N° 579

SÉNAT

SESSION ORDINAIRE DE 2018-2019

Enregistré à la Présidence du Sénat le 19 juin 2019

RAPPORT

FAIT

au nom de la commission des affaires économiques (1) sur la proposition de loi, ADOPTÉE PAR L'ASSEMBLÉE NATIONALE APRÈS ENGAGEMENT DE LA PROCÉDURE ACCÉLÉRÉE, *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 Mme Catherine PROCACCIA,

Sénateur

(1) Cette commission est composée de : Mme Sophie Primas, *présidente ;* Mme Élisabeth Lamure, MM. Daniel Gremillet, Alain Chatillon, Martial Bourquin, Franck Montaugé, Mmes Anne-Catherine Loisier, Noëlle Rauscent, M. Alain Bertrand, Mme Cécile Cukierman, M. Jean-Pierre Decool, *vice-présidents ;* MM. François Calvet, Daniel Laurent, Mmes Catherine Procaccia, Viviane Artigalas, Valérie Létard, *secrétaires ;* M. Serge Babary, Mme Anne-Marie Bertrand, MM. Yves Bouloux, Bernard Buis, Henri Cabanel, Mmes Anne Chain-Larché, Marie-Christine Chauvin, Catherine Conconne, MM. Roland Courteau, Pierre Cuypers, Marc Daunis, Daniel Dubois, Laurent Duplomb, Alain Duran, Mmes Dominique Estrosi Sassone, Françoise Férat, M. Fabien Gay, Mme Annie Guillemot, MM. Xavier Iacovelli, Jean-Marie Janssens, Joël Labbé, Mme Marie-Noëlle Lienemann, MM. Pierre Louault, Michel Magras, Jean-François Mayet, Franck Menonville, Jean-Pierre Moga, Mme Patricia Morhet-Richaud, M. Robert Navarro, Mme Sylviane Noël, MM. Jackie Pierre, Michel Raison, Mmes Évelyne Renaud-Garabedian, Denise Saint-Pé, M. Jean-Claude Tissot.

Voir les numéros :

Assemblée nationale (**15**ème législ.) : **1722**, **1830**, **1832** et T.A. **257**

Sénat : **454**, **569** et **580** (2018-2019)

SOMMAIRE

Pages

LISTE DES PRINCIPALES PROPOSITIONS

Réunie le mercredi 19 juin 2019, sous la présidence de Mme Sophie Primas, la commission des affaires économiques a examiné le rapport de Mme Catherine Procaccia et établi son texte sur la proposition de loi n° 454 (2018-2019) 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, déposée en première lecture sur le Bureau du Sénat le 11 avril 2019 et sur laquelle le Gouvernement a engagé la procédure accélérée.

Lors de cette réunion, la **commission a adopté 19 amendements**, dont 11 du rapporteur en vue de procéder à un rééquilibrage du texte afin que l'exigence de protection des libertés économiques ne soit pas sacrifiée au profit d'une approche excessivement sécuritaire.

Estimant que le **service rendu aux usagers ne saurait être dégradé** du fait d'un refus d'autorisation, elle a ainsi exigé du Premier ministre qu'il **proportionne les effets de ses décisions à leurs impacts potentiels sur les déploiements déjà effectués et sur les futurs déploiements de la 5G, en termes de rythme et de coûts**.

Dans le même esprit, la commission a affirmé la possibilité, pour le Premier ministre, de ne pas se limiter à une démarche binaire – autorisation ou refus – en **autorisant l'exploitation des équipements concernés sous condition**.

Constatant que le flou n'était toujours pas dissipé sur la question de l'« approche géographique » que pourrait retenir le Premier ministre dans son analyse, la commission a également supprimé la mention du périmètre géographique d'exploitation dans le dossier de demande, afin de **s'assurer que l'État ne dicte pas aux opérateurs leur politique d'achat**.

Au-delà, la commission a entendu **apporter un certain nombre de précisions au texte** afin d'en encadrer les effets.

Elle a ainsi affirmé que la **portée du texte se limiterait à la 5G et aux générations ultérieures**, soumis le décret d'application à l'examen du Conseil d'État, ou encore précisé que le niveau de sécurité des équipements concernés devrait être considéré par le Premier ministre dans l'analyse globale de la sécurité des réseaux.

Afin de renforcer le caractère non discriminatoire du texte, elle a adopté un amendement précisant que le Premier ministre devra prendre en considération le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un **État étranger plutôt que d'un État non membre de l'Union européenne**.

Enfin, en vue de **simplifier** l'articulation du dispositif avec le droit en vigueur, la commission a **fusionné deux catégories d'autorisation** pour ne laisser subsister que celle exigée par la proposition de loi.

Mesdames, Messieurs,

Comme toute technologie nouvelle, la 5G est porteuse de promesses. Celles-ci motivent le mouvement planétaire de « course à la 5G ». Mais cette nouvelle technologie apparaît également porteuse de risques, tant du fait de son architecture que des usages critiques qu'elle portera.

C'est pourquoi le Gouvernement entend **renforcer le cadre applicable à la sécurité des réseaux dits « mobiles »** en instaurant un **régime d'autorisation préalable** permettant au Premier ministre de s'assurer du caractère sécurisé de **l'exploitation** des équipements de ces réseaux par les opérateurs de communications électroniques d'importance vitale et, ainsi, de protéger les intérêts de la défense et de la sécurité nationale.

Si le rapporteur **déplore la méthode** adoptée par le Gouvernement dans la conduite des débats parlementaires, en particulier pour un texte d'une telle importance, il **soutient globalement l'esprit** de ce texte, qui fera de la France le premier pays européen à se doter d'un cadre juridique clair et propre à la sécurisation des réseaux 5G.

Cependant, le rapporteur est **particulièrement sensible aux conséquences néfastes** que pourrait avoir une approche excessivement sécuritaire pour notre pays, qui ralentirait le rythme de déploiement de ces futurs réseaux et en en renchérirait le coût, tout en faisant peser un risque sur l'accès des usagers aux réseaux déjà déployés. C'est pourquoi il a proposé à la commission des affaires économiques de **procéder à un certain rééquilibrage du texte**.

C'est donc dans un esprit constructif que le rapporteur a abordé ce texte et suggéré certaines améliorations.

EXPOSÉ GÉNÉRAL

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 enregistrée à la Présidence de l'Assemblée nationale le 20 février 2019 a été transmise au Sénat le 11 avril dernier et renvoyée à la commission des affaires économiques. Elle fait l'objet d'une procédure accélérée.

Composée de trois articles, sa rédaction initiale reprenait, sans modification, le dispositif de l'amendement n° 874[1] déposé par le Gouvernement au Sénat dans le cadre de l'examen en première lecture de ce qui était alors le projet de loi relatif à la croissance et la transformation des entreprises.

Alors qu'une démarche est engagée au niveau européen en vue d'harmoniser la réponse des États membres de l'Union européenne au défi que semble constituer la sécurité des réseaux 5G, cette proposition de loi entend fixer le cadre au niveau français.

I. LA 5G EST-ELLE RISQUÉE ?

A. UNE « COURSE À LA 5G » PORTEUSE DE PROMESSES ET DE RISQUES

1. La 5G promet un changement d'échelle dans les capacités des réseaux, permettant l'émergence de nouveaux usages

La cinquième génération de standards de télécommunications mobiles[2], appelée « 5G », est souvent désignée comme une « rupture technologique », pour plusieurs raisons.

Elle suscitera, d'abord, un **changement d'échelle dans les capacités des réseaux**[3]. Elle promet un accroissement des débits (multipliés par dix), une réduction du temps de latence (divisé par dix), et une plus grande flexibilité des réseaux (permettant de concentrer les flux en fonction des besoins). Elle sera également plus fiable que les précédentes générations, offrira une connexion plus stable en mobilité, et permettra de connecter en

---

[1] *http://www.senat.fr/amendements/2018-2019/255/Amdt_874.html.*

[2] *Après la norme R 2000 pour la 1G, la norme GSM pour la 2G (puis GPRS et EDGE), la norme UMTS pour la 3G (puis HSPA et HSPA +) et, enfin, la norme LTE pour la 4G (puis LTE advanced pour la 4G+).*

[3] *Sur ce sujet, le lecteur pourra utilement se référer aux travaux de l'Office parlementaire d'évaluation des choix scientifiques et techniques, consignés dans un rapport d'information de Pierre Henriet et Gérard Longuet, intitulé « Perspectives technologiques ouvertes par la 5G » publié en décembre 2018.*

temps réel de très nombreux objets. Elle sera, enfin, porteuse d'une plus grande efficacité énergétique.

Comparaison des performances de la 4G et de la 5G

Performances/Génération	4G	5G
1. Débit maximal (Gbit/s)	1	20
2. Débit aperçu par l'utilisateur (Mbit/s)	10	100
3. Efficacité spectrale	1x	3x
4. Vitesse (km/h)	350	500
5. Latence (ms)	10	1
6. Nombre d'objets connectés sur une zone (quantité d'objets/km²)	10^5	10^6
7. Efficacité énergétique du réseau	1x	100x
8. Débit sur une zone (Mbit/s/m²)	0.1	10

Source : Arcep, Les enjeux de la 5G, mars 2017

Elle permettra, ensuite et surtout, le **développement de nouveaux usages tant pour le grand public que pour les entreprises** (généralement rassemblés derrière les termes « industrie du futur » ou « industrie 4.0 »). Même si la plupart de ceux-ci restent à identifier, sont souvent cités le développement de la réalité virtuelle et augmentée, de la vidéo ultra-haute définition, du véhicule connecté, de la télémédecine, de la robotique ou, plus largement, de l'internet des objets. De très nombreux secteurs d'activité seraient donc concernés : les industries lourdes, les transports sur route, les transports ferroviaires, l'énergie, mais aussi les médias ou la santé.

Grâce à ces nouveaux usages, **d'importantes retombées économiques** sont attendues de la 5G, tant pour les opérateurs eux-mêmes que pour les entreprises utilisatrices des réseaux. Selon une étude citée par la Commission européenne dans son plan d'action pour l'Europe en matière de 5G[1], les revenus issus de la 5G pour les seuls opérateurs de ces réseaux pourraient atteindre près de 250 milliards de dollars par an dans le monde en 2025[2]. Il apparaît donc **crucial de faire de la France un marché porteur pour la 5G afin de renforcer la compétitivité de nos opérateurs et des secteurs industriels utilisateurs**.

[1] *Publié le 14 septembre 2016.*
[2] *https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue/.*

Selon l'Arcep[1], ces progrès sont rendus possibles par plusieurs **innovations qui permettent de répartir les capacités selon les besoins** :

– les **antennes actives[2]** – qui autorisent une meilleure efficacité spectrale et énergétique ;

– le « ***network slicing*** » – les réseaux seront configurés en « tranches » pour s'adapter à la demande de façon dynamique ;

– et l'utilisation, à terme, de **bandes hautes** (26 GHz) **sur des petites cellules**, pour des usages localisés avec une grande largeur spectrale et offrant des débits très élevés (théoriquement jusqu'à 10 gigabits par seconde)[3].

