOSÉ

L'article 3 dispose que le régime d'autorisation préalable créé par l'article 1er de la présente proposition de loi est applicable à l'exploitation des appareils installés depuis le 1er février 2019 (**alinéa 1**).

L'application rétroactive de ce dispositif implique que les opérateurs concernés préparent des dossiers de demande d'autorisation dès l'entrée en vigueur de la loi, pour des équipements déjà mis en place. L'**alinéa 2** précise qu'ils disposent d'un délai de deux mois à compter de cette entrée en vigueur pour déposer leur demande.

B. LA POSITION DE LA COMMISSION

Votre rapporteur note que **l'application rétroactive** du dispositif d'autorisation, pour tous les équipements exploités à partir du 1er février 2019, **se justifie pleinement** par les objectifs de sécurité nationale et de protection de l'intégrité des réseaux qui animent la présente proposition de loi.

Il convient d'éviter l'effet pervers consistant, pour les opérateurs, à rechercher un déploiement accéléré – mais moins soigneux en matière de sécurité – de leurs réseaux afin de contourner les contraintes du dispositif d'autorisation. Le délai ménagé pour permettre de régulariser la situation des appareils déjà exploités à la date de publication de la présente loi est, en outre, équilibré et ne devrait pas faire peser une contrainte administrative démesurée sur les opérateurs visés.

Votre commission a donc adopté cet article avec deux amendements de précision juridique proposés respectivement par votre rapporteur et par le Gouvernement. Ce dernier amendement explicite que le délai de deux mois prévu par le présent article pour demander l'autorisation des appareils déjà installés court à partir du moment où tous les textes règlementaires d'application seront publiés.

*

* *

*La commission **adopte** l'amendement de précision CE16 du rapporteur.*

Puis elle examine l'amendement CE17 du rapporteur.

M. Éric Bothorel, rapporteur. Il s'agit d'un amendement de précision.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Je vous suggère de retirer votre amendement au profit de l'amendement CE26 du Gouvernement, qui vient juste après celui-ci et qui précise que le délai de deux mois prévu par l'article 3 pour demander l'autorisation des appareils déjà installés court à partir du moment où tous les textes réglementaires d'application seront publiés.

*L'amendement est **retiré**.*

La commission est saisie de l'amendement CE26 du Gouvernement.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. L'amendement vient d'être présenté.

M. Éric Bothorel, rapporteur. Et j'y suis très favorable, et même enthousiaste !

M. Jérôme Nury. Ne risque-t-on pas de perdre beaucoup de temps ? Alors que des opérateurs posent des pylônes 4G, depuis le 1er février, dans le cadre du « *New Deal* mobile », ils vont devoir attendre pendant des mois que le décret paraisse, pour savoir si leurs équipements sont valables ou non.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Justement non : le décret sera préparé en temps

masqué. Nous venons d'ajouter un délai d'un mois pour consulter l'ARCEP et la CSNP. Nous faisons tout pour favoriser une publication très rapide.

La commission ***adopte*** *l'amendement.*

Puis elle ***adopte*** *l'article 3* ***modifié****.*

Après l'article 3

La commission examine les amendements CE5, CE3, CE6 et CE4 de M. Philippe Michel-Kleisbauer.

M. Philippe Michel-Kleisbauer. Ces quatre amendements participent d'une doctrine constante du groupe MODEM : le renforcement du rôle et des missions du Parlement. Ils visent à permettre au Parlement d'être informé de l'action du Gouvernement en matière de contrôle préalable de l'exploitation des équipements de réseaux radioélectriques. Cette évaluation lui permettra d'adapter sur le long terme le dispositif et les moyens aux enjeux soulevés par la proposition de loi, de même que le Parlement doit être informé de l'action du Gouvernement en matière de contrôle préalable des investissements étrangers en France. Ce dispositif s'inscrit ainsi directement dans l'esprit de l'article 55 *bis* du projet de loi PACTE, dont la commission de la défense a été anormalement exclue. Le caractère sensible des données est pris en compte, puisque nous souhaitons qu'un rapport ne soit remis qu'à certains membres du Parlement, afin d'en garantir la confidentialité.

Dans l'amendement CE3, le rapport annuel serait remis aux présidents de la commission des affaires économiques et de la défense de chaque chambre. Dans l'amendement CE4, il serait remis à la délégation parlementaire au renseignement. Dans les amendements CE5 et CE6, c'est un rapport plus détaillé qui serait respectivement remis aux mêmes destinataires. L'intérêt serait d'associer au moins les présidents de commission au rapport, de sorte qu'ils aient une visibilité à long terme, pour faire évoluer la loi.

