N° 1830

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 2 avril 2019.

AVIS

FAIT

AU NOM DE LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES
SUR LA PROPOSITION DE LOI (n° 1722),

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**,

PAR M. THOMAS GASSILLOUD,

Député.

Voir les numéros :

Assemblée nationale : 1722, 1832.

.

SOMMAIRE

Pages

INTRODUCTION

La cinquième génération de standards de télécommunications mobiles, appelée la « 5G », promet d'être une véritable rupture technologique, ouvrant la voie à des applications et des usages variés et nouveaux dans nombre de champs, tels que les objets connectés, les véhicules autonomes, les « villes intelligentes » ou les processus industriels.

Revers de la médaille, la 5G reposera sur des équipements de plus en plus virtuels et des architectures de réseaux de plus en plus déconcentrées, ce qui accroîtra inexorablement la vulnérabilité de ces réseaux.

La résilience de ces derniers revêt donc un enjeu de défense et de sécurité nationale, à deux titres au moins. D'une part, la sécurité des réseaux de télécommunication est devenue d'une importance vitale pour le fonctionnement de notre société. D'autre part, les armées et les forces de sécurité intérieure utilisent de plus en plus les réseaux civils de télécommunication, et utiliseront donc la 5G. C'est à ce titre que la commission de la Défense nationale et des forces armées s'est saisie pour avis de la présente proposition de loi.

L'objet de celle-ci est d'établir rapidement un cadre juridique permettant à l'État de maîtriser, au moins a minima, les réseaux de télécommunications mobiles sur le territoire national, afin de s'assurer de leur résilience sans pour autant entraver leur déploiement. C'est dans cet esprit de recherche d'équilibre entre les impératifs de sécurité et de soutien au développement du numérique sur l'ensemble de notre territoire que la commission a conduit ses travaux.

I. L'AVÈNEMENT DE LA « 5G » REVÊT DES ENJEUX MAJEURS DE DÉFENSE NATIONALE

Contrairement à ce que son appellation pourrait laisser penser, la cinquième génération de standards techniques pour les réseaux de téléphonie mobile, dite la « 5G », promet de se traduire par bien davantage qu'un simple accroissement de débit par rapport à la génération précédente de ces standards – la « 4G ». En effet, les technologies de 5G permettront de développer des applications et des usages tout à fait nouveaux, en même temps qu'elles présenteront des vulnérabilités nouvelles. Le passage de la 4G à la 5G revêt donc un enjeu de sécurité et de défense nationale à un double titre : d'une part, la résilience de ces réseaux dans leur ensemble est d'intérêt vital pour la défense nationale et, d'autre part, les forces utiliseront ces réseaux pour leurs propres activités.

A. LA 5G PROMET AUTANT D'INNOVATIONS TECHNOLOGIQUES QUE DE VULNÉRABILITÉS NOUVELLES

1. Une évolution technologique significative, qui va au-delà d'un incrément de puissance des réseaux actuels

a. La virtualisation des réseaux permet un changement d'échelle pour leurs capacités

Votre rapporteur pour avis ne prétend pas présenter ici une explication technique poussée des spécificités de la 5G ; il est néanmoins utile à la compréhension des enjeux de la présente proposition de loi de noter que la 5G repose sur un changement complet de modèle technologique ayant deux aspects principaux :

– **la virtualisation des réseaux** de télécommunication. Jusqu'à présent, les fonctionnalités des équipements de réseau reposaient certes déjà sur 20 % à 30 % d'équipements physiques et sur 70 % à 80 % de logiciels, mais ceux-ci étaient disséminés dans les équipements. Avec la 5G, ces logiciels seront concentrés dans des *clouds* qui agrégeront les fonctions logicielles de réseaux, ce qui permettra de réorienter les ressources du réseau – c'est-à-dire leur débit – en fonction des besoins observés sur le territoire. Ainsi, par exemple, en cas d'événement public se traduisant par une grande concentration de population en un lieu habituellement peu dense, les technologies de 5G permettront de mieux adapter les capacités du réseau au pic de demande en ce lieu ;

– la 5G reposera aussi sur des **technologies nouvelles dites de *network slicing*** (expression que l'on pourrait proposer de traduire par « opération du réseau par tranche »). Ces technologies consistent à affecter, dans un réseau, les flux de transmissions à telle ou telle application en fonction de son caractère

prioritaire, sans que soit pour autant nécessaire de laisser le flux concerné inutilisé lorsque l'application n'en a pas besoin. Elles permettent ainsi de créer de multiples réseaux virtuels adossés à un seul et même ensemble d'équipements physiques de réseau.

Ces technologies permettront un véritable changement d'échelle dans les capacités des réseaux de télécommunication et ce, à trois égards :

– un **accroissement considérable des débits de données**, qui pourraient atteindre dès 2020 un gigabyte par seconde, et davantage encore ultérieurement ;

– une **réduction des temps de latence** dans les communications, ces temps pouvant être réduits à quelques millisecondes au lieu de quelques dizaines avec la 4G ;

– un **accroissement de la densité des flux**, qui pourront être concentrés de façon souple et dynamique en fonction des besoins.

Il est possible aussi que ces possibilités techniques nouvelles entraînent une réorganisation de l'écosystème industriel des télécommunications, avec par exemple le développement d'opérateurs virtuels de nouveaux genres.

b. La 5G ouvre la voie à des innovations technologiques majeures

Ce saut capacitaire ouvre la voie à de nouvelles applications et de nouveaux usages des technologies de télécommunication, notamment dans le champ industriel ; d'ailleurs, comme l'a fait observer M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI), les usages de la 5G sont certainement loin d'être tous imaginés à ce jour. Parmi les plus fréquemment évoquées, on citera à titre d'exemple les applications envisageables de tous types d'objets connectés en matière de domotique, de « ville intelligente », de moyens autonomes de transport terrestre ou d'industrie « 4.0 ».

C'est ce qui fait dire à la Commission européenne [(1)] que « *les réseaux de cinquième génération (5G) seront à l'avenir l'épine dorsale de nos sociétés et de nos économies, reliant des milliards d'objets et de systèmes, y compris dans des secteurs critiques comme l'énergie, les transports, les banques et la santé, ainsi que des systèmes de contrôle industriel qui véhiculent des informations sensibles et étayent des dispositifs de sécurité* ». Nombre de ces applications trouveront des usages dans l'équipement des forces armées.

c. Le déploiement de la 5G est imminent

Des expérimentations de technologies de 5G ont été lancées en France en 2018, l'attribution de bandes de fréquences spécifiques est prévue pour la fin de

(1) « La Commission européenne recommande une approche commune de l'UE concernant la sécurité des réseaux 5G », communiqué de presse en date du 26 mars 2019.

l'année 2019 et le déploiement d'équipements de 5G doit commencer dès 2020. Le passage à la 5G sera probablement graduel :

– dans un premier temps, il s'agit d'adapter aux technologies de réseaux virtuels les « cœurs de réseaux » de 4G, c'est-à-dire les « routeurs » qui assurent l'interconnexion de tous les terminaux raccordés aux réseaux d'antennes, afin que ces équipements de « 4G+ » soient d'emblée compatibles avec la 5G (« 5G *ready* ») ;

– dans un second temps, il s'agit de raccorder à la radio de 5G les cœurs de réseaux « 4G » ainsi virtualisés ;

– dans un troisième temps seulement, il s'agit de déployer des cœurs de réseaux de 5G, c'est-à-dire des *clouds* logiciels, permettant le plein développement des usages de la 5G.

d. La 5G n'est pas sans impact sur la structure même de l'industrie des télécommunications

Les représentants des opérateurs et des équipementiers entendus par le rapporteur pour avis prévoient des modifications substantielles du paysage des acteurs du secteur à la faveur de l'essor de la 5G.

Selon les représentants de CISCO, **on verra arriver sur le marché de la « 5G » des opérateurs qui ne sont pas spécialisés dans les réseaux mobiles**, mais par exemple dans les logiciels. D'après eux, les industriels les plus avancés en la matière sont les acteurs du secteur du *cloud computing* ; ils ont développé des outils permettant de mettre en œuvre des infrastructures de stockage massives, sur lesquelles les acteurs du secteur des réseaux mobiles devront s'appuyer pour créer les cœurs « 5G ». Ainsi, l'opérateur jouera de plus en plus un rôle d'*enabler*, mais les « délivreurs d'applications » seront des tiers. À cet égard, pour CISCO, le passage de techniques de virtualisation à des technologies de *cloud* représente un saut technologique encore plus important que le passage d'équipements physiques à des réseaux virtualisés.

Il est surtout à noter que, dans l'attribution des fréquences utiles à la 5G, les enchères pourraient intéresser d'autres acteurs que les seuls opérateurs de télécommunications. On qualifie habituellement de « **verticaux** » ces opérateurs qui, en appoint d'une activité principale autre que les télécommunications, développent pour leur propre compte un réseau de télécommunication. Des acteurs comme la SNCF, Aéroport de Paris ou le port du Havre pourraient très bien se porter eux aussi acquéreurs de licences d'utilisation de fréquences radio. D'ailleurs, l'Allemagne est allée jusqu'à réserver une part du spectre hertzien utile à la 5G aux opérateurs verticaux. **Avec la 5G et ses multiples applications au-delà de la seule téléphonie mobile, les opérateurs verticaux pourraient ainsi prendre une part croissante dans le marché des télécommunications**.

2. Des vulnérabilités nouvelles

a. Des vulnérabilités liées à l'architecture des réseaux 5G

C'est par son architecture même, davantage que par la nature des équipements, que la 5G présentera des vulnérabilités nouvelles.

L'évolution technologique bouleverse en effet les équilibres actuels par l'effet conjugué de trois principaux facteurs de surcroît de complexité :

– d'abord, les cœurs de réseaux sont en voie de virtualisation, vers des serveurs dans un premier temps, et vers des *clouds* dans un second. En conséquence, il sera très difficile de dire demain où une fonction est « implémentée », tant les bases physiques s'éloignent des terminaux des utilisateurs. Or, **avec le *cloud*, l'extension des liaisons entre les utilisateurs et les cœurs de réseaux – qui, eux-mêmes, deviennent plus « logiques » que « physiques » – accroît les risques d'interception et appelle un contrôle renforcé**. Très schématiquement, là où l'interception d'un flux d'information nécessite dans les réseaux de 4G un dispositif technique particulier, telle une « porte dérobée » (*backdoor*), il suffira de posséder les codes d'administrateur pour accéder aux logiciels et aux *clouds* des réseaux de 5G ;

– ensuite, à côté des acteurs traditionnels des télécommunications qui sont les équipementiers et les opérateurs, émerge une **nouvelle catégorie d'acteurs majeurs : les intégrateurs**, comme Cap Gemini ;

– enfin, le passage d'infrastructures matérielles à des infrastructures logicielles rend les opérations de **mise à jour plus faciles, donc plus fréquentes et, partant, le suivi des différentes versions d'un même équipement en devient plus complexe**. Certains équipementiers en viennent d'ailleurs à rompre avec la logique même des versions successives pour proposer à leurs clients d'acquérir un service mis à jour en permanence et non un équipement ou un logiciel particulier.

Les équipementiers entendus par le rapporteur pour avis indiquent qu'ils prévoient en effet une ou deux mises à jour logicielles majeures par an en rythme de croisière, sachant par ailleurs que le déploiement d'une technologie qui n'est pas encore mûre peut, par nature, appeler dans un premier temps des modifications opérées à un rythme plus soutenu, à mesure qu'apparaissent des problèmes.

b. Une dissémination des vulnérabilités dans les réseaux

L'une des caractéristiques de la 5G est que **la circulation des informations sera moins centralisée** qu'avec les générations précédentes de réseaux de télécommunication.

Très schématiquement, alors que les antennes-relais ne servent aujourd'hui qu'à relayer de façon assez « passive » les flux de données entre les terminaux des utilisateurs et les cœurs de réseau – qui assurent l'essentiel des fonctions du

réseau –, les antennes du réseau de 5G auront pour fonction de traiter les flux d'informations d'une manière plus « active ». Là où les réseaux actuels présentent des points fixes de convergence, les réseaux de 5G s'apparenteront davantage à des réseaux maillés à la configuration évolutive.

Ce changement s'inscrit dans une évolution de long terme des réseaux de télécommunication, qui voit ce que l'on pourrait appeler « l'intelligence » être de plus en plus déconcentrée. Il se traduit, du point de vue technique, par l'installation d'équipements informatiques de plus en plus sophistiqués dans les « bords de réseau », ce qui permet d'opérer des interceptions au-delà des cœurs de réseaux, par exemple au niveau des antennes-relais.

Jusqu'à présent, les efforts de sécurisation des réseaux de télécommunication portaient pour l'essentiel sur les cœurs de réseaux, seuls points de convergence fixes dans des réseaux hiérarchisés. Avec la 5G, ces efforts devront donc être étendus au-delà de ces cœurs, jusqu'aux « bords de réseaux ».

B. LA DÉFENSE NE SAURAIT SE DÉSINTÉRESSER DE LA 5G

Les changements qu'induit la 5G dans le secteur des télécommunications intéressent la défense à deux titres au moins :

– compte tenu de la place qu'ont pris les réseaux de télécommunication dans notre société, ils constituent aujourd'hui une fonction essentielle à la vie de la Nation et leur résilience est, à ce titre, d'importance vitale ;

– l'activité des forces armées ou de certains services « critiques » repose elle-même sur une utilisation massive de services de télécommunications qui, sur le territoire national, sont de plus en plus adossés à des réseaux civils.