La flexibilité qu'apporte le « *network slicing* » est permise par une évolution majeure dans l'architecture des réseaux 5G déjà soulignée par le rapporteur pour avis de l'Assemblée nationale[4] : l'accentuation de la **virtualisation des réseaux**, c'est-à-dire le remplacement d'équipements matériels par des logiciels sur un serveur distant afin de permettre des adaptations rapides du réseau[5].

Il s'agit en somme de **passer d'une architecture passive et orientée sur la connectivité à des réseaux agiles et automatisés, conçus sur-mesure en fonction du besoin**.

Mais ces promesses n'arriveront pas du jour au lendemain : **la 5G se déploiera de façon progressive.** Les premiers équipements spécifiques à la 5G qui seront déployés seront ceux assurant la desserte radioélectrique (« stations de base »[6]), le reste des réseaux s'appuyant sur la technologie 4G existante (« *non stand-alone* » 5G) avant que les « cœurs de réseaux »[7] 5G ne deviennent totalement indépendants des équipements des précédentes générations (« *stand alone* » 5G). Il convient donc de distinguer, comme à chaque nouvelle génération, entre l'appellation 5G « commerciale », qui se

---

[1] Arcep, Les enjeux de la 5G, mars 2017 ; Arcep, programme de travail 5G, juillet 2018.

[2] Jusqu'à la 4G, il n'y avait qu'un seul lobe d'antenne pour tous les terminaux d'une cellule. Dans les réseaux 5G, les lobes des antennes deviennent dynamiques et personnalisés à chaque instant vers chaque terminal de la cellule, on parle de formation de faisceau ou « beamforming » *en anglais.*

[3] Les fréquences supérieures à 6 GHz, appelées « bandes millimétriques », n'ont jusqu'ici jamais été prises en compte pour le déploiement des réseaux mobiles. Ces fréquences ne seront attribuées que dans un second temps : la procédure d'attribution à venir cette année ne concerne que la seule la bande de fréquence des 3,5 GHz.

[4] Rapport pour avis de Thomas Gassilloud, fait au nom de la commission de la défense nationale et des forces armées enregistré à la présidence de l'Assemblée nationale le 2 avril 2019.

[5] Pour une analyse des techniques liées à cette virtualisation, voir les pages 18 et suivantes du rapport précité de l'Arcep de mars 2017.

[6] Selon le glossaire de l'AVICCA, une station de base est un équipement actif de type émetteur/récepteur qui assure la communication entre un appareil mobile et le réseau et qui fournit un point d'entrée dans le réseau aux abonnés présents dans sa cellule pour recevoir ou transmettre des appels, des données. Elle est quasi-systématiquement située sur un point haut dominant la zone qu'elle est destinée à couvrir.

[7] Les équipements du « cœur de réseau » recouvrent notamment les équipements de transmission et de commutation d'un réseau, par opposition aux stations de bases situées en « bord de réseau ».

déploiera dès 2020, et la « véritable » 5G, qui n'apparaîtra pas avant 2021 voire 2022.

La normalisation de la 5G

Une nouvelle génération standardisée de connectivité des terminaux mobiles est définie par deux principaux acteurs : l'Union Internationale des Télécommunications (UIT) et le *3rd Generation Partnership Project* (3GPP).

L'**UIT**, qui est l'agence des Nations unies spécialisée dans les technologies de l'information et de la communication, réalise des études via son « *Working Party 5D* », son sous-groupe en charge de traiter les questions techniques relatives aux radiocommunications. Dès 2013, ce groupe a commencé à travailler sur la définition des caractéristiques d'un nouveau standard IMT (*International Mobile Telecommunications*), le standard IMT-2020. L'objectif de l'UIT-R est d'achever ses analyses pour 2020.

En parallèle des travaux de l'UIT, des études sont menées par le **3GPP**. Le 3GPP a été instauré en 1998 et regroupe sept organismes de standardisation, plusieurs centaines d'industriels, des associations et des organismes publics. Il s'occupe du développement et de la maintenance des spécifications techniques relatives aux normes de téléphonie mobile. Lorsqu'un nouveau standard est en cours de définition à l'UIT, le 3GPP travaille sur les solutions techniques qui permettent de répondre aux objectifs définis par l'UIT.

La « ***release 15*** », première norme 3GPP relative à la 5G, a d'abord été validée en décembre 2017 pour les premiers usages de la 5G dite « *non stand-alone* ». En juin 2018, elle a été complétée pour la 5G dite « *stand alone* ». Cette version devrait être complétée pour d'autres usages par la « ***release 16*** » devrait être publiée début 2020.

2. Les pouvoirs publics européens et français entendent rester dans la « course à la 5G »

En raison de ces promesses, **la course est aujourd'hui lancée**. Le premier **lancement commercial** a eu lieu aux États-Unis en octobre dernier sous l'égide de l'opérateur Verizon avec les équipementiers Nokia, Ericsson et Samsung, pour fournir du très haut débit radio en usage fixe[1]. AT&T a commercialisé ses premiers services en décembre. En Corée du Sud, les opérateurs ont lancé une offre à destination des entreprises en décembre 2018 puis des offres grand public en avril 2019. Selon une étude récente[2], 170 opérateurs répartis dans 54 pays du monde auront lancé la 5G commercialement dès 2020.

S'agissant de **l'attribution des fréquences**, en mai 2019[3], six pays en Europe avaient déjà attribué des fréquences dédiées à la 5G[4]. Douze autres

[1] *Cet usage est donc similaire à celui déjà commercialisé dans le cadre des solutions « 4G fixe ».*
[2] *GSMA Intelligence, «* Global 5G Landscape Q1 2019 *», avril 2019.*
[3] *Source : GSA Research, Spectrum for Terrestrial 5G Networks: Licensing Developments Worldwide », rapport, 14 mai 2019.*
[4] *La Finlande, l'Italie, l'Irlande, la Lituanie, l'Espagne et le Royaume-Uni.*

avaient attribué des fréquences utilisables en 5G[1]. Le processus d'enchères des fréquences 5G vient de se terminer en Allemagne. Treize autres pays d'Europe, dont le nôtre, ont annoncé des enchères 5G entre mi 2019 et fin 2020.

L'Union européenne est particulièrement mobilisée sur ce sujet. Dès septembre 2016, la Commission européenne a publié un **plan d'action pour la 5G en Europe**. Il détermine deux objectifs de couverture communs à l'ensemble des États membres : connecter au moins une grande ville en 5G en **2020** et fournir une couverture 5G ininterrompue dans toutes les zones urbaines et les principaux axes de transport terrestre pour **2025**. Le calendrier d'attribution des « bandes cœur » de la 5G (3,4-3,8 GHz et 24,25-27,5 GHz) est, en outre, coordonné au niveau européen : en application du « code européen des communications électroniques », elles doivent être attribuées avant le 31 décembre 2020[2].

S'agissant de notre pays, l'enjeu est de ne pas commettre les erreurs du passé : la France a débuté le déploiement de la 4G avec trois ans de retard sur les États-Unis et la Corée du Sud. C'est ce précédent et les promesses de la 5G qui ont justifié **l'adoption, en juillet dernier[3], par le Gouvernement, d'une feuille de route** destinée à faciliter le développement et le déploiement de la 5G, coordonnée avec le programme de travail de l'Autorité de régulation des communications électroniques et des postes (Arcep).

Les objectifs et chantiers de la feuille de route du Gouvernement

On peut résumer les objectifs et chantiers de cette feuille de route selon les points suivants :

– lancer plusieurs **pilotes** 5G sur une variété de territoires et accueillir des premières mondiales d'application de la 5G dans les domaines industriels ;

– libérer et **attribuer de nouvelles fréquences** 5G ;

– avoir un **déploiement commercial dans au moins une grande ville dès 2020** et couvrir les **principaux axes de transport** en 5G d'ici **2025** ;

– favoriser le développement de nouveaux **usages industriels** ;

– assurer la **transparence et le dialogue** sur les déploiements de la 5G et l'exposition du public.

[1] L'Albanie, l'Autriche, la Croatie, la République tchèque, le Danemark, l'Allemagne, la Grèce, la Norvège, la Slovaquie, l'Espagne, la Suède et la Suisse.

[2] Article 54 de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte).

[3] Le Gouvernement était en retard sur le calendrier fixé au niveau européen par le plan d'action pour la 5G en Europe qui appelait les États membres à adopter leurs feuilles de route fin 2017 au plus tard.

Le 10 mai dernier, le Gouvernement a adressé au régulateur les objectifs qu'il lui reviendrait de poursuivre dans l'élaboration du cahier des charges pour **l'attribution de la première bande de fréquences** identifiée comme pertinente pour la couverture du territoire métropolitain (3,4-3,8 GHz), dont l'attribution est prévue pour la fin de l'année pour un déploiement dès 2020. Quatre préoccupations devront être prises en compte : tout en reprenant les objectifs figurant dans la feuille de route à échéance 2020 et 2025, le Gouvernement souhaite s'assurer que tous les territoires bénéficient les services de la 5G, il entend également que l'émergence d'offres répondant aux besoins des « verticaux »[1] soit garantie, ainsi que la préservation de la concurrence sur le marché. L'État indique vouloir « *valoriser au mieux ce patrimoine* » et fixera un prix de réserve d'ici l'été. La libération et l'attribution de la bande de fréquence 26 GHz devraient intervenir pour fin 2020.

Le rapporteur se satisfait de constater que la couverture numérique de l'ensemble du territoire est identifiée comme l'une des priorités. Il conviendrait de poursuivre également la logique du « *New Deal* » appliquée au déploiement des réseaux 4G en n'exigeant pas de redevances disproportionnées et en fixant des objectifs ambitieux aux opérateurs.

De nombreuses expérimentations sur la 5G sont déjà en cours sur le territoire métropolitain. Elles ont débuté dès l'année 2018[2].

[1] *Ce terme désigne généralement les entreprises actives dans des secteurs d'activités particuliers, autres que celui des télécoms (comme les trains, les routes ou les réseaux électriques), et qui pourraient souhaiter exploiter leurs propres réseaux.*

[2] *Le communiqué de presse en date du 16 juillet 2018 annonçant la feuille de route du Gouvernement évoquait des expérimentations déjà en cours.*

Carte des expérimentations en 5G en France métropolitaine en mai 2019

Source : site internet de l'Arcep

Dans sa feuille de route pour la 5G, le Gouvernement prévenait cependant que « *les changements technologiques de la 5G, combinés aux menaces cybersécuritaires qui se posent avec acuité, amèneront à rechercher des exigences élevées de niveau de sécurité* ». Cette feuille de route annonçait qu'« *une réflexion sera(it) conduite sur les impacts des nouvelles technologies et l'adaptation de la réglementation qui les encadre, avec la mobilisation de l'Agence nationale de la sécurité des systèmes d'information (Anssi)* ».