M. Éric Bothorel, rapporteur. Avis défavorable. Pour contrôler une telle action, la commission parlementaire compétente ou la délégation parlementaire au renseignement peuvent auditionner les ministres ; pour cette dernière, leurs membres sont habilités au secret défense, contrairement aux présidents des deux commissions que vous mentionnez. L'ANSSI peut également être auditionnée. Le projet de loi PACTE, que vous avez cité, visait à simplifier la vie des entreprises. Je vous invite à garder ce cap à l'esprit, afin de ne pas alourdir les dispositifs proposés, alors que nous avons déjà les moyens d'assurer un contrôle parlementaire efficace.

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. Avis défavorable à ces quatre amendements.

M. Guillaume Kasbarian. S'agissant du contrôle parlementaire, plusieurs outils permettent à l'Assemblée de l'effectuer : la délégation parlementaire au renseignement est habilitée au secret défense et a accès à des documents classifiés ; par ailleurs, avec la loi PACTE, nous avons introduit un nouveau mécanisme de contrôle, qui permet à deux présidents de commission et à deux rapporteurs généraux d'avoir accès à des documents et de mener des investigations relatives à la sécurité économique, dans son acception la plus large. Grâce à ces deux dispositifs solides, le Parlement peut déjà exercer un vrai contrôle sur l'action du Gouvernement.

M. Philippe Michel-Kleisbauer. Dans la mesure où la délégation parlementaire au renseignement est totalement étrangère à la commission de la défense et que ce texte porte sur les intérêts de sécurité nationale et de défense de notre Nation, je comprends mal que la commission de la défense ne puisse pas être impliquée au moins par un rapport remis à son président.

*La commission **rejette** successivement ces amendements.*

*Puis elle **adopte** l'ensemble de la proposition de loi **modifiée**.*

LISTE DES PERSONNES AUDITIONNÉES

- **Table ronde réunissant les opérateurs suivants :**

Iliad-Free

Mme Ombeline Bartin, responsable des relations institutionnelles

M. Pascal Mayeux, directeur des obligations légales

Altice-SFR *

Mme Marie-Georges Boulay, secrétaire générale adjointe

Bouygues Télécom *

M. Anthony Colombani, directeur des affaires publiques

Fédération Française des Télécoms *

M. Olivier Riffard, directeur des affaires publiques

- Auditions individuelles avec les acteurs suivants :

Orange *

M. Laurentino Lavezzi, directeur des affaires publiques

M. Franck Laurent, juriste sécurité – coordinateur sécurité globale du groupe

M. Pascal Nourry, expert sécurité à la direction technique « Réseaux et Services »

Cisco *

M. Bruno Bernard, directeur des affaires publiques

M. Jean-Charles Griviaud, chef de la sécurité

Samsung *

M. Yong Chang, vice-président, directeur de la division B2B·B2G, Samsung Electronics

M. Sang Pil Chun, directeur des relations institutionnelles, Samsung Electronics Europe

M. Daniel Borras, directeur de la stratégie, Samsung Networks Europe

M. Sangwoo Lee, directeur des affaires de la division B2B, Samsung Electronics France

Mme Florence Catel, directrice des relations publiques, Samsung Electronics France

Huawei *

M. Minggang Zhang, directeur général adjoint

M. Jean-Christophe Aubry, responsable des affaires publiques

Nokia *

M. Marc Charrière, directeur des relations institutionnelles

Agence nationale des fréquences (ANFR)

M. Gilles Brégant, directeur général

Autorité de régulation des communications électroniques et des postes (ARCEP)

Mme Cécile Dubarry, directrice générale

M. Olivier Delclos, chef de l'unité « Opérateurs et obligations »

Direction générale des entreprises (DGE)

Mme Sarah Finkelstein, conseillère attractivité et consommation de la secrétaire d'État Agnès Pannier-Runacher

M. Mathieu Weill, chef du service de l'économie numérique

M. Jean-Pierre Labé, chef du bureau de la réglementation des communications électroniques

Agence nationale de la sécurité des systèmes d'information (ANSSI)

M. Guillaume Poupard, directeur

** Ces représentants d'intérêts ont procédé à leur inscription sur le répertoire des représentants d'intérêts de la Haute Autorité pour la transparence de la vie publique (HATVP), qui vise à fournir une information aux citoyens sur les relations entre les représentants d'intérêts et les responsables publics lorsque sont prises des décisions publiques.*