1. L'usage croissant des réseaux civils par les forces armées sur le territoire national

Tant les forces de sécurité intérieure que les armées s'appuient aujourd'hui sur les réseaux civils de télécommunications pour leur activité opérationnelle sur le territoire national. Elles sont d'autant concernées par les opportunités comme par les vulnérabilités de la 5G qu'elles les utiliseront pour des usages par nature sensibles.

a. Les forces de sécurité intérieure s'appuient de plus en plus sur les réseaux civils pour certaines de leurs télécommunications

i. L'évolution du système de télécommunications des forces de sécurité intérieure est marquée par un adossement croissant aux réseaux civils

- *Des réseaux traditionnellement distincts des réseaux civils*

Selon les explications du général Bruno Poirier-Coutansais, chef du service des technologies et des systèmes d'information de la sécurité intérieure (ST-SI²) au ministère de l'Intérieur, et du colonel Gonzague Montmorency, chef du bureau de la prospective radio de la sous-direction des radios de ce service, les forces de sécurité intérieure opèrent aujourd'hui les réseaux suivants :

– pour la gendarmerie, le réseau Rubis, développé dans les années 1980, qui s'appuie sur environ 500 antennes de relais émettant dans la gamme des 80 MHz. Cette fréquence d'émission est peu performante en zone urbaine car elle pénètre mal les environnements complexes, mais elle est bien adaptée à la couverture du vaste territoire de la gendarmerie ;

– pour la police et les services d'incendie et de secours, l'infrastructure nationale partagée de télécommunications (INPT), la première l'utilisant sous le nom d'Acropol et les seconds sous celui d'Antarès. L'INPT repose sur 1 500 antennes de relais et fonctionne dans la gamme des 400 MHz, qui offre de plus grandes capacités tactiques en matière de pénétration des environnements complexes et de débits de transmissions.

Ces deux réseaux sont interopérables et couvrent ainsi **95 % à 98 % du territoire** en **télécommunications à bas débit**. Ils ont aujourd'hui une trentaine d'années mais restent opérationnels ; d'ailleurs, ils sont plus résilients que les infrastructures civiles, comme l'ont récemment montré, par exemple, les cas des inondations dans le Var et de Notre-Dame-des- Landes. Cette technologie a donc encore « *quelques années à vivre* », mais elle devra faire place à des systèmes à plus haut débit pour répondre aux nouveaux besoins des forces de sécurité intérieure – par exemple le partage de situations tactiques en temps réel.

- *Le choix d'un adossement partiel aux réseaux civils pour le renouvellement des capacités de télécommunication des forces de sécurité intérieure*

Les attentats de 2015 ont montré les limites des outils actuels pour le partage de situations tactiques au sein des forces de sécurité intérieure ; à défaut, les opérateurs ont été conduits à utiliser des réseaux civils de téléphonie peu sécurisés voire des applications de messagerie instantanée – tel Whatsapp. Des réflexions ont donc été conduites jusqu'en 2018 sur la modernisation des communications tactiques, aboutissant à un programme appelé **PC-Storm**.

Si l'on aurait pu envisager la construction d'un nouveau réseau propre aux forces de sécurité intérieure, basé par exemple sur des technologies de 4G, le ST-SI² a fait valoir que l'État ne serait probablement pas en mesure de consentir les investissements nécessaires non seulement à la création mais aussi à l'entretien d'un tel réseau, et que certains opérateurs de télécommunications français étaient tout à fait en mesure de le faire. Rubis et l'INPT reposent sur 2 000 antennes, contre 20 000 pour les réseaux des opérateurs civils ; en outre, ces derniers exploitent des bandes de fréquences beaucoup plus larges que les forces de sécurité intérieure.

C'est pourquoi qu'il a été choisi, dans le lot n° 3 du marché PC-Storm, de s'en remettre à la suite d'un appel d'offres aux services d'un opérateur civil – en l'espèce, Orange –, qui fournira aux forces de sécurité intérieure des services de télécommunications mobiles et leur garantira, en cas de saturation d'une cellule de communications, des **moyens propres à assurer la résilience des forces : service de préemption-*roaming* vers deux autres opérateurs** – en l'espèce, SFR et Bouygues. Les modalités de préemption et de priorisation négociées avec Orange ont pour intérêt d'éviter aux forces de sécurité intérieure les aléas des engorgements que connaissent parfois les services civils. De surcroît, Orange permet aux forces de disposer d'**un cœur de réseau spécifique**.

L'architecture des communications tactiques des forces de sécurité intérieure reposera donc sur les services d'un fournisseur civil, que compléteront :

– des **systèmes projetables de bulles tactiques** qui peuvent être déployées en cas de défaillance de l'opérateur. Un cœur de réseau national, en cours de construction dans le *data center* de la DGGN, permettra de mettre en réseau ces bulles tactiques ;

– les **bandes 28 et 68 dans la fréquence des 700 MHz**, qui ont été allouées au ministère de l'Intérieur. Il s'agit en effet pour la police et la gendarmerie nationales de savoir comment valoriser leur patrimoine radio après la fin du service des réseaux Rubis et INPT. Des tests sont en cours pour valider l'utilisation des bandes concernées par les *smartphones* ; leurs premiers résultats sont encourageants. Si ces capacités seront en tout état de cause insuffisantes en volume pour les besoins des forces de sécurité intérieure, elles n'en constituent pas moins pas moins un **moyen de fonctionnement** « **en mode dégradé** ».

ii. Les opportunités qu'offre la 5G et les vulnérabilités qu'elle crée sont prises en compte

- *Des opportunités : vers la « brigade sans fil » ?*

L'usage de la 5G par la police et la gendarmerie dépendra de la couverture du territoire national par cette technologie, la question de la couverture du territoire se posant avec davantage d'acuité pour la gendarmerie que pour la police voire pour les opérateurs, qui s'attachent davantage à la couverture de la

population que du territoire. La gendarmerie n'en poursuit pas moins une politique de numérisation nomade dont le général Bruno Poirier-Coutansais a résumé l'objectif en ces termes : « *la brigade sans fil* ».

D'ores et déjà, dans le cadre d'un programme appelé Néogend, la gendarmerie nationale a doté ses brigades de *smartphones* leur permettant d'accéder à nombre d'applications depuis le terrain, sans avoir à consulter les réseaux concernés depuis un poste fixe. Ainsi, l'esprit qui sous-tend la conception de Néogend consiste à aider les gendarmes à opérer un ensemble d'actes simples en situation de mobilité plutôt qu'à la caserne, où le déploiement des systèmes d'information les avait quelque peu recentrés depuis les années 1980. Néogend a permis de grands progrès en ce sens, mais la « brigade sans fil », c'est-à-dire le nomadisme, suppose des progrès en vidéo, en biométrie, en internet des objets, ou encore en exploitation de la domotique – source d'informations précieuses dans les enquêtes, mais aussi source de vulnérabilités. Pour ce faire, l'accroissement des débits permis par la 5G est très attendu.

- *Des vulnérabilités à maîtriser*

De l'étude du projet PC-Storm, le rapporteur pour avis retient trois séries d'enseignements sur le traitement des vulnérabilités dans l'utilisation par les forces des réseaux civils sur le territoire national :

– **l'appui de l'ANSSI est très utile à la conduite des programmes**, notamment pour les aspects stratégiques de la résilience des communications et, ce, très en amont dans l'élaboration des projets ;

– **le droit des marchés publics de défense et de sécurité, appliqué avec une certaine expertise, offre des leviers de maîtrise des équipements**. Pour le projet PC-Storm, deux lots sur sept ont pu être classifiés. Dans le cas du programme Néogend, par exemple, la gendarmerie voulait maîtriser non seulement les applications et les chiffres de son système de transmissions tactiques, mais aussi ses terminaux. Le marché a donc prévu l'obligation pour son titulaire de fournir à la gendarmerie les codes sources des matériels et des logiciels. Samsung, un temps pressenti, a finalement refusé cette exigence ; Sony l'a acceptée et a été retenu. De façon générale, une rédaction habile et soigneuse des cahiers des charges doit permettre de garantir la maîtrise par les forces des équipements qu'elles utilisent ;

– l'une des difficultés rencontrées dans le pilotage du projet PC-Storm a tenu au besoin de **s'assurer que les acteurs retenus sont dignes de confiance** ; or « *un acteur de confiance, ça se construit…* » Que l'opérateur retenu compte ou non l'État parmi ses actionnaires n'est pas dirimant ; il faut en revanche qu'il accepte de modifier une partie de son infrastructure et qui coopère efficacement avec l'ANSSI. **La plupart des États s'appuient sur un opérateur historique** : les forces armées britanniques n'ont plus de fréquences propres, AT&T a pris un clair *leadership* aux États-Unis et il en va de même en nombre d'endroits, par

exemple en Corée. Pour le projet PC-Storm, **Orange a fait preuve d'une grande maturité dans la prise en compte des besoins des forces** ; il leur a par exemple proposé un cœur de réseau dédié, là où d'autres soumissionnaires proposaient des cœurs mutualisés et, parfois, l'hébergement de données à l'étranger.

b. Les armées peuvent être conduites à utiliser les réseaux civils de télécommunication

Les armées elles-aussi peuvent être conduites à utiliser les réseaux civils de télécommunications sur le territoire national. Outre les cas dans lesquels les militaires utilisent des applications civiles destinées au grand public, tel Whatsapp, tel est le cas notamment pour deux systèmes conçus pour s'adosser – au moins en partie – à des réseaux civils ; Auxylium et DIPAD.

i. Le système DIPAD

Le système DIPAD, dispositif militaire d'agrégation de fréquences, a vu son déploiement commencer en 2016. Selon un récent rapport d'information sur le rôle des armées sur le territoire national (1), il s'agit d'un dispositif téléphonique qui repose en partie sur les réseaux GSM, peut être connecté au réseau ACROPOL en basculant d'un réseau d'arrondissement parisien à un autre, tout en étant compatible avec les réseaux militaires et doté d'une fonction de géoréférencement. Il vise à assurer la liaison entre les centres d'opérations – par exemple pour l'opération Sentinelle – et les hommes sur le terrain.

ii. Le système Auxylium

Le système Auxylium est constitué d'un téléphone de gamme commerciale, relié par Bluetooth à un poste radio. Le recours à un poste radio est en effet nécessaire pour que les militaires accèdent à leurs propres réseaux de communication, mais son articulation avec un *smartphone* leur permet d'utiliser aussi les réseaux civils de télécommunication. Par souci d'ergonomie, le modèle retenu pour ce poste radio, appelé Helium, est le moins encombrant du marché. Regrouper les réseaux civils et militaires sur un seul et même appareil aurait supposé de modifier le *smartphone*, ce qui s'est avéré difficile ; en outre, un dispositif de double carte SIM ne serait pas aussi efficace que l'architecture duale retenue, car il faudrait une ou deux minutes pour passer d'un réseau civil à un réseau militaire (et inversement), alors qu'Auxylium permet d'exploiter les deux types de réseaux civils simultanément. En outre, une architecture basée sur deux appareils présente des avantages en matière de sécurité de communications ; articulant deux batteries au lieu d'une, elle permet de ménager l'autonomie du système et elle constitue en elle-même une source d'économies, car le *smartphone* doit être renouvelé tous les trois ans, tandis que le poste radio peut durer six ou sept ans.

---

(1) Assemblée nationale, XIV^e^ législature, rapport d'information n° 3864 fait par MM. Olivier Audibert-Troin et Christophe Léonard sur la présence et l'emploi des forces armées sur le territoire national, juin 2016.

L'articulation trouvée entre réseaux civils et militaires permet d'utiliser le système Auxylium pour transmettre des ordres certifiés, même des ordres de tir, et géolocaliser les unités. Dès 2018, chaque chef de patrouille déployé en Île-de-France au titre de l'opération Sentinelle était équipé d'Auxylium.

Ainsi, les armées elles aussi, lorsqu'elles opèrent sur le territoire national, s'appuient sur les réseaux civils de télécommunications et sont donc intéressées au développement de la 5G.

2. L'importance vitale qui s'attache à la résilience des réseaux civils de télécommunication

Au-delà même du fait que les armées et les forces de sécurité intérieure utilisent les réseaux civils de télécommunications, la résilience de ce secteur constitue en soi un enjeu de sécurité nationale qui ne fait que gagner en acuité avec les opportunités offertes par la 5G et leurs corollaires en matière de vulnérabilités.

a. Un secteur reconnu d'importance vitale

Le code de la défense [(1)] établit un régime légal de sécurité des activités dites « d'importance vitale », qui repose sur un ensemble d'obligations faites aux « *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* », selon l'article L. 1332-1 de ce code.

La liste de ces opérateurs d'importance vitale (OIV) constitue un document classifié ; on peut néanmoins indiquer que **le secteur des communications électroniques, de l'audiovisuel et de l'information est reconnu comme un secteur d'activités d'importance vitale** et, qu'à ce titre, certains de ses acteurs peuvent être désignés comme OIV.

Les opérateurs et les équipementiers du secteur des télécommunications **travaillent ainsi de concert avec l'ANSSI**, ne serait-ce que pour la mise en œuvre des dispositifs d'autorisation de certains matériels présentés plus bas. L'Agence, dont l'encadré ci-après présente les missions, joue le rôle d'autorité nationale de sécurité des systèmes d'information ; c'est d'ailleurs sous l'autorité directe de la Secrétaire générale de la défense et de la sécurité nationale (SGDSN) qu'elle est placée. Ainsi, les acteurs du secteur des télécommunications sont d'ores et déjà en lien étroit avec le SGDSN et, lors des auditions du rapporteur pour avis, tous ont salué le haut niveau de compétence technique des personnels de l'Agence, estimant même pour certains que **grâce à l'ANSSI, la France est**

(1) Chapitre II « Protection des installations d'importance vitale » du titre III « Défense économique » du livre III « Mise en œuvre de la défense non militaire » de la première partie « Principes généraux de la défense » du code de la défense.

aujourd'hui « *en pointe* » dans la sécurisation des réseaux de télécommunications.