3. Elle semble cependant porteuse de risques à ne pas négliger

De façon générale, les réseaux de communications électroniques doivent être autant que possible protégés des risques suivants :

– le risque classique d'**espionnage** ;

– celui de **subversion** des informations traitées ;

– celui du **dysfonctionnement** du réseau, par une interruption du fonctionnement des équipements concernés ou un comportement anormal

perturbant le réseau – de tels dysfonctionnements pourraient résulter d'une panne, mais également s'inscrire dans une logique de sabotage ;

– celui de l'utilisation des équipements du réseau pour procéder à **l'attaque informatique** d'autres équipements numériques : un attaquant ayant pris le contrôle d'un équipement au sein du réseau d'un opérateur pourrait se servir de celui-ci comme relais pour injecter des logiciels malveillants dans les flux transitant par cet équipement, et infecter les systèmes d'information de ses clients.

Plusieurs éléments **liés à l'architecture des réseaux** de la 5G sont généralement présentés comme porteurs de vulnérabilités particulières, qui **accroissent les risques et génèrent une plus grande complexité à les maîtriser**.

Selon le Gouvernement, la **virtualisation** accrue des réseaux les rendra plus vulnérables en créant de **nouveaux risques d'erreur** de configuration. Elle pourrait également **modifier, à terme, la répartition des responsabilités entre les opérateurs** (qui pourraient devenir de simples distributeurs de réseaux) **et les équipementiers** (qui pourraient, dans les faits, être conduits à opérer les réseaux pour le compte des opérateurs[1]). Les opérateurs contestent cette hypothèse.

De façon plus générale, le Gouvernement estime que la 5G pourrait donner lieu à **davantage d'opérations de sous-traitance**. Elle pourrait concerner la définition et la mise en œuvre des choix initiaux de déploiement (prestataires intégrateurs), mais également l'exploitation des équipements (prestataires d'infogérance, voire d'hébergement). Le Gouvernement estime qu'un tel recours à la sous-traitance est porteur de risques, tant du fait de la possible méconnaissance des obligations de sécurité s'imposant aux opérateurs par les prestataires concernés qu'en raison de la potentielle soumission de ces derniers à des formes d'ingérence.

En conséquence, il estime que ces évolutions nécessitent une **approche globale de la cybersécurité de l'ensemble du réseau** alors qu'il suffisait auparavant de s'assurer qu'un équipement utilisé était sécurisé.

Le passage d'une architecture avec un « cœur de réseau » qui constitue le secteur le plus critique à une architecture avec une **vulnérabilité distribuée** participe également à l'apparition de nouveaux risques. Une part importante des fonctions sophistiquées de traitement des flux, jusqu'alors assurées par ces « cœurs de réseau », seront en effet intégrées aux stations de base, augmentant significativement le caractère sensible de ces équipements. Les opérateurs contestent cependant la nouveauté de ce risque, considérant que ces évolutions sont déjà en cours dans le cadre de la 4G et que si la 5G

---

[1] *Selon le Gouvernement, les principaux équipementiers proposent d'ores et déjà des offres d'hébergement et d'opération d'un « cœur de réseau » au profit d'un opérateur – qui visent à ce stade plutôt des opérateurs de petite taille ou très spécialisés, mais pourrait à terme être attractives pour les principaux opérateurs.*

est un élément facilitateur, elle n'en est pas pour autant l'élément déclencheur.

Au-delà de l'architecture des réseaux 5G, c'est également la **criticité de ses nouveaux usages** pour la sécurité des biens et des personnes (objets connectés) ou la continuité de l'action de l'État (réseaux régaliens de la sécurité intérieure ou civile). On imagine l'ampleur des conséquences en cas de panne d'un réseau permettant aux véhicules connectés de circuler en toute sécurité… Le directeur général de l'Anssi, Guillaume Poupard, estime ainsi que « *les réseaux 5G seront aussi sensibles que les réseaux électriques* ». En France, le rapporteur pour avis de l'Assemblée nationale avait également souligné « *l'usage croissant des réseaux civils par les forces armées sur le territoire national* » qui concourent sans nul doute au besoin de renforcement de sécurité de ces réseaux – dans sa contribution écrite, la Fédération française des télécoms semble d'ailleurs estimer que ce point constitue la principale motivation de l'État pour faire adopter la présente proposition de loi. Au-delà, les opérateurs soulignent que les équipements nécessaires à l'émergence d'usage aussi critiques ne seront pas déployés avant 2024-2027.

Au-delà des caractéristiques propres à la 5G, les regards se portent depuis quelques temps sur un équipementier en particulier.

B. HUAWEI EST-IL « L'ÉLÉPHANT DANS LA PIÈCE » ?

Le Gouvernement l'a affirmé à plusieurs reprises et le rapporteur partage pleinement cette analyse : la proposition de loi, d'une part, concerne tous les prestataires des opérateurs et pas Huawei en particulier, d'autre part, ne vise aucunement à interdire Huawei de commercialiser ses équipements auprès des opérateurs. Mais le bruit quasi-assourdissant de ce que l'on pourrait appeler « l'affaire Huawei » oblige à rappeler les principaux termes de ce débat.

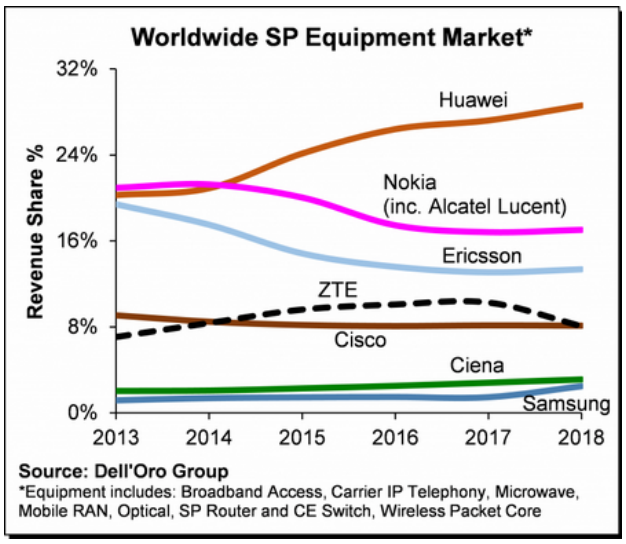
1. Le premier équipementier mondial fait l'objet de critiques tant sur la sécurité de ses équipements que sur un présumé « *dumping* »

a) Huawei est aujourd'hui premier équipementier télécoms mondial

Depuis 2014, Huawei est le premier équipementier dans les télécommunications, dépassant Nokia et Ericsson.

Il détenait, en 2018, 29 % des parts de marché au niveau mondial[1] et cette part de marché augmente rapidement, comme le montre le graphique ci-dessous.

Parts de marché des équipementiers de télécommunications dans le monde
(en %)



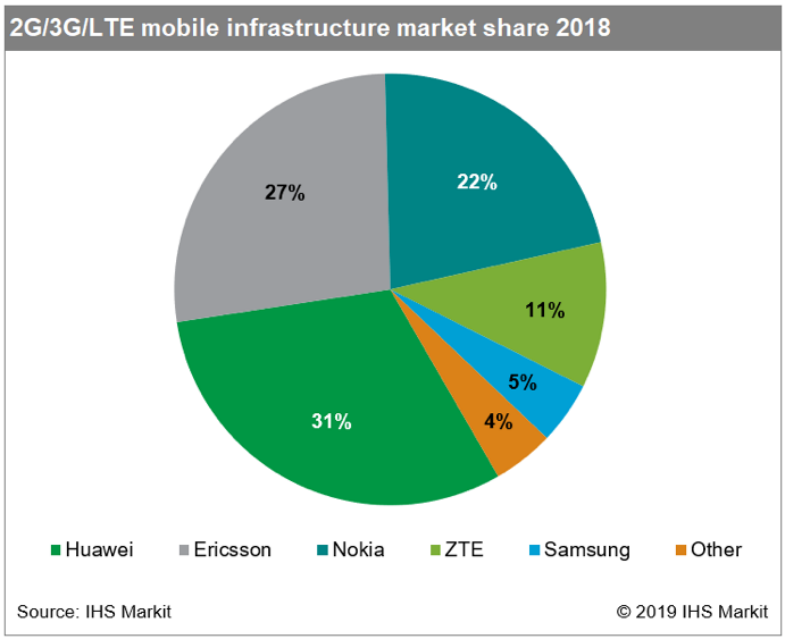
Source : Dell'Oro

De même, Huawei est le **premier équipementier dans les infrastructures de réseaux dits « mobiles »**[2], comme le montre le graphique ci-dessous.

[1] *Cette estimation est effectuée par le cabinet Dell'Oro, l'un des cabinets de référence sur le marché (http://www.delloro.com/delloro-group/telecom-equipment-market-2018). Elle porte sur l'ensemble des équipements télécoms équipant les réseaux. Le marché des terminaux – parmi lesquels les téléphones intelligents – n'est donc pas pris en compte.*

[2] *Le terme « mobile » est ici entre guillemets dans la mesure où la distinction entre réseaux « fixes » et « mobiles » est surtout une distinction effectuée dans le langage commun – en référence aux terminaux mobiles par opposition aux terminaux fixes, mais ne correspond pas aux termes définis par le code des communications électroniques et des postes.*

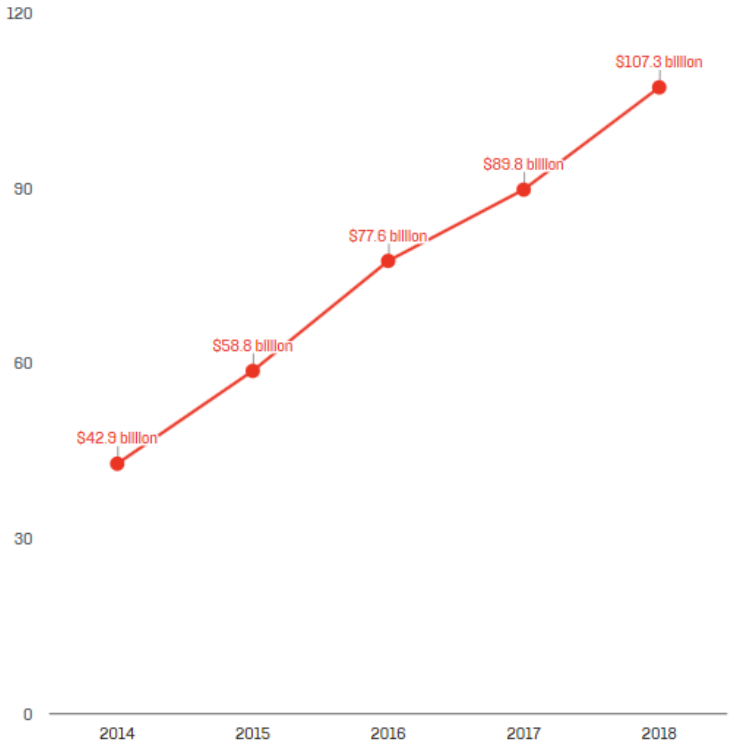
Parts de marchés des équipementiers dans les réseaux « mobiles »



Source : IHS Markit

Le chiffre d'affaires de l'entreprise a cru de façon impressionnante ces dernières années, comme le montre le graphique ci-dessous.