L'Agence nationale de sécurité des systèmes d'information

L'Agence nationale de sécurité des systèmes d'information est une entité relativement récente, créée il y a moins de dix ans sous la forme d'un service à compétence nationale. Elle est rattachée au Secrétariat général de la défense et de la sécurité nationale, lui-même directement rattaché au Premier ministre qu'il assiste dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

En application de l'article L. 2321-1 du code de la défense, la définition et la coordination de l'action gouvernementale en matière de sécurité et de défense des systèmes d'information relèvent de la compétence du Premier ministre, celui-ci disposant à cette fin de l'ANSSI qui assure la fonction d'autorité nationale de défense des systèmes d'information.

La principale mission de l'ANSSI est dès lors d'assurer la sécurité des systèmes d'information de l'État et de veiller à celle des administrations, des opérateurs d'importance vitale et des opérateurs de services essentiels, auprès desquels elle exerce par ailleurs une mission de conseil et de soutien. Elle a ainsi notamment vocation à intervenir au niveau technique en cas d'attaque affectant ces acteurs, en participant à la restauration des systèmes compromis et en mettant en œuvre des mesures de remédiation qui visent à bloquer l'attaquant et à « durcir » la sécurité des systèmes pour prévenir toute nouvelle intrusion. Elle peut également être amenée à intervenir ponctuellement auprès d'autres acteurs en cas de crise cyber, comme ce fut le cas auprès de TV5 Monde en 2015, ou de Saint-Gobain en 2017.

L'ANSSI a également vocation à conseiller les autorités publiques en amont d'une possible crise. C'est ainsi que l'ANSSI avait recommandé au Gouvernement de renoncer au vote électronique pour les Françaises et les Français de l'étranger lors des élections législatives de 2017, compte tenu d'un niveau de menace élevé et d'insuffisances constatées qui n'avaient pas permis d'homologuer la plateforme de vote.

En substance, il est possible de regrouper les missions de l'ANSSI au sein de trois domaines :

– la prévention, le conseil, la formation et la réglementation ;

– la détection des attaques, laquelle passe notamment par le développement, la mise en œuvre et le déploiement de sondes par l'ANSSI ;

– l'assistance apportée aux victimes d'attaques.

On soulignera par ailleurs que son article 4 prévoit que l'ANSSI est chargée de la qualification, de la certification, de l'agrément des services, produits et dispositifs de protection des systèmes d'information proposés par les prestataires privés.

Source : Assemblée nationale, XV^e^ législature, commission de la Défense nationale et des forces armées, rapport d'information n° 1141.

D'ailleurs, les dirigeants de l'Agence nationale des fréquences ont rappelé au rapporteur pour avis qu'historiquement, les bandes hertziennes appartenaient à la défense, ajoutant qu'en situation de guerre, l'ANFR transfère ses pouvoirs aux armées. Ils ont ajouté, d'ailleurs, que parmi les usagers du spectre hertzien, la

défense se distingue par son haut niveau de compétence technique, ce qui lui permet de coexister harmonieusement avec des opérateurs civils.

b. Un impératif stratégique de plus en plus prégnant

La protection des systèmes d'information et de communication contre les risques d'interception ou d'interférence, notamment par des moyens cybernétiques, a été identifiée comme une priorité par les documents stratégiques et les lois de programmation militaires successives depuis 2008. C'est d'ailleurs la loi de programmation militaire de 2013 qui a inscrit à l'article L. 2321-1 du code de la défense une disposition confirmant que la sécurité et la défense des systèmes d'information font partie intégrante de la stratégie de sécurité nationale et de la politique de défense que le Premier ministre a la charge de définir et de coordonner.

Dans la lignée de ces textes, la Revue stratégique de 2017 confirme que « *la résilience des fonctions essentielles à la continuité de l'État comme à la vie de la Nation [constituent] le fondement indispensable de notre liberté d'action* ». Elle constate que « *la numérisation massive que connaissent nos sociétés depuis une dizaine d'années et l'interconnexion globale des systèmes d'information et de communication suscitent l'émergence de nouvelles menaces comme de nouvelles opportunités* », soulignant que la numérisation et l'interconnexion des réseaux « *mettent à portée de tous de puissants outils d'expression, d'influence, de propagande et de renseignement, d'immenses volumes de données mais aussi de redoutables vecteurs d'attaque* », de même qu'elles « *favorisent la montée en puissance de nouveaux acteurs privés, qui s'imposent sur la scène internationale comme un défi à la souveraineté des États mais aussi comme des partenaires parfois essentiels* ».

3. Un enjeu de sécurité nationale bien compris par les grands acteurs stratégiques

Les enjeux stratégiques du déploiement de la 5G n'échappant à aucune des grandes puissances, la question de la sécurité de ces réseaux est au cœur de controverses – voire de litiges – qui tournent autour de la question de savoir si l'on peut avoir une égale et suffisante confiance en tous les équipementiers. Le fait que la législation chinoise fasse obligation aux entreprises ayant leur siège en Chine de collaborer avec les services de renseignement de ce pays cristallise des craintes autour des équipementiers de ce pays. Dans ces questions, la position de la France, à laquelle correspond d'ailleurs celle de l'Union européenne, n'est pas exactement la même que celle des États-Unis.

a. Une approche américaine de la sécurité des réseaux de 5G fondée sur la sélection des fournisseurs d'équipements

Les administrations américaines successives expriment publiquement, depuis une dizaine d'années au moins, leurs fortes réticences à voir des

équipements de réseaux américains fournis par l'industrie chinoise, dont les deux premiers acteurs du secteur sont Huawei et ZTE.

Ainsi, dès 2008, l'administration américaine a fait obstacle à la vente de la société américaine 3Com, spécialisée dans les équipements de réseaux, à Huawei en invoquant des raisons de sécurité nationale ; c'est pour les mêmes motifs qu'en 2011, selon la presse, elle a vivement découragé l'opérateur Sprint d'utiliser des équipements de la même société chinoise pour la construction de son réseau de 4G ; de même, en 2012, le même équipementier a été exclu du projet de câble sous-marin transatlantique *Hibernia Express*. En 2018, les autorités américaines ont interdit l'utilisation des équipements de Huawei et de ZTE dans les principaux réseaux des administrations publiques américaines.

Il ressort en outre des débats au Congrès et de la lecture de la presse américaine que les États-Unis envisagent d'interdire aux entreprises américaines d'utiliser des équipements d'origine chinoise dans les réseaux critiques de télécommunications. De telles mesures ont déjà été prises en Australie, où Huawei et ZTE sont écartés de la construction des réseaux de 5G, ainsi que, vraisemblablement, en Nouvelle-Zélande. Au Royaume-Uni, British Telecom a fait connaître publiquement son intention d'expurger les parties sensibles de ses réseaux de 3G et de 4G des équipements chinois, et de ne pas y avoir recours pour une large part de son futur réseau de 5G. Dernier événement notable en date dans cette série d'initiatives américaines contre les équipementiers chinois, les États-Unis auraient formellement mis en garde les autorités allemandes dans les termes suivants : « *si des acteurs non dignes de confiance se retrouvent dans les réseaux d'un allié, cela pourrait soulever, à l'avenir, des questions concernant l'intégrité et la confidentialité de communications sensibles entre un tel pays et ses alliés* » ce qui pourrait « *représenter une menace pour une bonne coopération et certains partages d'informations* ».

L'approche américaine de la sécurisation des réseaux de 5G fait ainsi une large part à la sélection d'équipementiers autres que chinois.

b. Une approche française fondée sur la certification des équipements et la résilience des architectures de réseaux

L'approche française de la sécurisation des réseaux de 5G ne fait pas reposer autant qu'aux États-Unis la résilience de ces réseaux sur le seul choix d'un équipementier. C'est en ce sens que le directeur général de l'ANSSI a assuré le rapporteur pour avis que, dans son soutien à la proposition de loi, le gouvernement ne s'inscrit pas dans le même état d'esprit que celui des États-Unis vis-à-vis de Huawei ou de ZTE. Au contraire, l'objectif poursuivi par les Français consiste à établir un cadre clair pour que les industriels planifient leurs investissements – qui sont lourds – de façon avisée.

Cette approche s'inscrit d'ailleurs dans un cadre européen qui doit être consolidé d'ici la fin de l'année 2019. Ainsi, le Conseil européen, à l'issue de sa

réunion du 22 mars 2019, considérant qu'« *il convient d'accorder une attention particulière à l'accès aux données, à leur partage et à leur utilisation, à la sécurité des données et à l'intelligence artificielle, dans un environnement de confiance* » et appelé la Commission à publier une recommandation relative à une approche concertée en matière de sécurité des réseaux de 5G.

Le 26 mars 2019, la Commission a publié une série de recommandations en ce sens, présentées comme « *une combinaison d'instruments législatifs et de moyens d'action destinés à protéger nos économies, nos sociétés et nos systèmes démocratiques* » :

– elle a invité chaque État membre à procéder d'ici la fin du mois de juin 2019 à une **évaluation des risques** liés aux infrastructures des réseaux de 5G tenant compte « *de différents facteurs, tels que les risques techniques et les risques liés au* ***comportement des fournisseurs ou des opérateurs, y compris ceux de pays tiers*** » ;

– sur la base de cette évaluation, les États sont invités à prendre, le cas échéant, les mesures nécessaires pour garantir « ***l'obligation renforcée, pour les fournisseurs et les opérateurs, de garantir la sécurité des réseaux*** » de 5G, la communication de la Commission rappelant explicitement que « *les États membres de l'Union européenne ont le droit d'exclure de leurs marchés, pour des raisons de sécurité nationale, des entreprises qui ne respectent pas leurs normes et leur législation* » ;

– le groupe de coopération constitué par la directive sur la sécurité des réseaux et des systèmes d'information entre les autorités nationales chargées de la sécurité des systèmes d'information travailleront ensuite, avec le soutien de la Commission et de l'Agence de l'Union européenne pour la cybersécurité, en vue d'une **évaluation coordonnée des risques** au plus tard le 1er octobre 2019 ;

– sur cette base, les États membres s'accorderont sur un ensemble de « ***mesures d'atténuation*** » du risque, la Commission précisant que ces mesures peuvent inclure « ***des exigences de certification, des essais, des contrôles, ainsi que le recensement des produits ou fournisseurs jugés potentiellement non sûrs*** » ;

– le cas échéant, des mesures supplémentaires pourraient être prises au niveau européen, où une première directive sur la sécurité des réseaux et des systèmes d'information vient d'être élaborée, où le Parlement européen vient d'approuver un règlement sur la cybersécurité et où la réglementation en matière de télécommunications est appelée à évoluer.

Ainsi, l'approche de la Commission européenne fait une large place à la certification des équipements. Le règlement susmentionné sur la cybersécurité prévoit d'ailleurs l'élaboration d'un futur cadre européen de certification de cybersécurité pour les produits, processus et services numériques ; la

communication de la Commission invite aussi les États membres à mettre au point des systèmes européens de certification spécifiques en ce qui concerne la 5G.

II. LE CADRE JURIDIQUE DE LA SÉCURISATION DES RÉSEAUX DE TÉLÉCOMMUNICATION DOIT ÊTRE ADAPTÉ À LA « 5G »

La présente proposition de loi tend à instituer un nouveau régime d'autorisation administrative des équipements constituant les réseaux de 5G – non seulement les matériels mais aussi les logiciels –, afin de permettre à l'État de conserver la maîtrise de l'architecture de ces réseaux d'importance vitale.

En la matière, l'État ne part pas de rien : un régime d'autorisation a déjà été mis en œuvre pour certains équipements de télécommunications en vue de contrôler leur fiabilité technique. Cependant, cette base juridique ne paraît plus suffisante pour garantir la résilience des réseaux tels qu'ils seront reconfigurés à l'occasion du déploiement de la 5G, ce qui appelle une initiative législative d'autant plus urgente que ce déploiement est prévu sous peu de temps.

A. LES LIMITES DU RÉGIME ACTUEL DE CONTRÔLE DES ÉQUIPEMENTS DE RÉSEAU À L'HEURE DE LA 5G

Le dispositif en vigueur d'autorisation administrative de certains équipements matériels ou logiciels composant les réseaux radioélectriques ont pour base légale les dispositions du code pénale protégeant **le secret de la vie privée et de la correspondance**. Jusqu'à présent, cette base légale a permis à l'État de contrôler l'intégrité de ces équipements, et ce au moins autant dans une optique de protection des intérêts de la défense et de la sécurité nationale que de protection du secret de la correspondance. Mais, avec la diversification considérable des usages des réseaux radioélectriques à laquelle la 5G ouvre la voie, cette base légale s'avère aujourd'hui trop étroite pour permettre à l'État de s'assurer de la résilience de ces réseaux dans des conditions cohérentes avec leur importance dans la résilience de la Nation.

1. Le cadre légal en vigueur

a. Un régime d'autorisation des équipements de réseau dérivée du droit de la protection du secret de la correspondance et de la vie privée

Le 1° de l'article 226-3 du code pénal réprime 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* », sans autorisation administrative, lorsque ces appareils ou dispositifs répondent à l'une des conditions alternatives suivantes :

– être « *de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15* », c'est-à-dire **l'atteinte au secret de la correspondance privée** ;

– s'ils sont « *conçus pour la détection à distance des conversations* », permettre de « *réaliser l'infraction prévue par l'article 226-1* », c'est-à-dire **l'atteinte à la vie privée** ;

– avoir pour objet « ***la captation de données informatiques*** ».

L'infraction est constituée même en cas de négligence. Les articles R. 226-1 à R. 226-12 du code pénal ont défini la procédure applicable pour la délivrance de cette autorisation administrative.