Évolution du chiffre d'affaires de Huawei (en milliards de dollars)



Source : foreignpolicy.com, The Improbable Rise of Huawei, *3 avril 2019, à partir du rapport annuel de Huawei pour l'année 2018 (taux de change du 2 avril 2019)*

Cependant **cette croissance provient principalement du marché à destination des consommateurs** et des terminaux mobiles (+364 % en cinq ans contre +53 % pour l'activité d'équipementier télécoms). L'activité de fournisseur d'équipements télécoms représente 40,8 % du chiffre d'affaires de l'entreprise en 2018[1].

Enfin, le groupe serait le **cinquième plus grand investisseur en recherche et développement du monde**, avec une dépense de plus de 11 milliards d'euros par an (derrière Samsung, qui investirait plus de 13 milliards d'euros par an)[2].

b) Des craintes sont régulièrement exprimées sur la sécurité des équipements commercialisés par la firme

Si l'entreprise Huawei a été mise sous le feu des projecteurs par les autorités américaines, cela fait néanmoins longtemps que de nombreux pays s'interrogent sur les risques de recourir aux équipements produits par les équipementiers chinois.

En France, dès 2012, le rapport de Jean-Marie Bockel sur la cyberdéfense plaidait « *pour une interdiction totale sur le territoire européen des « routeurs de cœur de réseaux » et autres équipements informatiques sensibles d'origine chinoise* »[3]. Une récente publication de l'Institut Montaigne résume l'ensemble des griefs généralement adressés à Huawei[4]. Y est notamment cité le récent rapport du centre d'évaluation mis en place conjointement par l'entreprise et les autorités au Royaume-Uni, qui estime que « *les logiciels déployés par Huawei sont défectueux et comportent de nombreuses failles* »[5].

De fait, aujourd'hui, **aucun équipement Huawei n'est utilisé en France sur les « cœurs de réseaux »**, ce qui est rendu possible par l'application de l'article 226-3 du code pénal, qui soumet les équipements télécoms des « cœurs de réseaux » à une autorisation préalable à la mise sur le marché. La presse s'était d'ailleurs fait l'écho du démontage d'équipements produits par des entreprises chinoises installés dans les « cœurs de réseau » sans autorisation dans certaines collectivités d'outre-mer[6].

La réticence dont peuvent faire preuve certains acteurs à l'encontre des équipements d'origine chinoise est renforcée par une **loi chinoise du 27 juin 2017 sur le renseignement,** qui impose à toute entreprise chinoise de

---

[1] *Source : rapport d'activité de l'entreprise.*

[2] *Source : Commission européenne, EU R&D scoreboard, 2018.*

[3] « La cyberdéfense : un enjeu mondial, une priorité nationale », *Rapport d'information n° 681 (2011-2012) de M. Jean-Marie Bockel, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.*

[4] *Institut Montaigne, L'Europe et la 5G : le cas Huawei, mai 2019.*

[5] *Huawei cybersecurity evaluation centre oversight board: annual report 2019.*

[6] *Les Échos,* « Les États-Unis font à nouveau obstacle à Huawei », *28 mars 2018.*

coopérer avec les autorités dans la collecte de renseignement par tous moyens, y compris techniques, à l'encontre d'entités implantées en Chine et à l'étranger[1].

Le rapporteur rappelle cependant que Huawei n'est pas le seul équipementier sur lequel peuvent peser des soupçons quant à la nature des liens qui l'unissent à un État étranger. Il a été publiquement avéré – contrairement, à ce jour, à Huawei – que les États-Unis ont volontairement implanté des « *portes dérobées* » dans les équipements de l'américain Cisco afin que leurs services de renseignements puissent porter atteinte au secret des correspondances, comme cela a pu être révélé par l'« **affaire Snowden** »[2].

De même, les autorités américaines peuvent s'appuyer sur le ***Cloud Act***[3], qui permet aux forces de l'ordre de contraindre les fournisseurs de services américains à fournir des données stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers.

c) Des accusations régulières de « dumping »

Les accusations de « *dumping* » à l'encontre de Huawei (et de ZTE !) sont récurrentes, en raison :

– des **tarifs** que cet équipementier affiche et qui seraient en moyenne, selon les informations transmises au rapporteur, **18 % inférieurs** à ceux de ses concurrents Ericsson, Nokia et Samsung ;

– du **soutien financier du gouvernement chinois** aux entreprises du secteur des technologies de l'information et de la communication.

---

[1] *C'est ce qui motive d'ailleurs formellement la décision d'interdiction en Australie, voir* infra.

[2] *Voir, sur ce sujet,* « L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne », *rapport d'information n° 696 (2013-2014) de Mme Catherine Morin-Desailly, fait au nom de la MCI sur la gouvernance mondiale de l'Internet, déposé le 8 juillet 2014. Ce rapport rappelait :* « il a également été rapporté, preuves photographiques à l'appui publiées dans la presse, que des agents de la NSA installaient des « Chevaux de Troie » dénommés *beacon* (…) sur les routeurs CISCO à l'insu de l'équipementier et de ses clients », *qui s'était d'ailleurs traduit à l'époque par une baisse des commandes adressées à l'équipementier.*

[3] *Pour* "Clarifying Lawful Overseas Use of Data Act". *Cette loi a été promulguée le 23 mars 2018.*

Si Huawei n'a pas été condamnée pour violation des règles de la concurrence[1], ses rapports annuels montrent que l'équipementier a obtenu, au cours des dix dernières années, 11 milliards de yuans (1,42 milliard d'euros) d'aides publiques, dont plus de la moitié sous forme de dotations directes en raison de la contribution de l'entreprise « *au développement des techniques de pointe* ». Ces fonds publics ont représenté jusqu'à 14 % des bénéfices de Huawei en 2011, une part qui a diminué depuis à mesure de l'explosion des profits du mastodonte. Plus globalement, lors de son discours au deuxième forum sur les nouvelles routes de la soie, le 26 avril 2019, le Président Xi Jinping a d'ailleurs reconnu que les aides publiques octroyées par l'État chinois pouvaient « *fausser la concurrence* », promettant d'y mettre fin.

En somme, c'est sans doute M. Pierre Bellanger qui, dans son ouvrage « *La Souveraineté numérique* », publié en 2014, résumait le mieux les diverses formes d'accusations à l'encontre des fournisseurs chinois de télécommunications. Évoquant « *l'affrontement industriel entre la Chine et l'Occident (…) sur le terrain des équipements de réseau* », il avertissait en ces termes : « *qui contrôle les équipements aujourd'hui peut les mettre hors-service chez l'adversaire en cas de conflit, a accès à l'intégralité des données qui y transitent, notamment la propriété intellectuelle et les secrets militaires et commerciaux, et contrôle les technologies clefs des infrastructures de réseau au cœur de notre mutation numérique. Telle est la stratégie chinoise : dérober la propriété intellectuelle des équipementiers, résultat de décennies d'investissements, proposer ensuite des équipements à prix imbattables, remporter ainsi tous les contrats et mettre en faillite les équipementiers historiques. Enfin, utiliser les positions acquises dans les équipements pour s'emparer du marché des périphériques et des terminaux* ». Il estimait que « *tout contrat aujourd'hui avec un équipementier chinois eut équivalu, au temps de la guerre froide, à développer son programme nucléaire en partenariat avec le KGB, le service secret soviétique d'alors* ».

[1] *En Europe, une plainte a été déposée en 2010 par la société belge Option, spécialisée dans les clés 3G, à l'encontre de Huawei et de ZTE. Cette plainte fut finalement retirée quelque temps plus tard après un accord signé avec les deux entreprises chinoises, impliquant notamment le versement de plusieurs dizaines de millions d'euros à la société belge.*
En 2013, la Commission européenne a mis publiquement en cause nommément Huawei et ZTE pour violation des règles de la concurrence. L'enquête qu'elle avait menée alors lui aurait permis de découvrir des documents faisant état de lignes de crédit à très bon marché équivalentes à 30 milliards de dollars pour Huawei et 25 milliards de dollars pour ZTE de la part de la China Development Bank *(CDB) et de la* China Export-Import (China Eximbank). *Par crainte de représailles (ouverture d'enquêtes en Chine, notamment sur les vins européens), ce conflit ouvert entre l'Union européenne et la Chine se solda par un accord à l'amiable.*

2. Ce qui a amené les États-Unis et certains autres États à établir une interdiction de droit ou de fait aux motivations en réalité multiples

a) Après ZTE, les Américains ont décidé de s'en prendre à Huawei afin, notamment, de renforcer la sécurité de leurs réseaux radioélectriques...

Le débat sur la sécurité des réseaux 5G s'est récemment cristallisé autour des critiques des États-Unis envers l'entreprise Huawei. Comme l'a noté le rapporteur pour avis de l'Assemblée nationale, les États-Unis expriment depuis une dizaine d'années de fortes réticences à voir des équipements de réseaux américains fournis par l'industrie chinoise, craignant pour la confidentialité des correspondances. De fait, **Huawei est déjà absente en tant qu'équipementier dans les réseaux 4G aux États-Unis.**

L'entreprise ZTE, l'autre principal équipementier chinois, **a déjà fait l'objet de plusieurs mesures adverses en provenance des États-Unis ces dernières années**[1]. Condamnée à une amende de 1,2 milliard de dollars pour violation des embargos contre l'Iran et la Corée du Nord en mars 2017, puis mise en cause pour des faits de corruption, elle a été inscrite, le temps d'un trimestre l'année dernière, sur l'« *entity list* », lui interdisant, sauf autorisation, d'acheter des composants électroniques américains. En fin d'année dernière, ZTE a s'attendre à une perte pouvant s'élever à 7,2 milliards de yuans (936 millions d'euros) en 2018.

Les autorités américaines s'en prennent désormais à Huawei. Joignant les actes à la parole, le président Trump a signé le 15 mai dernier un décret (*executive order*) établissant un **cadre juridique propice à l'interdiction**[2] **de recourir à Huawei** pour les réseaux 5G, qui s'ajoute au *National Defense Authorization Act* de 2018, lequel prévoyait déjà d'interdire aux administrations fédérales de se fournir auprès de l'entreprise[3].

Le texte adopté par le Gouvernement américain

Le décret présidentiel interdit l'acquisition ou l'usage des technologies de communication produites par des entités contrôlées par une puissance étrangère hostile (« *a foreign adversary* ») et pouvant :

– générer un risque de « **sabotage** » des technologies et services d'information et de communication aux États-Unis ;

[1] *Pour mémoire, ZTE ne dispose que d'une part de marché très minoritaire en Europe et proche de nulle en France.*

[2] *https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.*

[3] *https://www.reuters.com/article/us-usa-trade-huawei/white-house-seeks-delay-on-huawei-ban-for-contractors-idUSKCN1TA0T1?feedType=RSS&feedName=technologyNews.*

– générer un risque susceptible d'engendrer des « **effets catastrophiques** » sur la sécurité et la résilience des infrastructures critiques ou l'économie numérique des États-Unis ;

– ou fait peser un **risque « inacceptable** » sur la sécurité nationale des États-Unis et des Américains.

Le Département du commerce dispose d'un délai de 150 jours pour établir les règles d'application de ces orientations générales.

Le groupe chinois a officiellement réagi à ce décret en soulignant qu'une interdiction de ses équipements aux États-Unis ne ferait que retarder le déploiement de la 5G dans ce pays et en relevant les difficultés d'ordre juridique posées par ce texte[1]. Huawei a depuis saisi la justice américaine pour contester la constitutionnalité des mesures adoptées par le Gouvernement américain.

b) …mais cette mesure doit cependant s'analyser à la lumière de la guerre commerciale et technologique que se livrent actuellement les États-Unis et la Chine.

Il convient de ne pas omettre le contexte dans lequel s'inscrivent ces mesures.

Ce contexte est d'abord celui des **négociations commerciales féroces** entre la Chine et les États-Unis, pouvant amener les Américains à se ménager un levier de négociation en faisant pression sur une entreprise chinoise considérée comme l'un des géants du numérique.

Il est également celui d'une **course technologique** sans répit entre les deux pays-continents. Comme a pu le relever le chercheur Julien Nocetti, cette offensive se justifie notamment par « *la crainte de Washington de perdre sa supériorité technologique face à Pékin* »[2].

c) D'autres États adoptent une position proche de celle des États-Unis

Selon des modalités différentes, l'Australie[3], la Nouvelle-Zélande[1], Taïwan[2], le Japon[3] et le Canada[4] semblent suivre la même voie que les

[1] *https://www.cnbc.com/2019/05/16/huawei-us-5g-block-after-trump-executive-order.html.*

[2] *Julien Nocetti, chercheur à l'Institut français des relations internationales (Ifri),* « Donald Trump et l'affaire Huawei : un pari hasardeux ? », *Libération, 24 mai 2019.*

[3] *L'Australie s'est appuyée sur la* Telecommunications Sector Security Reforms*, entrée en vigueur en octobre 2018, pour interdire aux opérateurs l'utilisation d'équipements dont le fournisseur est susceptible d'être soumis aux instructions d'un Gouvernement étranger (Source : https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers).*

États-Unis, en visant plus précisément l'activité relative aux équipements de réseau pour des motifs de sécurité. L'État d'Israël est également réputé pour n'utiliser aucun équipement chinois.

Il convient de souligner que la presse a plusieurs fois fait état de **menaces proférées par les États-Unis**, qui réexamineraient leur politique de partage de renseignement envers tout allié qui aurait recours à Huawei[5].

Au début de cette année, le site d'information Bloomberg a effectué un inventaire cartographique des pays susceptibles ou non d'interdire l'utilisation d'équipements Huawei en soulignant le poids économique des pays concernés. S'il ne reflète pas suffisamment les nuances entre les positions des différents pays, il donne cependant une idée de l'ampleur du risque pour l'entreprise Huawei.

---

[1] *En novembre 2018, l'agence de la sécurité des communications (*Government Communications Security Bureau*), qui est en charge de superviser la sécurité des réseaux télécoms depuis le* Telecommunications Interception Capability and Security Act *de 2013, a refusé à l'opérateur Spark la possibilité d'utiliser des équipements Huawei pour son réseau 5G en raison de l'identification d'un risque sérieux pour la sécurité des réseaux (sources : https://www.gcsb.govt.nz/news/gcsb-statement/ et https://www.sparknz.co.nz/news/GCSB_declines_Spark_proposal_Huawei/).*

[2] *En avril dernier, le Gouvernement a interdit aux administrations publiques d'utiliser des équipements provenant de « pays dangereux ».*

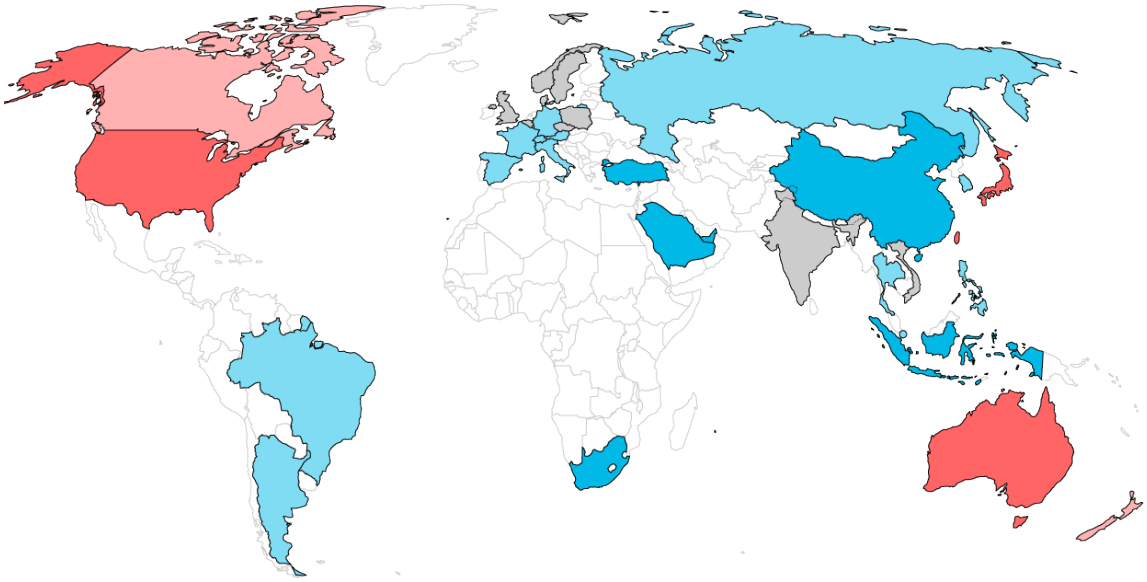
[3] *Le Gouvernement n'a pas pris de décision formelle à ce stade mais la presse a rapporté l'adoption prochaine de nouvelles dispositions visant à interdire l'utilisation de tels équipements par les administrations japonaises. Par ailleurs, les principaux opérateurs japonais ont annoncé fin 2018 ne pas souhaiter s'appuyer sur des fournisseurs chinois pour leurs réseaux 5G, voire avoir engagé un plan de remplacement des équipements Huawei déjà déployés par des alternatives européennes.*

[4] *Le gouvernement n'a pas pris de décision formelle à ce stade mais les opérateurs évitent maintenant le choix de ce fournisseur.*

[5] *Voir, par exemple, s'agissant de l'Allemagne : https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827.*

Positions des différents pays du monde au regard de leur poids dans le produit intérieur brut mondial

Stance on Huawei	Percentage of World GDP
Ban in effect Australia, Japan, Taiwan and U.S.	32.6%
Likely to ban Canada and New Zealand	2.3%
On the fence Belgium, Czech Rep., Denmark, India, Norway, Poland, Sweden, U.K. and Vietnam	9.9%
Unlikely to ban Argentina, Austria, Brazil, France, Germany, Italy, Philippines, Russia, Singapore, South Korea, Spain, Switzerland and Thailand	21.6%
Embracing Huawei China, Indonesia, Saudi Arabia, South Africa, Turkey and UAE	19.8%



Source : Bloomberg.com

Note de lecture : la position de l'Australie, du Japon, de Taïwan et des États-Unis, qui représentaient 32,6 % du produit intérieur brut mondial en 2018, serait d'interdire l'utilisation de Huawei sur leur territoire.

Dans ce contexte, le risque, pour les États européens, est d'être réduit au théâtre d'affrontement entre les deux puissances que sont les États-Unis et la Chine. La position des européens a donc tout intérêt à retenir une approche objective centrée sur la sécurité et s'affranchissant de considérations d'ordre diplomatique.

II. L'UNION EUROPÉENNE ENTEND ÉVITER L'APPARITION D'UN « MAILLON FAIBLE » DANS LA SÉCURITÉ DES RÉSEAUX 5G

A. LES ÉTATS EUROPÉENS SONT EN PHASE DE RÉFLEXION SUR LA SÉCURITÉ DES RÉSEAUX 5G

Le **marché européen est particulièrement stratégique dans l'affrontement** entre les États-Unis et Huawei, dans la mesure où celui-ci

représente, toutes activités confondues, 28,4 % du chiffre d'affaires de Huawei[1].

Un récent rapport rédigé par l'association professionnelle des opérateurs européens[2] dont les conclusions ont été publiées par la presse invite les États européens à ne pas bannir Huawei du déploiement des réseaux 5G. L'association y estime qu'une telle mesure entraînerait un retard de dix-huit mois et un coût supérieur de 55 milliards d'euros dans les déploiements de la 5G si Huawei devait être interdit sur le territoire européen. S'ils sont concernés à des degrés très divers par les équipements chinois[3], **aucun pays européen ne semble, à ce jour, avoir publiquement fait état de velléités de se passer de Huawei**.

Ceci étant, **rares sont ceux qui ont arrêté leur position sur la question plus globale de la sécurité des réseaux 5G**.

Les **autorités allemandes** conduisent actuellement une concertation avec l'industrie. Les éventuelles mesures contraignantes ne devraient pas être adoptées avant l'automne. Le 7 mars dernier, l'autorité allemande de régulation des télécommunications[4] a publié, avec le concours de l'homologue allemand de l'Anssi[5], une **liste de nouvelles exigences de sécurité** qu'elle souhaite rendre applicable aux réseaux 5G. Elle met notamment l'accent sur des **procédures de certification des équipements** de télécommunication. Elle recommande aux opérateurs d'éviter la dépendance exclusive envers un fournisseur unique, et de s'appuyer sur des fournisseurs de confiance. Selon l'Anssi, il existe une divergence d'approche entre l'Allemagne et la France : la première souhaite davantage objectiver le processus, en listant l'ensemble des éléments attendus pour une autorisation, sans marge d'interprétation possible. Ce n'est pas l'approche retenue par le Gouvernement français, qui estime impossible de tout prévoir dans une liste de questions avec des cases à cocher.

De même, le **Royaume-Uni** n'a toujours pas fait officiellement connaître sa position, même si la piste de distinguer entre les infrastructures essentielles, desquelles Huawei serait exclue et les infrastructures non essentielles, pour lesquelles l'entreprise serait admise en tant qu'équipementier, a été évoquée[6]. Les conclusions du gouvernement sont attendues d'ici la fin de l'été. L'approche qui consistait à mettre en place un centre de cybersécurité par les équipementiers est considérée comme

---

[1] *Source : rapport annuel de l'entreprise.*

[2] *GSM association, ou GSMA.*

[3] *Ceux-ci seraient notamment particulièrement présents au Royaume-Uni (selon le rapport précité de l'Institut Montaigne, 70 % de l'infrastructure 4G du pays a été construite par l'équipementier chinois), aux Pays-Bas, en Allemagne, en Pologne ou en Belgique (où ils seraient en situation de monopole).*

[4] Bundesnetzagentur.