Selon leurs dispositions, l'autorisation mentionnée est délivrée par le Premier ministre après avis d'une commission consultative, présidée par le directeur général de l'ANSSI et composée de représentants des administrations de l'État concernées, d'un représentant de la Commission nationale de contrôle des interceptions de sécurité et de deux personnalités qualifiées désignées par le Premier ministre. C'est l'ANSSI qui instruit les dossiers et se trouve, ainsi, investie d'un rôle de premier plan dans la mise en œuvre des dispositions pénales précitées. C'est à ce titre qu'elle s'est imposée comme l'interlocuteur de référence des opérateurs pour la sécurisation de leurs réseaux radioélectriques.

Comme l'a fait observer M. Guillaume Poupard, ce dispositif constitue une **spécificité française** ; il a en effet pour objet la protection de la vie privée et du secret des correspondances, droit qui n'a pas son équivalent dans tous les pays.

Lors de l'établissement de ce régime d'autorisation, il s'agissait selon ses explications de contrôler non pas les « cœurs de réseaux » de téléphonie mobile, mais divers matériels tels que les « micros espions ». C'est néanmoins cette base juridique qui a permis à l'administration de contrôler la sécurité des équipements les plus sensibles des réseaux de télécommunications mobiles, ce qui représente aujourd'hui la plus grande part des dossiers instruits en application de l'article 226-3 précité. **Ce régime d'autorisation pèse non seulement sur les équipementiers mais aussi sur les opérateurs qui utilisent leurs produits**.

b. Un champ d'application progressivement étendu, au fur et à mesure de l'évolution technologique

La liste des équipements dont la mise sur le marché est soumise à l'autorisation du Premier ministre est fixée, par un renvoi prévu à l'article R. 226-1 du code pénal, par un arrêté du Premier ministre en date du 4 juillet 2012 [(1)].

Cette liste a été étendue par un nouvel arrêté en date du 11 août 2016 [(2)] en application de l'article 23 de la loi de programmation militaire de 2013, qui a étendu le champ d'application de l'article 226-3 précité des équipements « *conçus*

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

(2) Arrêté du 11 août 2016 modifiant l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal.

pour réaliser » des interceptions ou des captations de données à l'ensemble de ceux qui sont « *de nature à permettre la réalisation* » des mêmes faits. Ainsi, seront soumis à autorisation administrative « *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* ». Le régime d'autorisation fondé sur le droit pénal s'applique ainsi à tous types de matériels permettant l'écoute de personnes à leur insu, l'enregistrement de communications téléphoniques, l'interception les données transmises sur les réseaux de télécommunications de tous types – internet comme la téléphonie – et, ce, quelle que soit leur nature, comme des données de connexion à des sites internet, des textos ou des captures d'écran.

Afin de laisser aux sujets de cette obligation le temps de se préparer aux démarches administratives nécessaires, l'entrée en vigueur de cette modification de la liste a été renvoyée au 1er octobre 2021 à la demande de l'ARCEP. En effet, sous une apparence anodine, la modification prévue par la loi de programmation militaire de 2013 a pour conséquence un considérable surcroît de travail en raison d'une tendance, dans l'évolution technologique des équipements de télécommunication, à ce que les équipements d'interface en bordure de réseau deviennent de plus en plus « regardants » sur le contenu des flux d'information qu'ils transportent, ne serait-ce que pour hiérarchiser les flux en fonction de leur caractère prioritaire. Selon les explications de M. Guillaume Poupard, ce sont de véritables techniques d'inspection profonde de paquets – ou *deep packet inspection* (DPI) – qui sont mises en œuvre.

2. Les limites du dispositif actuel face aux spécificités de la 5G

a. Une base légale trop étroite à l'ère de la 5G

Si le droit en vigueur, trouvant sa base juridique dans les règles pénales de protection du secret de la correspondance et de la vie privée, a offert à l'État des moyens de s'assurer de l'intégrité des réseaux jusqu'à la 4G, il apparaît qu'au rythme actuel de l'évolution technologique, le dispositif de contrôle de la sécurité des nouveaux réseaux perd en efficacité à plusieurs égards :

– ce n'est qu'à partir du 1er octobre 2021 que la procédure prévue par l'article 226-3 du code pénal permettra à l'ANSSI de contrôler « *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* », c'est-à-dire **non seulement les cœurs de réseau, mais aussi les équipements d'interface en bordure de réseau, notamment les antennes-relais**. Ainsi, par un effet

d'aubaine, certains acteurs peuvent être tentés de presser leurs investissements afin de les réaliser avant la mise en œuvre des contrôles élargis prévue à partir du 1er octobre 2021. Ce risque est d'autant plus grand que la 5G, dont le déploiement devrait être largement entamé avant cette date, accélérera la tendance qu'a, dans les réseaux, « l'intelligence » à déborder de leurs cœurs vers leurs bords, la 5G étant précisément conçue pour que les flux d'information ne transitent pas systématiquement par les cœurs de réseau afin de ne pas les engorger. Comme l'explique M. Guillaume Poupard, « *un cœur de réseau 5G, ce sera dans le fond un réseau IP* ». Ainsi, pour un contrôle efficace de la sécurité des réseaux, le champ des équipements à contrôler s'accroît considérablement ;

– surtout la base légale sur laquelle a été fondée la procédure de contrôle prévue à l'article R. 226-3, pour légitime qu'elle soit, se limite au secret de la correspondance et à la protection de la vie privée des personnes. Or, **avec la 5G, cette base légale peut devenir insuffisante** : quand deux automates se transmettront des informations, difficile d'y voir un élément de la vie privée à protéger au titre du secret de la correspondance.

En somme, on pourrait dire, pour simplifier les choses, que le régime de contrôle des équipements de réseaux repose aujourd'hui sur une base légale conçue à une époque où ces réseaux servaient essentiellement à des correspondances privées et guère à des applications industrielles, et qu'il se limite au contrôle de l'intégrité technique des équipements sans prise en compte de la résilience de l'architecture des réseaux en elle-même. Le changement de paradigme technologique qu'opère la 5G appelle un changement de paradigme juridique pour son dispositif de contrôle.

b. L'urgence d'un changement de paradigme juridique

Compte tenu de la nouveauté des technologies de 5G et du coût des investissements nécessaires, les équipementiers ont besoin de guides pour garantir que les produits qu'ils vendent font bien ce qu'ils sont censés faire, de même que les opérateurs ont besoin de savoir quels équipements ils seront autorisés à exploiter. Les représentants de CISCO ont souligné que l'expérience de la 4G montre qu'il est plus simple pour l'industrie que les pouvoirs publics fixent d'emblée une doctrine claire sur diverses questions techniques. Là réside l'attente d'une part de l'industrie vis-à-vis de la loi et de ses textes d'application.

Or, le déploiement des réseaux de 5G étant prévu dans des délais très rapides, la modernisation du cadre juridique du contrôle de leur sécurité revêt un certain caractère d'urgence. Tel est l'objet du texte proposé.

B. LE DISPOSITIF PROPOSÉ

1. Un nouveau régime d'autorisation préalable à l'exploitation d'équipements de réseaux radioélectriques

L'**article 1er** de la présente proposition de loi tend à insérer au chapitre II du titre I du livre II du code des postes et des communications électroniques une nouvelle section intitulée « Régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques » et composée de quatre articles.

a. Un régime d'autorisation visant à préserver les intérêts de la défense et de la sécurité nationale

i. Un régime d'autorisation fondé sur l'importance stratégique de la résilience des réseaux

La rédaction proposée pour le I. de l'article L. 34-11 du code précité par les **alinéas 4 et 5** vise à soumettre à une autorisation du Premier ministre l'exploitation, sur le territoire national, « *d'appareils, à savoir tous dispositifs matériels ou logiciels* » permettant de connecter les équipements des usagers au réseau radioélectrique mobile. **Cette autorisation est explicitement « *destinée à préserver les intérêts de la défense et de la sécurité nationale* »**. Selon les précisions de la direction générale des entreprises du ministère de l'Économie, si cette base juridique est très différente de celle du droit en vigueur, le gouvernement n'envisage pour autant **aucun changement majeur de doctrine dans la pratique de ces contrôles**.

Son champ d'application matériel est limité aux appareils qui « *présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau* », dont l'alinéa 5 charge de Premier ministre d'établir la liste par arrêté. Les représentants des opérateurs, faisant valoir qu'il est indispensable pour eux de connaître cette liste avant de planifier de lourds investissements, ont souhaité pouvoir en disposer dans les meilleurs délais. Cette demande paraît raisonnable aux yeux du rapporteur pour avis.

Si le droit commun veut que le silence gardé par l'administration vaille accord, il a été précisé au rapporteur pour avis que le gouvernement envisageait de prendre un décret portant dérogation à ce principe pour l'autorisation en question. Ainsi, **le silence gardé par le Premier ministre ne vaudra pas autorisation implicite**.

ii. Un régime aussi souple que possible pour les mises à jour

Le premier alinéa du texte proposé pour le II. de l'article L. 34-11 du code des postes et des communications électroniques (**alinéa 6**) précise que l'autorisation est donnée pour « *un ou plusieurs modèles* » et « *une ou plusieurs versions* » des appareils susmentionnés.

Cette disposition vise à **éviter que toute mise à jour logicielle ou que toute modification technique d'un équipement déjà contrôlé soit systématiquement soumise à une nouvelle procédure** d'autorisation préalable, dans les mêmes formes que l'autorisation initiale et, partant, avec les mêmes délais et les mêmes coûts administratifs. Ainsi, l'ANSSI pourra choisir de traiter les mises à jour au cas par cas, suivant trois modalités :

– pour les cas les plus simples, l'autorisation du matériel ou du logiciel initial pourra porter également sur certains types de mises à jour ;

– le cas échéant, l'ANSSI pourra assortir l'autorisation du matériel ou du logiciel initial d'une obligation de déclaration de certains types de mises à jour ;

– pour les cas comportant des risques éventuels, les mises à jour pourront être soumises à autorisation au même titre que le matériel ou le logiciel initial.

iii. Une durée qui peut être longue

Le même alinéa fixe à **huit ans** la durée maximale pour laquelle sera donnée l'autorisation. Selon le rapporteur pour avis, cette durée représente un délai manifestement un peu long au regard des évolutions technologiques. Le directeur général de l'ANSSI a expliqué que ce délai, qui n'est prévu par le texte que comme un plafond, a été choisi en vue de rassurer les opérateurs. En effet, des autorisations de durée trop limitée peuvent déstabiliser leurs plans d'investissement. Cependant, à l'inverse, accorder une autorisation pour une durée excédant largement l'horizon des évolutions prévisibles des technologies pourrait conduire l'État à laisser un opérateur déployer de grands équipements coûteux, comme les antennes, pour retirer l'autorisation peu de temps après, ce qui ne serait guère plus satisfaisant, d'autant que le remplacement d'un équipement constitue pour un opérateur une opération complexe à plusieurs égards :

– un remplacement d'équipements physiques (appelé *swap*) est en soi une opération lourde et coûteuse ;

– chaque opérateur est en réalité assez étroitement lié à l'équipementier retenu pour une installation de « plaque » de réseau, dans la mesure où accumuler des équipements de plusieurs fournisseurs est techniquement possible selon les représentants de Samsung, mais fort complexe selon les représentants des opérateurs.

Ainsi, c'est dans la pratique qu'un équilibre sera à trouver pour fixer aux autorisations une durée qui offre le plus de sécurité possible aux plans d'affaires des opérateurs.

b. Un régime pesant sur les seuls opérateurs

Le champ d'application subjectif de cette obligation est **limité aux opérateurs reconnus d'importance vitale** en application des articles L. 1332-1 et

L. 1332-2 du code de la défense et, plus précisément, à ceux qui sont ainsi reconnus « ***en vertu de leur activité d'exploitant****, direct ou par l'intermédiaire de tiers fournisseurs, d'un réseau de communications électroniques ouvert au public* ». Ainsi, **le champ d'application proposé pour ce régime d'autorisation exclut les opérateurs dits « verticaux »**. L'obligation porte ainsi sur les opérateurs et non sur les équipementiers.

Cette **approche par opérateur** et non par équipement est particulièrement nécessaire avec la 5G, car avec un équipement virtualisé, le même équipement peut avoir un effet tout à fait différent selon ses conditions d'exploitation par un opérateur ou un autre. Les représentants des opérateurs entendus par le rapporteur pour avis ont cependant fait valoir que les opérateurs dépendent de leurs fournisseurs pour répondre avec précision aux questions que pose l'ANSSI sur les spécifications de leurs équipements, estimant qu'une telle dépendance pouvait les placer en situation d'insécurité juridique en cas de déclaration erronée, même faite de bonne foi. Le fait que le régime d'obligation proposé – qui pèse sur les seuls opérateurs – s'ajoute au régime en vigueur, qui pèse aussi sur les équipementiers, devrait contribuer à simplifier le traitement des demandes, dans la mesure où l'ANSSI devra étudier un équipement au titre de la procédure fondée sur l'article 226-3 du code pénal avant d'instruire les demandes d'autorisation d'utilisation du même équipement au titre du dispositif proposé.

c. Un régime d'autorisation a priori

Le texte proposé prévoit une **procédure d'autorisation *a priori*, et non une procédure de déclaration avec droit d'opposition** comme peuvent le souhaiter certains acteurs du secteur, soucieux d'alléger la charge administrative liée au nouveau dispositif et de ne pas allonger les délais procéduraux qui pourraient retarder le déploiement des réseaux. Cependant, une approche *a priori* paraît *in fine* plus sécurisante pour ces acteurs. En effet, des dommages résultant d'actes malveillants seraient très lourds à traiter *ex post* et, si les règles de contrôle devaient être durcies ultérieurement, les opérateurs auraient à supporter des investissements correctifs coûteux.