[5] Bundesamt für Sicherheit in der Informationstechnik *(BSI).*

[6] *Le ministre de la Défense britannique, Gavin Williamson, a été exclu du Gouvernement britannique le 2 mai dernier, accusé d'avoir fait fuiter cette piste dans la presse.*

défaillante suite à la révélation de vulnérabilités importante des équipements Huawei déjà évoquée.

Monaco a, à l'inverse, décidé de recourir aux services de Huawei pour déployer la 5G sur son territoire. Les opérateurs présents en **Espagne**[1] ont également déjà passé commande auprès de l'équipementier.

B. L'UNION EUROPÉENNE TENTE DE DÉFINIR LES MODALITÉS D'UNE RÉPONSE COORDONNÉE À L'ÉCHELLE DE L'ORGANISATION

Aucune mention relative à des exigences de sécurité particulières n'était inscrite dans le plan pour la 5G publié par la Commission européenne en 2016. Fin mars 2019, la Commission européenne a cependant publié des recommandations spécifiques à la question de la **sécurité des réseaux 5G**[2]. Une approche commune en la matière se justifie par le fait que la sécurité des réseaux nationaux ne peut pas être totalement décorrélée de celle des réseaux des États voisins, dans la mesure où ils sont très largement interconnectés. La maîtrise collective du risque pesant sur les réseaux européens est ainsi le principal objectif du travail en cours, notamment afin d'**éviter que le défaut de sécurisation d'un État ne constitue le « maillon faible »** qui abaissera la sécurité de l'ensemble des réseaux européens[3].

Reconnaissant le fait que la sécurisation des réseaux de télécommunications relève des prérogatives nationales, la Commission recommande à **chaque État membre de procéder à une évaluation** des risques au niveau national avant le **30 juin 2019**. Sur la base de cette évaluation, les États membres sont invités à prendre, le cas échéant, les mesures nécessaires pour garantir la sécurité de la 5G.

La Commission européenne évaluera ensuite les **risques au niveau de l'Union** avec l'Agence de l'Union européenne pour la cybersécurité (ENISA) et **avant le 1er octobre** de cette année au niveau de l'Union européenne. Sur cette base, une « **boîte à outils** » de dispositifs européens susceptibles de faciliter la mise en œuvre de mesures nationales devrait être adoptée d'ici au **31 décembre 2019**.

Il n'est **pas exclu qu'un schéma européen de certification des caractéristiques techniques des équipements 5G soit envisagé à terme**, sur la base des premiers travaux engagés par l'Allemagne, dans le cadre du

---

[1] *Telefonica, Vodafone et Orange.*

[2] *Commission européenne, recommandations,* Cybersecurity of 5G Networks*, 26 mars 2019.*

[3] *Il existe quoi qu'il en soit des moyens de gestion de ce risque par la mise en place de mesures techniques adaptées dans l'interconnexion des réseaux nationaux aux réseaux partenaires.*

« *Cybersecurity Act* » européen[1] qui établit un cadre européen de certification de cybersécurité[2].

III. SI LA SÉCURITÉ DES RÉSEAUX « MOBILES » EN FRANCE APPARAÎT AUJOURD'HUI ASSURÉE, LE GOUVERNEMENT SOUHAITE ADOPTER UN CADRE PROPRE À LA 5G AXÉ SUR LE CONTRÔLE DES MODALITÉS DE DÉPLOIEMENT ET D'EXPLOITATION

A. LA SÉCURITÉ DES RÉSEAUX « MOBILES » APPARAÎT AUJOURD'HUI ASSURÉE DANS NOTRE PAYS

En application du droit en vigueur (voir le commentaire de l'article 1er), **tout opérateur de communications électronique** doit respecter des **obligations concernant la sécurité des réseaux** qu'il exploite. Les **opérateurs d'importance vitale** sont par ailleurs soumis à des règles particulières quant à la **sécurité de leurs systèmes d'information** d'importance vitale. Enfin, un **régime d'autorisation préalable à la mise sur le marché et à la détention de certains équipements** télécoms (actuellement limité aux équipements de « cœur de réseau » et étendu, à compter de 2021, aux « stations de base » situées en « bord de réseau ») établi par l'article 226-3 du code pénal en vue de protéger le secret des correspondances s'applique aussi bien aux équipementiers qui souhaitent commercialiser leurs équipements en France (article R. 226-3 du code pénal) qu'aux opérateurs qui souhaitent les exploiter (article R. 226-7 du même code).

Ces trois régimes font intervenir l'Anssi, bien qu'à des degrés divers. Selon l'Agence, ces dispositifs ont prouvé leur efficacité pour assurer la sécurité des réseaux de télécommunications. En particulier, le régime d'autorisation préalable en vigueur lui a permis d'instaurer une **relation de confiance et de faire émerger une coopération technique intense et constructive tant avec les opérateurs qu'avec les équipementiers**, les négociations techniques menées dans ce cadre amenant souvent à des solutions d'équilibre. Cela se comprend d'ailleurs aisément : il est dans l'intérêt de tous d'avoir des réseaux sûrs et résilients. Pour l'État, cela va de soi, pour les opérateurs, cela renforce la confiance de leurs clients. Du reste, l'Anssi a précisé prendre en compte l'intérêt des opérateurs lorsqu'elle instruit un dossier d'autorisation.

---

[1] *Ce règlement issu de la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité, a été adopté par le Parlement européen le 12 mars 2019 puis par le Conseil de l'Union européenne le 7 juin.*

[2] *Voir, pour un résumé de ce cadre : https://www.ssi.gouv.fr/entreprise/reglementation/cybersecurity-act-2/le-cadre-de-certification-europeen/.*

Ce constat est également celui qu'avait effectué le président de l'Arcep, Sébastien Soriano, lors de son audition du 10 avril dernier devant la commission des affaires économiques : « ***notre pays est mieux préparé et moins exposé que d'autres***. *Le Secrétariat général pour la défense et de la sécurité nationale (SGDSN) et l'Anssi, depuis une dizaine d'années, travaillent très régulièrement avec les opérateurs, les équipementiers des Télécoms et l'Arcep. (…) En tant qu'expert du secteur, je peux néanmoins souligner que sur cette question, la France s'avère moins exposée que d'autres États. (…) Tel est mon message principal sur la sécurité : nous ne partons pas de zéro, puisque les acteurs se connaissent et les procédures sont bien établies*. »

Quels sont les équipementiers présents en France ?

En France, **le marché des équipements déployés sur les « sites » mobiles est réparti entre les trois grands équipementiers de façon relativement équivalente**, comme cela a pu être rappelé par la secrétaire d'État Agnès Pannier-Runacher lors de son audition devant la commission[1]. Si l'équipementier **Cisco** est absent de ce segment de marché, il est, en revanche, avec ses routeurs et interrupteurs, **très présent dans les « cœurs de réseaux » –** ce qui, comme déjà souligné, n'est pas le cas de Huawei.

Tous les opérateurs n'ont, en revanche, pas recours aux mêmes équipementiers. Ainsi, Ericsson est particulièrement présent dans les réseaux de Bouygues et d'Orange, Nokia dans ceux de Free, Orange et SFR, quand Huawei est particulièrement présent chez Bouygues et SFR **–** ce qui rend, en conséquence, ces derniers plus sensibles au risque de « bannissement » de Huawei.

Parts de marché des équipementiers dans les « sites »mobiles détenus en propre par opérateur en France

	Ericsson	Huawei	Nokia
Bouygues Telecom	52,5 %	47,5 %	
Free		0,7 %	99,3 %
Orange	55,6 %		44,4 %
SFR		52 %	48 %

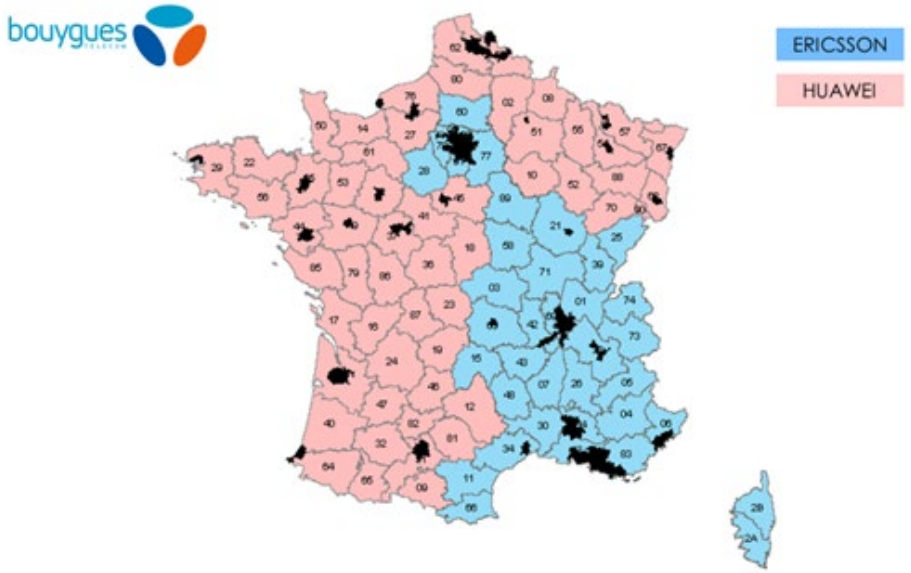
Source : Fédération française des télécoms

Ces équipements sont déployés par la plupart des opérateurs sur **cinq à sept « plaques géographiques »**, dont la délimitation précise varie d'un opérateur à l'autre. Sur chaque plaque, les équipements déployés sont tous du même fournisseur, voire du même modèle. Au niveau national, la plupart des opérateurs ont adopté une logique de **répartition de ces plaques entre deux fournisseurs**.