Certes, une telle procédure suppose une instruction, laquelle nécessite du temps et quelques moyens. Plusieurs représentants des opérateurs et des équipementiers ont jugé, devant le rapporteur pour avis, que l'ANSSI ne pourrait mettre en œuvre cette nouvelle procédure qu'avec des moyens accrus. Au contraire, le directeur général de l'ANSSI a indiqué que l'Agence ne réclamait pas de moyens supplémentaires pour mettre en application la procédure proposée. Pour lui, **la clé de la fluidité de la procédure réside dans l'anticipation des demandes** : il est bon que les opérateurs engagent des discussions avec l'ANSSI sur leurs projets à une phase très amont de ces derniers.

En tout état de cause, l'importance que revêt la garantie de la résilience des réseaux de télécommunication justifie aux yeux du rapporteur pour avis une procédure de contrôle sérieuse.

d. Un régime d'autorisation « territorialisé »

L'**alinéa 6** précise que l'autorisation est délivrée « *pour un périmètre géographique* » précisé par l'opérateur qui soumet la demande. La procédure actuelle, s'attachant seulement à l'intégrité technique des matériels, ne comporte aucune disposition permettant à l'État de contrôler l'architecture des réseaux du point de vue de leur agencement géographique.

Selon les explications du ministère de l'Économie, cette approche géographique, qui constitue une nouveauté, poursuit deux buts principaux :

– permettre d'exiger des **conditions de sécurité plus élevées pour les zones dans lesquelles sont situées des installations ou des services plus sensibles**, de façon cohérente avec les préoccupations de défense nationale ;

– **éviter un monopole d'équipement** dans certaines zones et, avec le développement de la concurrence, pousser les opérateurs et les équipementiers à rechercher les voies et moyens d'une plus grande interopérabilité de leurs réseaux. C'est à ce titre que le zonage s'appréciera non seulement au regard de la sensibilité des installations de la zone concernée, mais aussi de façon à **garantir la résilience des réseaux en cas de défaillance – involontaire ou non– d'un équipementier**.

Pour l'ANSSI, il est cependant vraisemblable que les opérateurs ne seront pas conduits à dessiner la carte de leurs réseaux « en dentelle » : ils opèrent des zonages en six ou sept plaques au plus et ne créeront pas une zone spécifique autour d'une installation isolée intéressant la défense. En effet, le zonage n'est pas imposé par l'État ; ce sont les opérateurs qui présentent leurs choix de délimitation des « plaques » de réseau.

L'intérêt principal de cette approche par le zonage consiste en réalité à **éviter une homogénéité trop poussée des équipements**. En effet, le fait que tout équipement soit faillible, pour des raisons de confiance ou d'autres raisons, a pour conséquence que l'impératif de résilience suppose une certaine hétérogénéité des équipements, **quitte à ce que, dans une même zone, un même équipement puisse être autorisé pour un opérateur mais pas pour un autre**. D'ailleurs, à ce titre, l'arrivée de Samsung et de ses partenaires japonais sur le marché français représente une bonne chose.

2. Des sanctions en cas d'infraction aux règles d'autorisation

L'**article 2** vise à créer au chapitre V du titre premier du livre II du code des postes et des communications électroniques un article L. 39-1-1 qui établit un régime de sanction en cas d'infraction au nouveau régime de d'autorisation.

Il crée ainsi deux infractions, punies d'un an d'emprisonnement et de 150 000 euros d'amende pour toute personne physique, ces quantums de peine étant quintuplés pour les personnes morales :

– l'exploitation sans autorisation préalable des appareils entrant dans le champ de l'autorisation ;

– le défaut d'exécution, même partiel, des injonctions que peut prononcer le Premier ministre en cas de défaut d'autorisation.

De surcroît, des sanctions pénales complémentaires sont prévues par renvoi aux articles L. 39-6 et L. 39-10 du même code : la confiscation des équipements, leur destruction aux frais du condamné, l'interdiction d'établir un réseau radioélectrique mobile pour une durée d'au plus trois ans, l'interdiction (temporaire ou définitive) d'exercer directement ou indirectement cette activité, ainsi que l'affichage de la décision de sanction ou sa diffusion par voie électronique.

3. Un régime applicable de façon rétroactive

L'**article 3** fixe au 1er février 2019 la date d'installation des équipements auxquels s'applique le dispositif proposé par la présente proposition de loi. Les opérateurs concernés auront deux mois à compter de l'entrée de vigueur de ce texte pour déposer leurs dossiers de demande d'autorisation.

Cette application rétroactive permettra de dissuader les opérateurs de hâter des opérations dont ils pourraient craindre que l'État n'y soit pas favorable pour des motifs qui tiennent aux intérêts de la défense et de la sécurité nationale mais sur lesquels la législation actuelle ne permet pas de formuler une décision de refus d'autorisation.

C. POUR UNE EXTENSION DU DISPOSITIF AUX OPÉRATEURS DITS « VERTICAUX »

Le rapporteur pour avis observe que le dispositif proposé s'applique aux seuls opérateurs d'importance vitale qui exercent l'activité d'opérateur de réseau à titre principal, et non aux opérateurs dits « verticaux », fussent-ils reconnus d'importance vitale.

Certes, le dispositif de l'article 226-3 continuera à s'appliquer à eux, de même que ceux qui exercent une activité sensible sont par ailleurs soumis aux obligations des OIV. L'ANSSI dispose donc de certains outils pour contrôler la résilience de leurs systèmes de télécommunication. L'argument principal en faveur de leur exclusion du champ d'application subjectif du texte proposé consiste surtout à faire valoir que les opérateurs de télécommunications « grand public » présentent un **risque systémique plus fort** que les opérateurs « verticaux ».

Pour le rapporteur pour avis, il ne s'en attache pas moins aux réseaux des opérateurs « verticaux » trois grands enjeux de sécurité, que la 5G pourrait rendre particulièrement prégnants :

– si les opérateurs en question ont été désignés comme OIV, c'est par nature que **leurs activités sont sensibles et, à ce titre, la sécurité de réseaux qui sous-tendent ces activités mérite d'autant plus d'attention que la 5G en accroîtra les vulnérabilités** ;

– nombre de ces OIV sont en **situation de monopole ou de quasi-monopole** dans leur secteur d'activité. Leur situation est à cet égard différente de celle des opérateurs de télécommunications mobiles destinées au grand public : dans ce secteur concurrentiel, la coexistence de plusieurs réseaux offre à l'infrastructure d'ensemble une certaine redondance. À l'inverse, pour des OIV en situation de monopole, les intérêts de la défense et de la sécurité nationale supposent que l'État puisse **s'assurer de la résilience des réseaux nécessaires à la continuité de leurs activités sensibles, même en l'absence de réseaux concurrents**. Les vulnérabilités accrues que la 5G fera peser sur ces réseaux rendent leur résilience d'autant plus nécessaire ;

– contrairement peut-être à ce qui était anticipé il y a encore peu de temps, il est possible que des opérateurs « verticaux » sollicitent l'attribution de fréquences utiles à la 5G, comme l'ont déjà fait certains de leurs homologues allemands. En effet, en Allemagne, 100 MHz de bandes hertzienne ont été réservés à ces opérateurs dans l'allocation des fréquences dédiées à la 5G allemande. Or, comme on l'a dit plus haut, **les opérateurs « verticaux » peuvent tout à fait avoir intérêt à ouvrir leurs services de télécommunications à un public de plus en plus large à la faveur des applications et usages nouveaux que promet la 5G**. Dans ces conditions, aux yeux du rapporteur pour avis, il n'y a pas de raison que le contrôle de la résilience de leurs réseaux soit moins approfondi que pour les opérateurs de réseaux téléphoniques, dès lors que ces acteurs sont reconnus d'importance vitale.

De façon générale, la frontière entre réseaux publics et réseaux privés est appelée à s'estomper avec la 5G et, s'agissant d'opérateurs reconnus d'importance vitale, **le risque systémique s'étendra probablement au-delà des réseaux des quatre grands opérateurs** de téléphonie mobile actuels.

TRAVAUX DE LA COMMISSION

La commission de la défense nationale et des forces armées examine, sur le rapport de M. Thomas Gassilloud, 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), au cours de sa réunion du mardi 2 avril 2019.

M. le président Jean-Jacques Bridey. Nous sommes réunis aujourd'hui pour examiner 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, dont la commission s'est saisie pour avis.

M. Thomas Gassilloud, rapporteur, vous présentera le texte. Après les interventions des représentants des groupes, nous examinerons les amendements déposés à la commission. Cette proposition de loi sera examinée demain par la commission des Affaires économiques, saisie au fond, puis en séance publique, le 10 avril.

M. Thomas Gassilloud, rapporteur pour avis. Je tiens à vous remercier de m'avoir nommé rapporteur pour avis. Il nous a semblé important que la commission de la Défense se saisisse de ce texte et marque ainsi toute l'attention qu'elle porte à cette question. Cet examen nous conduit à nous aventurer au-delà du code de la défense, mais cette problématique revêt d'indéniables enjeux de défense et de sécurité nationale.

Commençons par souligner que la 5G constitue une rupture technologique : les réseaux deviendront de plus en plus virtuels, au point que nombre de leurs composants seront remplacés par des logiciels ; ils seront aussi déconcentrés, les fonctions « intelligentes », aujourd'hui situées dans les cœurs de réseaux seront disséminées jusqu'aux antennes. Pour sécuriser ces réseaux, il ne faudra plus uniquement protéger les cœurs de réseaux mais l'ensemble des éléments déconcentrés. La 5G ouvre de nouvelles fonctionnalités, mais en rendant le réseau plus sensible, elle l'expose plus largement aux cyberattaques.

La 5G revêt des enjeux de défense et de sécurité nationale pour des raisons qui tiennent davantage à ses usages et à ses applications, dont nous avons encore du mal à imaginer l'étendue. Cette technologie permettra des progrès considérables pour ce qui est de la capacité des réseaux. D'abord, elle accroîtra considérablement les débits, qui pourraient atteindre un ou plusieurs gigaoctets par seconde, ce qui revêt une importance considérable dans le domaine de la défense, notamment pour le combat « collaboratif ». Les temps de latence dans les transmissions seront également réduits, ce qui permettra notamment aux véhicules autonomes d'être beaucoup plus réactifs et, sur le champ de bataille, de mettre

plus rapidement en relation un capteur et un effecteur, et de gagner ainsi la supériorité opérationnelle. Enfin, les réseaux virtualisés de 5G pourront être orientés presque en temps réel en fonction des besoins locaux, ce qui permettra d'éviter la saturation des réseaux ; notons que la concentration des moyens est une logique bien maîtrisée par les forces dans leurs zones d'intervention.

Les forces armées et de sécurité intérieure utiliseront beaucoup la 5G, comme elles le font déjà avec la 4G. La gendarmerie a ainsi complété son réseau dédié Rubis, avec des relais sur l'ensemble du territoire national, par le système NéoGend, qui est adossé aux réseaux mobiles de 4G et qui permet à chaque gendarme d'interroger les bases de données nécessaires *via* un smartphone. L'armée de terre, quant à elle, utilise le système Auxylium, dont il est question dans le rapport que j'ai publié avec Olivier Becht, pour piloter sur le terrain les équipes de l'opération Sentinelle. La tendance veut ainsi que les services de l'État disposent de moins en moins de leurs propres réseaux dédiés, ce qui rend l'usage des réseaux d'autant plus sensible. La 5G intéresse donc la défense et la sécurité nationale à double titre : les réseaux sont de plus en plus vitaux pour le fonctionnement des services de la Nation et les secours, les forces de sécurité intérieure et les armées en auront de plus en plus besoin.

À l'heure de la 5G, quelles mesures le texte propose-t-il pour garantir la sécurité des réseaux – éviter la fuite de données – et leur résilience – permettre la continuité du service ?

Tandis que les États-Unis et les pays anglo-saxons ont choisi une approche rigoriste en sélectionnant les équipementiers – les États-Unis visent à exclure purement et simplement les fournisseurs chinois –, une approche européenne de la sécurisation des réseaux est en train de se construire. La France est en pointe, puisqu'elle a utilisé l'article 226-3 du code pénal, qui visait initialement à protéger la vie privée et le secret de la correspondance, pour soumettre à autorisation les équipements de réseau. Le 22 mars, le Conseil européen a appelé la Commission à prendre des initiatives en vue d'établir un cadre européen de sécurisation de la 5G, ce qu'elle a fait le 26 mars. Prenant sans doute en compte les enjeux économiques de l'accès au marché chinois, l'approche européenne repose davantage sur la certification des équipements que sur la sélection des équipementiers.

Le texte est conforme à cette approche. Il prévoit de créer un nouveau régime d'autorisation administrative qui complétera utilement le dispositif de l'article R. 226-3. Cette autorisation sera fondée explicitement sur la protection des intérêts de sécurité et de défense nationale, et non sur les questions de vie privée. Cela semble plus pertinent pour la 5G, qui permettra notamment le fonctionnement de véhicules autonomes : quand il s'agit de communication entre des automates, on ne peut pas invoquer la protection de la vie privée pour réglementer ces communications.

De façon cohérente avec l'objectif de protection des intérêts de la défense et de la sécurité nationale, le nouveau régime d'autorisation ne concerne que les

opérateurs d'importance vitale, les OIV. Leur liste est classifiée, mais on peut estimer qu'ils sont plusieurs centaines à l'échelle nationale, parmi lesquels les grands opérateurs de téléphonie mobile nationaux ont toutes les chances de figurer.

La procédure de l'article R. 226-3 du code pénal ne concerne que la fiabilité technique des équipements. La procédure supplémentaire que nous allons examiner va beaucoup plus loin, puisqu'elle s'applique également aux logiciels, dont j'ai souligné qu'ils prendraient une place essentielle dans les réseaux de 5G, ainsi qu'aux modalités d'exploitation des réseaux. On entend par là les conditions de recours à la sous-traitance, mais aussi la répartition géographique des équipements par « plaques de réseau ». Il y a à cela deux raisons fondamentales : les enjeux de sécurité peuvent être variables en fonction de la zone géographique et il convient sans doute de prêter une attention particulière à la plaque parisienne qui concentre nombre de centres de décisions ; ce régime d'autorisation « par plaque » permettra par ailleurs aux autorités nationales de veiller à une certaine diversité d'équipements sur le même lieu géographique, de sorte que si une gamme d'équipements était défaillante, la résilience serait assurée sur l'ensemble du territoire.

Le régime de la nouvelle autorisation est calibré de façon à ménager un équilibre entre les impératifs de sécurité des réseaux et le souci de ne pas entraver trop lourdement le déploiement de la 5G, dont notre économie pourra tirer beaucoup d'avantages. C'est un équilibre subtil qu'il s'agit de trouver. Le double regard porté par la commission de la Défense et par la commission des Affaires économiques sera à cet égard utile. Le texte permettra, au cas par cas, de ne pas soumettre à autorisation toutes les mises à jour logicielles. Nous en reparlerons lors de l'examen des amendements.

L'équilibre général du texte me semble satisfaisant. J'ajouterai cependant une remarque, qui tient au périmètre d'application. Le texte concerne les opérateurs de téléphonie mobile. Or, avec la 5G, d'autres industriels seront sans doute tentés de proposer de nouveaux services à leurs clients : il s'agit des opérateurs « verticaux », qui utiliseront la 5G pour leurs besoins propres. Un fabricant de voitures pourrait être amené à déployer son propre réseau 5G pour maîtriser l'ensemble de la chaîne de valeurs. Il faut noter que dans certains pays, comme l'Allemagne, des bandes de fréquences leur sont explicitement réservées. Il me semble que si le risque systémique est moins évident avec ce type d'opérateurs, il n'en reste pas moins important : la chute du réseau d'un fabricant de voitures développant des services utiles à leur utilisation pourrait provoquer la congestion du trafic, voire des accidents. J'estime que ces opérateurs de réseaux privés devraient être soumis aux mêmes règles que les opérateurs de téléphonie mobile, car les enjeux de résilience et de sécurité sont les mêmes.

J'émets un avis favorable à cette proposition de loi. La saisine pour avis de la commission de la Défense a permis de mettre en avant les enjeux de défense à chaque audition et de promouvoir l'esprit de défense, aussi bien auprès de nos

interlocuteurs que de nos collègues siégeant dans d'autres commissions. Nous ne pouvons que nous en féliciter.

M. Joaquim Pueyo. Cette proposition de loi vise à préserver nos intérêts stratégiques face aux évolutions technologiques. Trop souvent, le législateur intervient après que les avancées technologiques ont été mises en place et ont produit leurs premiers effets négatifs. Cette fois, nous savons que l'arrivée de la 5G offrira de grandes opportunités de connectivité ou de rapidité, mais que, du fait de ses caractéristiques intrinsèques, elle comporte aussi des risques, notamment pour nos infrastructures et nos réseaux.

Cette question, du reste, a animé le débat européen, puisque la visite du président chinois a été l'occasion de se poser la question de l'ouverture des marchés européens de la 5G au géant chinois Huawei. La Commission européenne a fait savoir qu'elle n'interdirait pas l'opérateur et ses produits sur le marché européen, mais que les États membres devaient prendre des mesures nationales de protection.

Du fait de l'interdépendance des réseaux et de l'ouverture mondiale sur ces questions, la législation française ne suffira pas si les partenaires européens n'adoptent pas un contrôle de la sécurité des réseaux antérieur au déploiement des équipements de 5G.

Les risques sont trop importants pour que nous ne protégions pas notre pays face aux menaces visant le cyberespace. Celui-ci est déjà un lieu de lutte de faible intensité, où s'imposent des acteurs étatiques et non étatiques. Assurer la protection de nos infrastructures et réseaux de communication est essentiel pour garantir l'indépendance stratégique de notre pays dans un monde globalisé. Je présenterai un amendement pour renforcer la sécurité de nos réseaux. Le groupe Socialistes et apparentés partage l'avis de la commission.

M. Yannick Favennec Becot. Le déploiement du réseau mobile de cinquième génération constitue une innovation de rupture, dans un domaine touchant à la souveraineté et à la sécurité. Sur des questions aussi sensibles que celles relatives à la protection des données, à la sûreté nationale ou à des choix technologiques structurants, il est dommage que le Gouvernement fasse le choix de passer en catimini, d'abord *via* un amendement au projet de loi PACTE, puis par une proposition de loi, projet de loi déguisé qui permet de faire l'économie de l'étude d'impact et de l'avis du Conseil d'État utiles pour éclairer le législateur.

Il semble qu'il faille adopter ce texte dans l'urgence, avant la mise en vente des fréquences qui devrait intervenir au second semestre de 2019. En raison de ce délai très court, les opérateurs mobiles ne semblent pas avoir été consultés lors de la préparation du texte. Leur bonne information, voire leur association, est pourtant indispensable dans la perspective de l'attribution des fréquences de 5G.

Les grands choix en matière numérique ont des implications sécuritaires indéniables, mais les risques potentiels relatifs au déploiement de la 5G, tant du

fait de la nature du réseau que de ses usages, notamment dans le domaine industriel, demeurent mal connus.

Le secteur des réseaux radioélectriques mobiles est marqué par un très petit nombre d'acteurs des télécoms, mais la montée en puissance du tigre Huawei, et ses relations étroites avec l'État chinois, peuvent nous inquiéter.

Sur le fond, obliger les opérateurs préalablement à toute activité à adresser une demande d'autorisation au Premier ministre afin de déterminer s'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale est une garantie nécessaire. Ce texte répond ainsi en partie aux incertitudes sur le développement de la technologie 5G mais il doit être encore enrichi. C'est ce à quoi s'emploiera le groupe Libertés et Territoires lorsque le texte sera débattu en séance publique.

M. Bastien Lachaud. La question des communications est un enjeu décisif de souveraineté dans une société de plus en plus interconnectée, comme l'a montré le rapport que j'ai rendu avec Alexandra Valetta-Ardisson en juillet dernier. L'organisation de notre société repose toujours davantage sur les outils numériques, qu'il faut protéger, notamment contre les risques de cyberespionnage. Or la France, et l'Union européenne de façon générale, est en net retard dans le développement de technologies nouvelles comme la 5G, et ne peut fournir de couverture au pays qu'en passant par des technologies étrangères.

Cette proposition de loi vise à introduire une entorse au sacro-saint principe de concurrence libre et non faussée et de commerce à tout-va ; c'est une bonne chose ! Nous devons aborder les menaces de cyberespionnage sans naïveté et protéger nos intérêts nationaux, que le risque vienne de *hackers* individuels ou de puissances étrangères – quelles qu'elles soient. Passer préalablement par une autorisation avant de mettre en service une telle technologie est une bonne chose, à condition que les mécanismes de contrôle permettent réellement de s'assurer que les outils concernés ne comportent pas de risque majeur pour la protection des données des citoyens français et pour les intérêts nationaux.

Si nous sommes favorables à un mécanisme de contrôle, nous voulons en savoir plus sur les modalités d'autorisation. Cela relève-t-il d'une simple formalité administrative ? Comment l'administration entend-elle contrôler de tels équipements ?

Il faut aborder cette proposition de loi sans naïveté géopolitique. Il n'est pas question d'approuver des dispositions destinées uniquement à soutenir les États-Unis dans leur entreprise d'offensive économique et diplomatique vis-à-vis de la Chine. Il est vrai qu'il convient de se protéger contre des risques d'un cyberespionnage chinois, qui pourrait passer par l'équipement des réseaux mobiles. En 2017, une loi a été votée en Chine, qui prévoit que tout citoyen ou organisation doit coopérer avec les services de renseignement national et maintenir le secret sur une activité de renseignement dont il aurait connaissance.

Mais il n'est pas moins vrai qu'il faut aussi se protéger contre l'espionnage, parfaitement avéré, des services d'écoute américains, révélé au grand public en 2013 par Edward Snowden. Avec l'interception, totalement illégale, de 62 millions de données téléphoniques pour la seule année 2012, les États-Unis sont allés jusqu'à espionner trois présidents de la République française ainsi que les intérêts diplomatiques français à l'ONU et à Washington. Des informations confidentielles ont ainsi été dérobées à la France. Selon les révélations d'un journal allemand en 2017, la NSA est également passée par l'Allemagne, pays supposé allié, pour espionner la France.

Comment en sommes-nous arrivés là ? Il n'y a pas si longtemps, la France avait un géant des télécommunications, Alcatel. Depuis 2012, malgré nos alertes constantes sur les tentatives de pillage industriel de ce fleuron français, rien n'a été fait : Alcatel s'est fait piller ses brevets et a fini par être racheté par Nokia en 2015. Voilà pourquoi la France est en retard ! Nous aurions pu disposer d'une solution française souveraine, en protégeant notre industrie et en développant notre technologie. À cause des dogmes libéraux, nous avons laissé faire le démantèlement. Nous voilà donc réduits à devoir nous protéger contre des technologies étrangères qui pourraient être un vecteur d'espionnage !

Nous avons besoin d'une politique industrielle souveraine. Aussi, cette proposition de loi, même si elle va dans le bon sens, entérine le fait que nous sommes devenus incapables de produire une technologie souveraine. Pourtant, la France est riche de ses savoirs et de ses ingénieurs. Si nous mettons en place une politique industrielle digne de ce nom, nous pourrons concevoir une solution souveraine qui nous mettra à l'abri des technologies étrangères, vecteurs potentiels d'espionnage.

M. Philippe Michel-Kleisbauer. Le groupe Mouvement Démocrate et apparentés s'associe à l'esprit de cette proposition de loi, dont le dispositif législatif est clair : toute technologie, quelle que soit son origine, doit être soumise à un contrôle, l'absence de risque pour la sécurité et la défense nationale étant le seul impératif auquel doivent se plier les dispositifs techniques et ceux qui les mettent en œuvre.

Si certains se sentent visés, dont acte. Ce trouble peut mener certains jusqu'à demander un contrôle d'opportunité technique des parlementaires. Cela doit nous interroger, tout comme la défiance quant à notre volonté de nous protéger.

À ce titre, cette proposition de loi vise à préserver, seulement et pleinement, les intérêts de la défense et la sécurité nationale. Toute connexion constitue une opportunité, mais elle rend aussi vulnérable. Les réseaux mobiles sont un objet économique, un marché, mais ils sont surtout des vecteurs qui touchent à nos intérêts économiques vitaux. Je pense par exemple au système de communication de nos forces de sécurité.

Je salue, au nom de mon groupe, le travail effectué depuis la loi PACTE. Monsieur le rapporteur, pouvez-vous préciser ce que sera le régime du contrôle des mises à jour, qui tiendront une grande place dans la 5G ? Pour ce qui est de l'efficacité du dispositif, existe-t-il une évaluation des effets éventuels des recours qui seraient introduits contre les actes de cette procédure ?

Il ne nous a pas échappé que la loi PACTE visait à mettre en place un dispositif d'évaluation de l'action du Gouvernement en matière de contrôle des investissements étrangers en France. Or la commission de la Défense est exclue de ce dispositif, ce qui est inacceptable. Notre groupe a donc déposé des amendements – devant la commission des Affaires économiques car le délai de dépôt ne permettait pas de le faire devant la commission de la Défense – prévoyant notamment la remise d'un rapport confidentiel au président de la commission de la Défense, par analogie au dispositif prévu à l'article 55 *bis* de la loi PACTE.

M. Claude de Ganay. Je veux saluer, au nom du groupe Les Républicains, le travail de Thomas Gassilloud, qui fait la démonstration, une fois de plus, de sa maîtrise du sujet. Il a évoqué le système Rubis pour la gendarmerie ou encore les voitures autonomes : on voit bien que les enjeux sont considérables.

Sur le plan sécuritaire, la structure des réseaux de 5G se démarque nettement, car le stockage des données est de plus en plus partagé entre les cœurs de réseau et les dispositifs de relais sont accentués. Cette proposition de loi reprend mot pour mot un amendement du Gouvernement au Sénat, rejeté sur la forme. Elle fait partie des velléités européennes tendant à encadrer juridiquement le déploiement de cette technologie et à garantir une forme de souveraineté sur des installations susceptibles de constituer des failles critiques au cœur des systèmes d'information vitaux.

On sent poindre une stratégie anti-Huawei derrière cette initiative, mais nous sommes d'accord aussi bien sur les objectifs que sur l'approche. Nous attendons les débats en séance publique pour nous prononcer, en espérant qu'ils seront l'occasion d'enrichir le texte.

M. Mounir Belhamiti. L'enjeu de l'aménagement numérique du territoire est primordial. Il s'agit de permettre aux citoyens d'accéder à des services indispensables, tant pour leur vie quotidienne que pour l'activité économique. Dans cette perspective, le déploiement de la 5G constitue une opportunité et le préparer au mieux est de la responsabilité des pouvoirs publics. La question de la cybersécurité est centrale : les spécificités techniques de la 5G représentent des risques qu'il s'agit de maîtriser.

L'objectif de cette proposition de loi est de faire évoluer les exigences de sécurité sur les nouveaux équipements qui supportent les réseaux 5G. Il est essentiel de garantir la sécurité et la fiabilité des réseaux, dont certains serviront,

par exemple, au fonctionnement des véhicules connectés. Les investissements étant colossaux, il y va aussi de l'intérêt économique sur le long terme.

Il nous revient de définir un cadre clair qui permette un déploiement rapide et garantisse un niveau optimal de sécurité et de résilience. La question de la fiabilité des équipements de desserte 5G se pose également dans la mesure où la sécurité nationale pourrait être atteinte en cas de faille. C'est la raison pour laquelle le texte prévoit un régime d'autorisation préalable, fondée sur des motifs de défense et de sécurité nationale.