[1] *Les chiffres transmis au rapporteur par la fédération française des télécoms font cependant état de la répartition suivante, au regard des sites déployés en propre par chaque opérateur : 48 % pour Nokia, 31 % pour Ericsson et 21 % pour Huawei.*

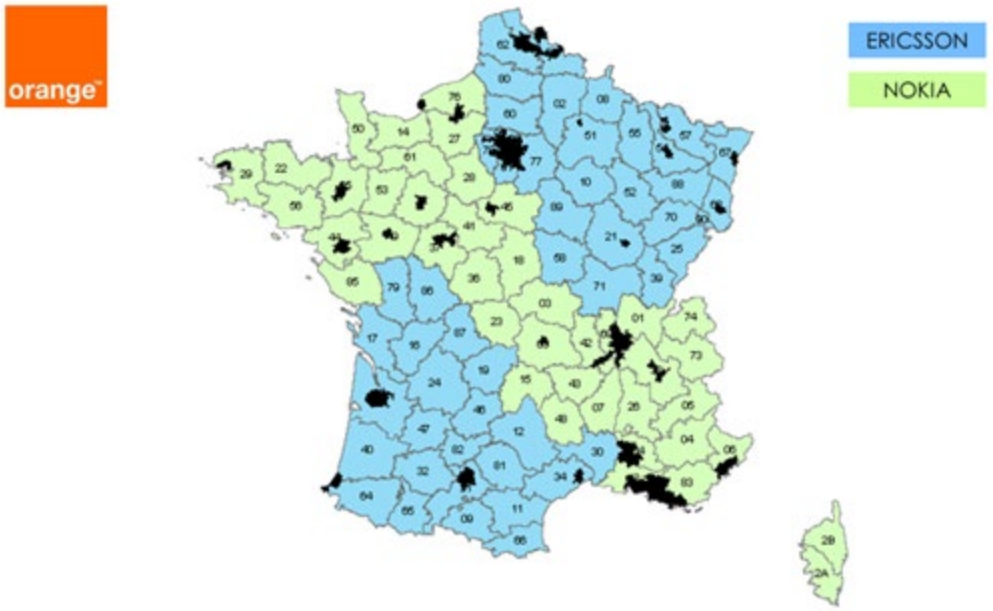
Cette répartition résulte d'une **logique économique** : il s'agit d'assurer un équilibre entre l'économie sur les coûts de déploiement et d'entretien du réseau résultant du choix d'un seul fournisseur (cette uniformité évite par exemple de former les techniciens d'intervention locale à des technologies hétérogènes, et facilite la planification centralisée des opérations de maintenance) et le maintien d'une diversité des fournisseurs permettant d'entretenir une certaine compétition entre ces derniers.

Les cartes ci-dessous montrent la répartition géographique des déploiements sur le territoire de la France métropolitaine par opérateur.

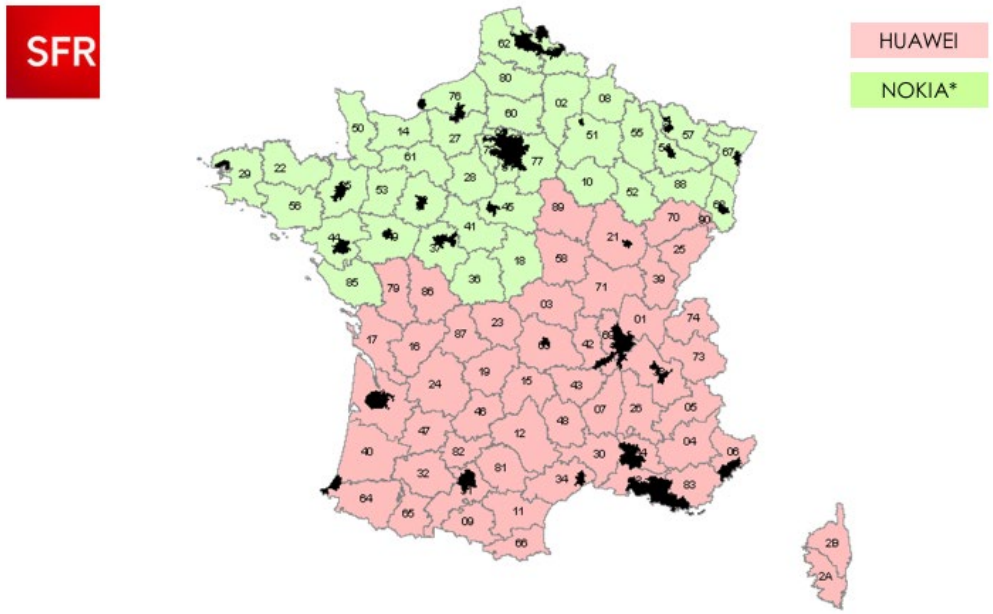


Source : Fédération française des télécoms

Source : Fédération française des télécoms



Source : Fédération française des télécoms



Source : Fédération française des télécoms

Cette situation pourrait évoluer avec l'arrivée de la 5G et les velléités de Samsung de proposer son offre sur le marché européen.

Cependant, il semble que plus un équipementier est présent dans une génération précédente, plus il a de chances d'être également retenu pour la génération ultérieure. Cela s'explique par **l'absence d'interopérabilité** (ou par le coût élevé de gestion de cette interopérabilité) entre les produits des différents équipementiers, qui nécessiterait de remplacer les équipements des précédentes générations déjà en place en cas de changement de fournisseur pour les déploiements en 5G. Il est ainsi moins coûteux de procéder à une simple mise à jour des équipements 2G/3G/4G déjà déployés. Déplorant cet état de fait, la secrétaire d'État auprès du ministre de l'économie et des finances a souligné, lors de son audition par la commission, que le sujet avait été abordé au *Mobile World Congress* de Barcelone, et qu'il appartient aux opérateurs d'exiger de leurs fournisseurs des solutions interopérables[1].

Néanmoins, le fait que les différents opérateurs s'orientent actuellement, en vue du déploiement de la 5G, vers des consultations ouvertes à l'ensemble des fournisseurs tend à démontrer qu'ils n'écartent pas en tout état de cause la possibilité d'un tel changement de fournisseur à l'occasion du déploiement de la 5G.

B. L'ÉTAT SOUHAITE POUVOIR ANALYSER LES MODALITÉS D'EXPLOITATION DES ÉQUIPEMENTS 5G EN VUE DE PRÉSERVER LES INTÉRÊTS DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

1. Un nouveau régime d'autorisation préalable…

La présente proposition de loi établit une **nouvelle autorisation administrative préalable à l'exploitation d'équipements de réseaux « mobiles » dans le but de « *préserver les intérêts de la défense et de la sécurité nationale* »**. Ce nouveau dispositif serait **ciblé sur les opérateurs de communications électroniques d'importance vitale**. Les autorisations seraient délivrées par le Premier ministre, après instruction de l'Anssi.

Si le Gouvernement reconnaît que les réseaux « fixes », de même que les réseaux « mobiles » des générations antérieures, soulèvent leurs propres enjeux de sécurité, il estime que ceux-ci ne sont pas nouveaux et sont déjà pris en compte par le cadre existant de façon efficace, contrairement à ceux soulevés par les réseaux 5G déjà évoqués par le rapporteur.

Il estime ainsi que cette proposition de loi **vient donner un cadre juridique à des pratiques déjà en cours entre l'Agence et les opérateurs**, mais qui reposent aujourd'hui uniquement sur la confiance, ce qui ne peut suffire lorsqu'il s'agit de s'assurer de la protection des intérêts de la défense et de la sécurité nationale.

---

[1] *« L'interopérabilité n'est pas la priorité des départements de recherche et développement des équipementiers, or elle est possible. Il faut être capable, tant en stratégie d'achat qu'en stratégie technologique, de demander des comptes à ses équipementiers. (…) Le sujet a été évoqué à Barcelone. Nous devons pouvoir avancer ».*

2. …en réponse aux lacunes du droit en vigueur

a) La nécessité d'aller au-delà du régime en vigueur pour contrôler les modalités d'exploitation des appareils au regard de la défense et de la sécurité nationale

Pour le Gouvernement, le risque d'atteinte au secret des correspondances provenant de l'intelligence en « bord de réseau »[1] est couvert par le régime de l'article 226-3 du code pénal par le biais de son extension prévue aux stations de base à compter du 1er octobre 2021.

En revanche, le régime d'autorisation en vigueur ne permet pas au Premier ministre de répondre à la virtualisation des réseaux et à la criticité des nouveaux usages.

S'agissant de ces nouveaux usages, ce n'est pas tant le secret des correspondances que la disponibilité des réseaux qui doit être assurée. Il est donc selon lui nécessaire de **fonder un nouveau dispositif d'autorisation sur l'exigence de protection de la sécurité et de la défense nationales**, au-delà du secret des correspondances.

La virtualisation et le fait que l'architecture du réseau dépendra en partie de son usage ont pour conséquence qu'une analyse centrée uniquement sur les caractéristiques techniques propres des équipements, tels qu'ils sont fournis par les équipementiers, ne suffit plus à couvrir l'ensemble des enjeux de sécurité, et qu'une **analyse complémentaire des modalités d'exploitation** (opérations de configuration et de supervision du réseau, recours à la sous-traitance) adoptées par chaque opérateur **devient indispensable**. Le directeur général de l'Anssi estime en effet « *possible de déployer de très mauvais réseaux télécoms en termes de sécurité avec des équipements parfaitement sécurisés. En revanche, une architecture de réseau bien sécurisée permet d'utiliser des équipements d'un niveau de sécurité moins exigeant* ».

Selon le Gouvernement, la **plus grande liberté conférée aux opérateurs dans les choix de déploiement et d'exploitation de leurs équipements rend nécessaire qu'ils jouent un rôle accru dans leur sécurisation**. Le Premier ministre pourra ainsi réaliser un **accompagnement au cas par cas de chaque opérateur et de ses sous-traitants** dans la définition des modalités d'exploitation de leur réseau. Pour le directeur général de l'Anssi, ce dispositif permettrait de s'assurer que les opérateurs restent, sur le long terme, les « maîtres du jeu » sur leurs réseaux.

---

[1] *Cette intelligence du « bord de réseau » par opposition au « cœur de réseau » provient notamment du développement des antennes actives déjà décrit.*

b) L'insuffisant ciblage du dispositif applicable aux « OIV »

Le Gouvernement estime que **les dispositions existantes visant à garantir la cybersécurité des opérateurs[1] d'importance vitale ou « OIV » n'offrent pas la souplesse requise pour répondre à ces nouveaux enjeux**. En effet, la qualification d'un système d'information comme système d'information d'importance vitale (SIIV) est du seul ressort des OIV, et les obligations qui leur sont imposées sont génériques. Par conséquent, ce dispositif ne permet pas la mise en œuvre de mesures techniques précises et propres à une technologie donnée comme la 5G, ni l'appréciation au cas par cas des facteurs de risques que la proposition de loi apporte, et qui semble justifiée au regard de la nouveauté et de la forte évolutivité des technologies 5G.

IV. LA POSITION DE LA COMMISSION : AMÉLIORER UNE PROPOSITION DE LOI RÉDIGÉE DANS LA PRÉCIPITATION

Constatant l'importance du dispositif pour le Gouvernement, et partageant sa préoccupation de s'assurer de la sécurité des réseaux 5G, le rapporteur a entendu adopter une approche constructive dont l'axe principal est l'idée de proportionnalité. Il n'en reste pas moins que le Gouvernement a fait preuve d'une précipitation qu'il conviendrait de ne pas réitérer.

A. UNE PRÉCIPITATION DÉNOTANT UN CERTAIN MANQUE DE MÉTHODE DE LA PART DU GOUVERNEMENT

Comme déjà évoqué, les réflexions entamées par le Gouvernement dans le cadre de sa feuille de route sur la 5G ont abouti au début de cette année dans une certaine précipitation.