Il est nécessaire aujourd'hui de légiférer. Le déploiement de la 5G a été engagé, et des expérimentations, lancées en 2018, sont en cours. La définition de règles claires et pérennes permettra aux opérateurs de sécuriser en amont leur stratégie de déploiement 5G. Je remercie le groupe La République en Marche de m'avoir confié le rôle de responsable pour ce texte et salue le travail de qualité effectué par le rapporteur, dans des délais contraints. Notre groupe soutiendra cette proposition de loi.

M. Loïc Kervran. Nous avons voté il y a quelques mois, à l'article 34 de la loi de programmation militaire, un dispositif d'autorisations pour l'installation sur les réseaux de ce que l'on a appelé des « marqueurs techniques », en l'occurrence des sortes de sondes. Or, vous l'avez bien montré, Monsieur le rapporteur, avec la 5G, la déconcentration est au centre du processus et la notion même de cœur de réseau change complètement. Je voudrais donc savoir si votre rapport aborde la question de l'impact de la 5G sur les dispositifs tout récents de la loi de programmation militaire, notamment ces sondes ou marqueurs techniques.

M. Laurent Furst. Il n'y a pas de honte à reconnaître qu'il y a des sujets sur lesquels on a du mal à être au niveau. Les questions que je vais vous poser, Monsieur le rapporteur, vous paraîtront donc peut-être élémentaires.

Une réflexion, tout d'abord : on s'aperçoit que, dans le champ technologique et industriel dont nous parlons, la France a disparu au fil des décennies, et que l'Europe existe à peine. C'est là un premier sujet de préoccupation. Par ailleurs, on sent bien que le questionnement tourne autour de la Chine et de Huawei, mais la captation d'informations transitant par les réseaux sous-marins – et ce alors que 93 % des communications internationales passent par eux – ou encore par les satellites – chaque Français en utilise, en moyenne, quarante-six par jour – pose elle aussi question. Or ces aspects ne sont pas abordés dans la proposition de loi.

Je le répète, je ne connais pas beaucoup le sujet, mais je pose quand même la question : se protège-t-on de tout avec ce dispositif, appréhende-t-on l'ensemble du champ concerné par la protection de l'information ? Au demeurant, l'enjeu dépasse largement la protection de l'information ou de la source puisque, ce qui est en cause, c'est la manipulation des systèmes technologiques, la captation ou

l'introduction d'informations erronées et, tout simplement, la capacité à abîmer un système économique ou social.

Enfin, on sent bien que notre opérateur national, Orange, qui est le seul en mesure d'avoir une dimension mondiale, a une appétence particulière pour la marque que nous mettons en cause collectivement aujourd'hui. J'aimerais donc connaître l'analyse que fait le rapporteur pour avis de cette situation.

M. Thibault Bazin. Les sujets que nous abordons sont techniques et complexes. Nous nous apprêtons, afin de préserver nos intérêts en matière de défense – objectif assez largement approuvé –, à donner à l'exécutif un pouvoir discrétionnaire. Je me pose donc la question : comment le Parlement va-t-il participer ? Comment allons-nous évaluer les choix faits par l'exécutif ? Il faut en effet trouver un équilibre entre, d'une part, la préservation des intérêts supérieurs de la Nation, en termes de défense, et, d'autre part, celle de la liberté d'entreprendre, de manière que les opérateurs, notamment nos opérateurs nationaux, conservent de l'agilité, gardent une certaine souveraineté technique en la matière. Je me permets de poser cette question car nous sommes en plein dans le grand débat – dont il serait temps de sortir, d'ailleurs. Il faut redonner la parole au peuple, y compris à ses représentants.

M. Thomas Gassilloud, rapporteur pour avis. Tout d'abord, nous pouvons nous féliciter du fait que tout le monde s'accorde à reconnaître l'intérêt de cette proposition de loi et en approuve la philosophie globale.

Nous sommes effectivement dans un calendrier adéquat – je n'avais pas mentionné cet élément dans mon propos introductif – au regard de celui de l'attribution des fréquences, qui sera effective à la fin de l'année, mais également des grands choix d'investissement que nécessite la 5G. Il faut sécuriser dès à présent le cadre juridique applicable car, une fois que l'on a choisi un équipementier, les coûts liés à des modifications ultérieures sont extrêmement importants, de même que les délais nécessaires pour s'adapter : cela peut prendre plusieurs années.

Bien entendu, je partage ce qui a été dit : nous serions beaucoup plus à l'aise si les *leaders* mondiaux en matière d'équipements électroniques étaient français, ou au moins européens. Il faut évidemment conserver l'ambition d'avoir des *leaders* dans le domaine, en développant des stratégies industrielles et un cadre réglementaire adaptés, ce qui était, entre autres, l'objet de la loi PACTE. Tel n'est pas tout à fait celui du texte que nous examinons. Au-delà des risques intentionnels, nous devons également nous prémunir contre les risques non intentionnels. Telle est bien la philosophie du présent texte et le sens des mesures que nous prenons.

Monsieur Bazin a évoqué le contrôle parlementaire des dispositifs. La saisine pour avis de notre commission a bien pour objet de réintroduire une forme de contrôle parlementaire sur le sujet. En matière de défense et de sécurité, nous

avons effectivement intérêt à trouver le bon équilibre entre ce que fait l'exécutif et ce que fait le Parlement. On pourrait s'étonner, à cet égard, que le Parlement n'ait pas accès – entre autres – à la liste des OIV. Pour ma part, je trouve que le mécanisme est bien conçu. Nous pouvons, chacun à notre niveau, échanger avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), pour savoir quelles sont les modalités d'autorisation des équipements de réseau. Aller plus loin risquerait de poser des problèmes de sécurité nationale.

Monsieur Kervran, la LPM prévoit effectivement la pose de sondes. Le réseau est désormais beaucoup plus décentralisé ; il faut modifier la méthodologie pour l'application des sondes, de manière à s'adapter à cette réalité. Il convient également de rappeler que les sondes opèrent sur des flux non cryptés. Or, dans les années à venir, il y aura de plus en plus de flux cryptés sur les réseaux, ce qui rendra difficile l'utilisation des sondes.

Monsieur Furst, un certain nombre des sujets que vous avez évoqués ont déjà été abordés. Plus globalement, vous posiez la question du périmètre de cette proposition de loi. Il s'agit de faire évoluer la réglementation des réseaux radioélectriques mobiles. Nous nous limitons à ce cadre, mais nous pourrions voir dans ce texte une invitation à étudier plus largement les sujets qui y sont liés, tels que les risques en matière de cybersécurité – dont il a été question –, avec notamment la capacité à prendre en main des systèmes à distance. Je voudrais également appeler votre attention sur les risques d'ingérence dans les processus démocratiques auxquels sont désormais soumis nos pays. Pendant dix ans, on a beaucoup parlé de cybersécurité, mais un nouveau risque est en train d'émerger, lié à la capacité d'entités tierces à s'ingérer dans nos processus démocratiques, notamment en manipulant l'information.

Monsieur Belhamiti, vous avez parlé de l'aménagement numérique du territoire. C'est quelque chose que nous devons bien entendu garder à l'esprit. L'une des craintes que l'on pouvait avoir à l'égard de cette proposition de loi tenait au fait que l'on vient de conclure un *new deal* avec les opérateurs, qui s'est traduit par des engagements importants de leur part concernant le déploiement de nouveaux relais 4G. Le Premier ministre a d'ailleurs fait des annonces il y a une dizaine de jours à ce sujet. Dans ma circonscription, par exemple, un nouveau relais 4G va être installé du fait de cet accord. La liste des 400 premiers – soit, en moyenne, un peu moins d'un par circonscription – a été révélée, me semble-t-il. Il faut effectivement rester attentif à l'exigence d'un aménagement numérique du territoire. Certes, ce n'est pas le rôle principal de la commission de la Défense que de s'intéresser à la question mais, au-delà du service rendu à nos concitoyens, l'aménagement numérique de tout le territoire est aussi important pour le fonctionnement de nos services critiques – il a ainsi été question de la gendarmerie.

Nous aurons l'occasion de reparler du contrôle des mises à jour dans le cadre de la discussion des amendements.

M. Favennec Becot parlait de la brièveté des délais dans lesquels cette proposition de loi a été déposée et examinée. Je partage ce constat, mais justement : on nous reproche parfois un manque de réactivité, mais là, compte tenu du contexte que j'ai indiqué précédemment – notamment l'attribution des fréquences et les plans d'investissement des opérateurs, qui sont en cours d'élaboration –, la rapidité s'imposait. Les opérateurs ont tous été consultés, bien sûr. Nous-mêmes, nous les avons auditionnés : nous avons mené plus d'une douzaine d'auditions, dans des délais extrêmement courts.

Monsieur Lachaud, je salue la qualité du rapport que vous avez rédigé avec Alexandra Valetta Ardisson, qui est tout à fait intéressant et complémentaire à la mission d'information que j'ai moi-même conduite avec Olivier Becht sur les enjeux du numérique pour les armées – vous vous étiez davantage attachés, en ce qui vous concerne, à la cybersécurité. Bien entendu – je l'ai d'ailleurs dit précédemment –, la souveraineté technologique est un enjeu important. Les nouveaux risques qui apparaissent doivent nous encourager à être encore plus dynamiques dans notre stratégie industrielle, afin de protéger ces secteurs. Nous savons bien dans quel monde nous vivons, avec de l'espionnage et des pertes d'informations tous azimuts.

Enfin, Monsieur Pueyo, il est vrai que le législateur est parfois en retard ; mais, en l'espèce, je crois que nous sommes dans le bon tempo : comme je le disais, le contexte est favorable. Au niveau européen, la doctrine est en train d'être stabilisée : nous sommes donc en mesure de faire émerger une approche européenne de la 5G.

La commission en arrive à l'examen des articles de la proposition de loi.

Article 1er

La commission examine l'amendement DN10 de M. Jacques Marilossian.

M. Mounir Belhamiti. L'objectif de cet amendement est d'ajouter le mot « mobiles » au titre de la section que nous créons dans le code : il s'agit des réseaux radioélectriques mobiles. Si cet amendement n'était pas adopté, il faudrait, par cohérence, de supprimer le mot « mobiles » dans le titre de la proposition de loi.

M. Thomas Gassilloud, rapporteur pour avis. Avis défavorable : partout ailleurs dans le code des postes et des télécommunications, on trouve l'expression « réseaux radioélectriques ». Si l'on suivait les auteurs de l'amendement, il conviendrait de modifier l'ensemble des occurrences dans ce code. Cela dit, effectivement, la dénomination « réseaux radioélectriques mobiles » figure dans le titre de la proposition de loi.

M. Mounir Belhamiti. Je retire l'amendement.

L'amendement est ***retiré.***

La commission examine ensuite l'amendement DN11 de M. Jacques Marilossian.

M. Mounir Belhamiti. Il s'agit de mettre le texte en cohérence avec les dispositions de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme, notamment, en parlant non pas des intérêts « de la défense » mais des intérêts « fondamentaux de la Nation ».

M. Thomas Gassilloud, rapporteur pour avis. De la même manière, comme vous le savez, on trouve plusieurs occurrences, dans le code des postes, de l'expression « intérêts de la défense et de la sécurité nationale », qui renvoie à un objet bien identifié, contrairement à celle d'« intérêts fondamentaux de la Nation », beaucoup plus vague. Avis défavorable.

M. Laurent Furst. Le texte se situe dans une logique de défense alors que, fondamentalement, l'enjeu est d'ordre économique. En voici un exemple : un jour, Airbus s'est rendu compte que son principal concurrent avait connaissance de ses propositions commerciales, ce qui montre que l'information avait été interceptée. L'enjeu du combat est peut-être militaire, autour de questions de sécurité, mais il est avant tout, et à court terme, économique. Je souhaite donc savoir, Monsieur le rapporteur pour avis, dans quelle mesure cette question est appréhendée et trouve une juste réponse.

M. le président. Je ne vois pas le rapport avec l'amendement.

M. Laurent Furst. Ah si : les « intérêts fondamentaux de la Nation », c'est de l'économie !

M. le président. Pas seulement.

M. Thibault Bazin. Je comprends l'argument légistique du rapporteur pour avis, mais je pense que la question posée par les auteurs de cet amendement mérite quand même d'être étudiée de plus près d'ici à l'examen du texte en séance : la captation des données est un problème de grande ampleur et il ne s'agit pas seulement d'une question de défense ; il y va de la protection de la Nation tout entière.

M. Thomas Gassilloud, rapporteur pour avis. Ma réponse est effectivement d'ordre juridique ; elle tient à la nécessité de maintenir la cohérence du texte. Bien entendu, je partage la philosophie des auteurs de l'amendement. J'entends bien, Monsieur Furst, qu'il existe une dimension économique, mais le fait d'envisager la question à travers les enjeux de défense nous permet une approche plus largement dérogatoire à ces certains principes de droit économique.

M. Alexis Corbière. Nos collègues ont raison d'ouvrir ce débat : les événements des dernières années nous montrent, notamment à travers le cas des métadonnées révélées par Edward Snowden, que les enjeux d'ordre économique et politique sont extrêmement importants. On l'a vu par exemple à propos d'Alstom,

me glisse mon collègue Bastien Lachaud. Cela dépasse largement la seule question de la sécurité nationale : cela concerne les intérêts économiques et les stratégies économiques et industrielles. Il y a donc sans doute un intérêt à élargir la formulation pour que l'ensemble de ces éléments soient bien pris en compte.

M. Thomas Gassilloud, rapporteur pour avis. Sur le plan de la philosophie, je le répète, la question dépasse bien entendu les enjeux de défense, mais du point de vue du formalisme juridique, ce sont bien ces derniers qui nous donnent une base pour intervenir de la façon souhaitée.

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

Elle est alors saisie de l'amendement DN12 du rapporteur pour avis.

M. Thomas Gassilloud, rapporteur pour avis. Comme je le disais dans mon propos introductif, je propose de supprimer, après les mots « code de la défense », la fin de l'alinéa 4. Il s'agit d'étendre les dispositions du texte aux OIV qui ne sont pas seulement des opérateurs de télécommunications. Même si leur activité ne présente pas pour l'heure de risque systémique, leurs réseaux peuvent subir des atteintes mettant en péril la sécurité nationale.

M. Alexis Corbière. J'approuve ce que vous venez dire, Monsieur le rapporteur pour avis mais, si vous me permettez de vous taquiner, je vous ferai remarquer que vos propos vont dans le sens de ce que nous vous disions à propos de l'amendement précédent.

M. Thomas Gassilloud, rapporteur pour avis. Il s'agit ici des OIV, qui sont classés en tant que tels en raison d'enjeux liés à la sécurité et à la défense s'attachant à leur activité. L'amendement ne vise pas l'ensemble des acteurs économiques susceptibles de déployer des réseaux 5G.

M. Charles de la Verpillière. Pourriez-vous être plus précis, Monsieur le raporteur pour avis ? Le texte continuera à se référer aux opérateurs relevant du code de la défense. Je voudrais que vous nous expliquiez en quoi l'amendement va améliorer le texte.

M. Thomas Gassilloud, rapporteur pour avis. Je propose de supprimer la partie de l'alinéa qui limite la disposition aux seuls OIV qui sont télésignés comme tels au titre de leurs activités d'opérateurs de télécommunications. Modifié comme je le propose, l'article visera l'ensemble des OIV – j'ai donné l'exemple d'un constructeur automobile qui voudrait déployer son réseau 5G, mais on peut également penser aux plateformes aéroportuaires.

M. le président. Ou à la SNCF.

M. Thomas Gassilloud, rapporteur pour avis. Effectivement. Il peut s'agir de services dont l'importance est critique ou de réseaux délivrant par la suite un service au grand public. La SNCF, par exemple, pourrait déployer un

réseau 5G pour ses propres usages puis, quelques années plus tard, sur la base de ce réseau, ouvrir le service à ses usagers pour divers services. Je rappelle que le droit des OIV dépend du code de la défense : d'où le fait que nous visions, dans ce texte, les intérêts de défense.

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

Elle examine ensuite l'amendement DN2 de M. Bastien Lachaud.

M. Bastien Lachaud. Cet amendement vise à élargir le champ de la proposition de loi aux logiciels et aux fournisseurs de logiciels. En effet, les logiciels sont désormais essentiels pour l'ensemble de la technologie, y compris les relais 5G. Me vient à l'esprit l'exemple d'une entreprise américaine qui a été financée par la CIA à sa création et dont les produits sont désormais utilisés par la direction générale de la sécurité intérieure (DGSI) ou encore par Airbus, sans que l'autorité publique effectue des contrôles administratifs. Je considère qu'il est nécessaire de faire entrer les logiciels et les prestataires de logiciels dans le champ de la proposition de loi pour que celle-ci soit pleinement opérationnelle.

M. Thomas Gassilloud, rapporteur pour avis. Je comprends tout à fait l'objectif recherché. Olivier Becht et moi-même, dans notre rapport d'information, avions d'ailleurs soulevé des interrogations, pour ne pas dire émis des critiques, au sujet du choix de la DGSI que vous évoquiez. Au-delà de la question de la compatibilité de votre amendement avec le droit européen des marchés publics, les logiciels, entendus au sens large, n'entrent pas dans le périmètre de cette proposition de loi, laquelle se concentre sur les réseaux radioélectriques mobiles et ne vise que les logiciels nécessaires à ces derniers, dont le choix est soumis à autorisation par le texte. Par ailleurs, je rappelle que, lorsque la sécurité et la défense sont en jeu, des règles dérogatoires au droit commun des marchés publics existent d'ores et déjà. Le choix du logiciel que vous mentionnez aurait donc pu être évité. L'acheteur public n'était pas contraint de faire ce choix. Avis défavorable à votre amendement.

M. Alexis Corbière. La réponse de notre rapporteur met en évidence une faille du dispositif. En effet, si nous prenons la mesure des enjeux mais que nous considérons que les logiciels peuvent très bien être eux-mêmes porteurs de logiciels espions – car c'est de cela que nous parlons –, nous risquons, en définitive, de voter un texte qui soit comme un couteau sans lame dont on aurait aussi perdu le manche. Nous pointons des enjeux fondamentaux, vous considérez vous-mêmes qu'il y a là quelque chose qui laisse la porte ouverte à des problèmes éventuels mais, lorsque notre collègue Bastien Lachaud veut préciser un peu les choses pour que nous ayons dispositif efficace, nous ne votons pas en faveur de son amendement. Je considère que nous gagnerions à adopter cette précision.

M. Laurent Furst. Je ferai une réflexion de profane sur le sujet. Tout à l'heure, j'ai abordé la question des satellites et de la sécurité des câbles sous-marins ; maintenant, il s'agit des logiciels. On voit bien que tous ces problèmes

forment un ensemble. Or la proposition de loi ne traite que d'une partie de la question, qui va se poser pour ainsi dire immédiatement, car le déploiement de la 5G sur le territoire national va se faire de manière extrêmement rapide. Je nous invite donc tous à reprendre, dans le cadre de nos travaux, l'ensemble de la question dans les semaines et les mois à venir.

Mme Natalia Pouzyreff. Monsieur le rapporteur pour avis, pouvez-vous nous préciser ce que contient exactement la proposition de loi en matière de vérification et de contrôle des logiciels afférents aux réseaux de 5G ?

M. Thomas Gassilloud, rapporteur pour avis. Monsieur Lachaud, votre amendement concernerait l'ensemble des appels d'offres publics, y compris par exemple celui d'une mairie souhaitant commander un logiciel de bureautique. Le périmètre paraît donc très large. Je rappelle, une fois encore, que des règles dérogatoires existent déjà en matière de défense et de sécurité. Nous pouvons porter la même appréciation que vous sur le choix fait par certaines entités ; de là à proscrire l'acquisition de logiciels étrangers par l'ensemble des acheteurs publics, il y a un pas qui me semble potentiellement excessif car, parfois, le choix de ces logiciels est pertinent dans un contexte donné. Leur laisser la liberté d'appréciation, sous le contrôle du Parlement, peut être une option tout à fait souhaitable.

Laurent Furst nous appelle à continuer nos efforts en la matière. Bien entendu, je ne peux que partager son avis. Au travers des deux missions d'information que nous avons menées sur la cyberdéfense et le numérique, nous avons déjà engagé des efforts en début de législature. La saisine pour avis de notre commission sur cette proposition de loi permet de les poursuivre, et il y en aura évidemment d'autres dans les mois et les années qui viennent.

Madame Pouzyreff, les logiciels figurent explicitement parmi les éléments contrôlés par l'ANSSI et dont l'installation est subordonnée à l'autorisation du Premier ministre, qu'il s'agisse de leur installation initiale ou de mises à jour. Dès lors qu'ils concourent au fonctionnement du réseau de communication mobile, ils sont bien entendu visés par le texte.

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

Elle examine ensuite l'amendement DN5 de M. Philippe Chalumeau.

M. Philippe Chalumeau. Cet amendement vise à demander un rapport.

M. le président. Vous connaissez mon avis en la matière. *(Sourires.)*

M. Philippe Chalumeau. Nous en avons déjà discuté, effectivement. L'idée était de demander des précisions par l'intermédiaire d'un rapport, mais il y a déjà beaucoup de choses dans le texte : je retire mon amendement.

*L'amendement est **retiré.***

La commission est saisie de l'amendement DN3 de M. Mounir Belhamiti.

M. Mounir Belhamiti. L'objectif de cet amendement est de préciser les procédures applicables aux mises à jour des dispositifs préalablement autorisés, notamment afin de couvrir les cas de modification des logiciels. Il s'avère que des précisions ont été apportées par le rapporteur pour avis sur les modalités de contrôle *a posteriori*. Je retire donc mon amendement.

L'amendement est ***retiré.***

La commission examine l'amendement DN6 de M. Philippe Chalumeau.

M. Philippe Chalumeau. L'idée était, à travers cet amendement, d'engager le débat sur l'utilisation dans le texte de l'adjectif « sérieux », qualifiant la notion de risque. Il s'agit de donner les moyens au Premier ministre de contrôler les matériels qui présentent des risques. Or le fait de qualifier le risque de « sérieux » restreint peut-être trop le périmètre du contrôle, puisqu'il ne s'agirait que de risques déjà avérés. En supprimant l'adjectif, on élargit donc le champ d'action du Premier ministre. Je m'en remets à votre sagacité, mes chers collègues.

M. Thomas Gassilloud, rapporteur pour avis. C'est une lourde responsabilité qui m'est confiée puisque, dans le cadre de ce texte, vous l'avez bien compris, on cherche à trouver un équilibre : il s'agit de préserver la sécurité de la Nation, s'agissant d'un certain nombre d'enjeux, sans pour autant entraver le développement des télécoms, et donc notre économie. En ne fondant pas son action sur un risque « sérieux », on pourrait donner l'impression que l'intervention du Premier ministre est susceptible d'être aléatoire ou arbitraire. En effet, en matière de télécommunications et d'informatique, au sens large, le risque existe en permanence.

M. Philippe Chalumeau. Monsieur le rapporteur pour avis, votre réponse me convient. De toute façon, c'est un sujet dont nous aurons l'occasion de rediscuter. Pour rendre nos débats plus fluides, je retire mon amendement.

L'amendement est ***retiré.***

La commission examine l'amendement DN7 de M. Philippe Chalumeau.

M. Philippe Chalumeau. Il s'agit de substituer une obligation à une simple faculté donnée au Premier ministre de prendre en compte les éléments considérés pour l'élaboration de la décision d'octroi ou de refus d'autorisation. Mais après en avoir discuté en amont avec le rapporteur pour avis, je retire cet amendement tout comme les deux suivants, DN8 et DN9.

Les amendements DN7, DN8 et DN9 sont ***retirés.***

La commission émet un avis ***favorable*** *à l'adoption de l'article 1er* ***modifié.***

Article 2

La commission est saisie de l'amendement DN4 de M. Mounir Belhamiti.

M. Mounir Belhamiti. Cet amendement avait pour objet d'assortir la non-déclaration d'une modification logicielle auprès des services du Premier ministre des mêmes sanctions pénales que celles prévues pour l'exploitation des appareils sans autorisation préalable et pour le manquement à l'exécution des injonctions du Premier ministre, mais la discussion précédente l'a rendu sans objet ; c'est pourquoi je le retire.

L'amendement est ***retiré****.*

M. Charles de la Verpillière. Pourquoi, alors qu'une peine de prison et une peine d'amende sont prévues, la saisie des matériels en cause ne l'est-elle pas ?

M. Thomas Gassilloud, rapporteur pour avis. La saisie des matériels est prévue par un renvoi au code des postes et des communications électroniques, elle n'a donc pas besoin d'être littéralement mentionnée dans ce texte.

La commission émet un avis ***favorable*** *à l'adoption de l'article 2* ***sans modification****.*

Article 3

La commission émet un avis ***favorable*** *à l'adoption de l'article 3* ***sans modification****.*

Enfin, elle émet un avis ***favorable*** *à l'adoption de l'ensemble de la proposition de loi* ***modifiée.***

*
* *

ANNEXE :

LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR POUR AVIS

(Par ordre chronologique)

1. Auditions communes avec M. Éric Bothorel, rapporteur au nom de la commission des Affaires économiques

- **Iliad (Free) – M. Pascal Mayeux**, directeur des obligations légales et **Mme Ombeline Bartin**, responsable des relations institutionnelles ;

- **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 ;

- **CISCO – M. Bruno Bernard**, directeur des affaires publiques pour la France et **M. Jean Charles Griviaud**, chef de la sécurité ;

- **Samsung – M. Yong Chang**, vice-président chargé de la division des clientèles publiques et professionnelles, **M. Daniel Borras**, responsable de la stratégie et des marchés pour l'Europe, **M. Sangwoo Lee**, responsable de la clientèle professionnelle pour la France et **Mme Florence Catel**, directrice des relations publiques pour la France ;

- **Huawei – M. Minggang Zhang**, directeur général adjoint pour la France et **M. Jean-Christophe Aubry**, responsable des affaires publiques ;

- **Nokia – M. Marc Charrière**, directeur des relations institutionnelles ;

- **Agence nationale des fréquences – M. Gilles Brégant**, directeur général ;

➢ **Autorité de régulation des communications électroniques et des postes** – **Mme Cécile Dubarry**, directrice générale et **M. Olivier Delclos**, chef de l'unité « Opérateurs et obligations » ;

➢ **Orange** – **M. Laurentino Lavezzi**, directeur des affaires publiques, **M. Franck Laurent**, coordinateur de la sécurité globale et **M. Pascal Nourry**, expert en matière de sécurité à la direction technique des réseaux et services ;

➢ **Agence nationale de sécurité des systèmes d'information** – **M. l'ingénieur général de l'armement Guillaume Poupard**, directeur général.

2. Auditions du rapporteur pour avis

➢ **Ministère de l'Intérieur** – **M. le général Bruno Poirier-Coutansais**, chef du service des technologies et des systèmes d'information de la sécurité intérieure et **M. le colonel Gonzague Montmorency**, chef du bureau de la prospective radio de la sous-direction des radios ;

➢ **État-major des armées** – **M. le général Jean-Jacques Pellerin**, officier général en charge du numérique auprès du major-général des armées.