Le Gouvernement a en effet été amené à déposer **un amendement en première lecture au Sénat dans le cadre du projet de loi relatif à la croissance et la transformation des entreprises – dit « PACTE »**, fin janvier. L'Arcep avait dû rédiger un avis en urgence sur ce projet d'amendement – avis qui n'a été publié qu'en avril. Estimant nécessaire de disposer de davantage de temps pour trancher sur un sujet aussi important, le Sénat avait rejeté l'amendement.

Renonçant à ce « cavalier » législatif, le Gouvernement a donc transformé cet amendement en texte de loi sans pour autant en faire un projet de loi. Il a ainsi choisi de le faire déposer sous forme de proposition de loi par le groupe La République en Marche de l'Assemblée nationale.

---

[1] *Le terme est ici générique et ne désigne pas, contrairement au reste du présent rapport, les opérateurs de communications électroniques.*

Cette précipitation se traduit non seulement par la présence d'**erreurs dans l'exposé des motifs** (qui cite, par exemple, une entrée en vigueur à compter du 1er janvier alors que le texte dispositif cite le 1er février…), mais a également pour conséquence de **priver le Parlement de l'étude d'impact et de l'avis du Conseil d'État qui accompagnent tout projet de loi**. Sur un sujet pourtant capital, cette absence est regrettable.

De fait, aucun des organismes auditionnés n'a été en mesure de fournir une évaluation précise des impacts de cette proposition de loi sur les réseaux déjà déployés et à venir.

Les auditions menées par le rapporteur ont néanmoins permis de dissiper certaines craintes et ont souligné la nécessité d'un rééquilibrage du texte en faveur des libertés économiques.

B. S'IL CONVIENT A PRIORI *DE DISSIPER CERTAINES CRAINTES…*

1. La proposition de loi ne vise pas à interdire Huawei, et ne devrait donc pas avoir d'impact sur les approvisionnements des opérateurs

D'après les informations recueillies, le Gouvernement entend, par ce texte, adopter une approche équilibrée et visant à répondre à toutes les potentielles vulnérabilités liées au déploiement de la 5G, quelle qu'en soit la source. Ainsi, la proposition de loi, d'une part, ne vise pas à interdire Huawei, d'autre part, ne concerne pas que Huawei : les modalités d'exploitation des équipements seraient vérifiées pour la totalité de la chaîne du réseau, **quel que soit le prestataire des opérateurs** – équipementier ou autre. Le Gouvernement souligne, par ailleurs, que cette initiative est **indépendante du contexte international**.

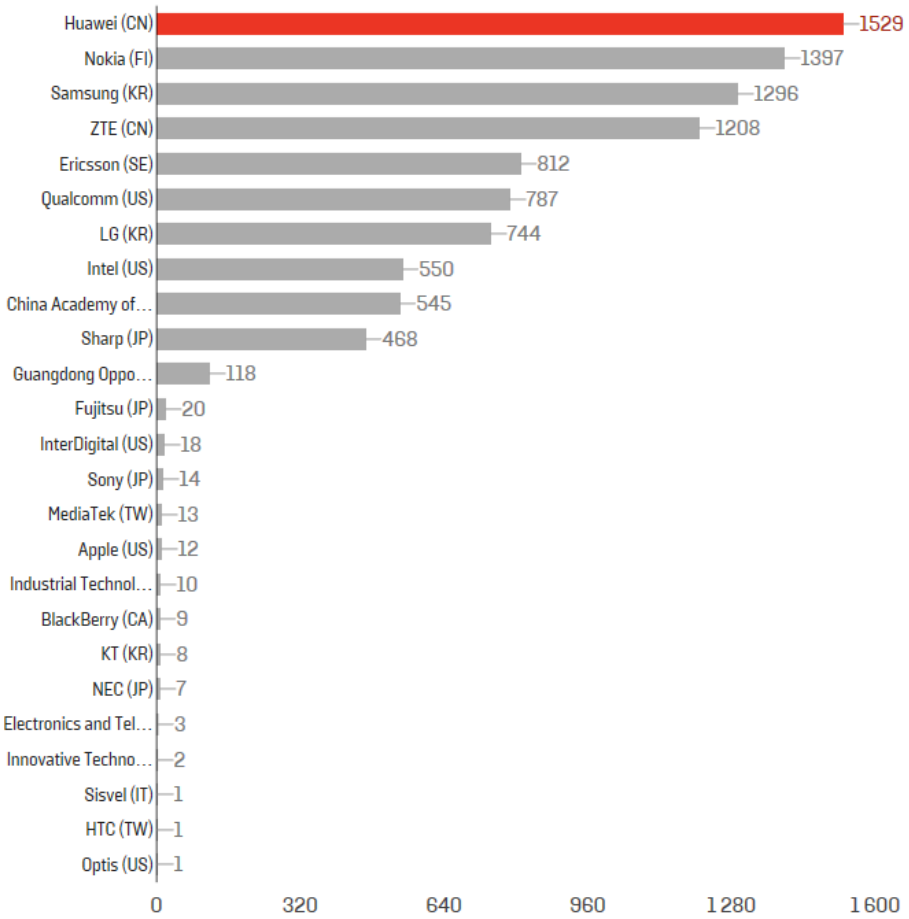
En conséquence, **deux craintes apparues dans les débats**, à savoir un risque de rupture d'approvisionnement et un risque tenant au manque de compétitivité des opérateurs dans les cas où ils ne pourraient pas recourir aux équipements de Huawei, **devraient pouvoir être dissipées**. Ces craintes paraissent, par ailleurs, en elles-mêmes peu fondées.

Premièrement, les opérateurs **craignent que le nouveau régime d'autorisation ne les oblige à se priver de l'un de leurs fournisseurs**, les exposant à une hausse des prix ou à une potentielle rupture d'approvisionnement. Pour ceux ayant recours à Huawei, une interdiction de fait de ce dernier pourrait les contraindre à retirer leurs équipements déjà installés, les obligeant à engager des coûts particulièrement importants – dont le montant n'est cependant pas évaluable car ce type de données est couvert par le secret des affaires.

Il peut être remarqué que, quand bien même le Gouvernement choisirait d'interdire un équipementier, le marché français ne représente qu'une petite partie de la production industrielle des trois grands équipementiers. Un tel risque serait donc *a priori* plutôt théorique – du reste, comme déjà évoqué, il semble que Samsung souhaite faire son entrée sur le marché européen, ce qui serait de nature à animer sa dynamique concurrentielle. Enfin, à moyen terme, le risque de rupture d'approvisionnement matériel va décroître avec la 5G du fait de la virtualisation.

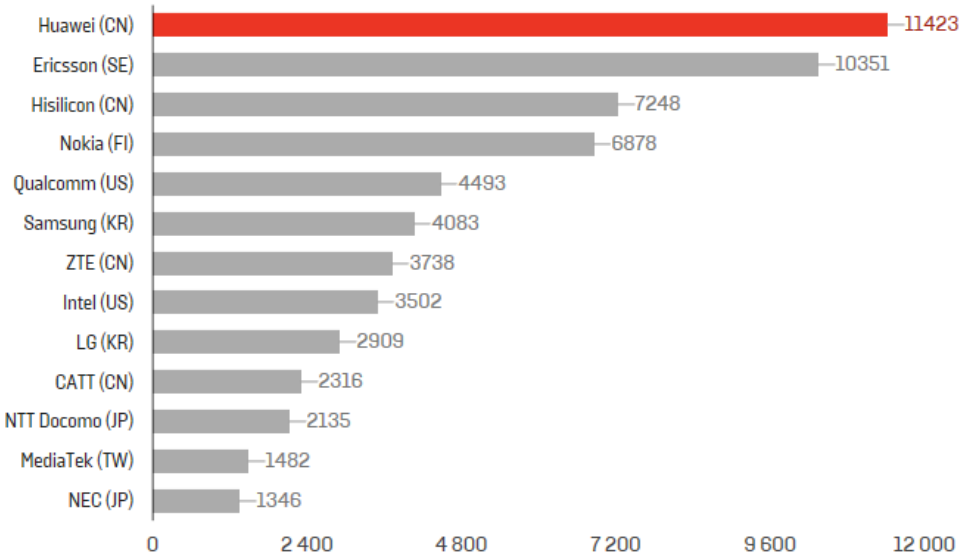
Deuxièmement, **selon certains, les équipements du chinois Huawei en matière de 5G seraient plus performants que ceux de ses concurrents européens**. Plusieurs indicateurs sont généralement cités pour démontrer l'investissement de l'entreprise sur cette génération de télécommunications : elle est aussi bien la première détentrice de brevets que la première contributrice à l'élaboration des normes techniques internationales. Elle réalise par ailleurs de nombreuses expérimentations 5G à grande échelle en Chine.

Détenteurs de brevets essentiels à la 5G



Source : foreignpolicy.com, The Improbable Rise of Huawei, 3 avril 2019, d'après les données disponibles sur le site IPlytics

Principales entreprises contribuant à la définition des normes 5G



Source : foreignpolicy.com, The Improbable Rise of Huawei, 3 avril 2019, d'après les données disponibles sur le site IPlytics

On peut cependant constater, à la lecture de ces graphiques, que :

– les concurrents européens (Nokia, Ericsson) et Samsung sont également en très bonne position sur ces deux indicateurs ;

– du reste, ces trois équipementiers sont également en très bonne position sur les expérimentations et autres lancements commerciaux déjà effectués à travers le monde.

Lors de leur audition par le rapporteur, ceux-ci ont d'ailleurs réaffirmé leur **souhait de ne pas être protégés par une quelconque barrière réglementaire excluant l'un des acteurs du marché**.

Par ailleurs, si le groupe Nokia a admis que son groupe devrait rattraper un retard « *de quelques semaines à deux mois* » sur la 5G[1], il a pu être précisé au rapporteur que **l'avance de tel ou tel acteur du marché sur telle ou telle fonction technique reste en pratique marginale** par rapport aux autres facteurs figurant sur le chemin critique de l'adoption de la 5G, tels que la disponibilité des terminaux ou l'adoption des usages. Au demeurant, les travaux de normalisation de la 5G ne seront pas finalisés avant fin 2019. Tous les déploiements effectués avant cette date devront donc être remis à niveau[2].

[1] *https://fr.reuters.com/article/technologyNews/idFRKCN1SR1LE-OFRIN.*

[2] *Pour une analyse concordante relativisant l'avance technologique de Huawei, voir : https://www.spglobal.com/en/research-insights/articles/bans-on-huawei-will-hit-tech-harder-than-telecom.*

2. L'Anssi estime avoir les moyens de traiter les demandes dans les temps

Le Gouvernement a réaffirmé à plusieurs occasions au cours des débats que l'Anssi aurait les moyens de traiter les nouvelles demandes d'autorisation dans les temps.

Selon les réponses qu'il a apportées au rapporteur, « *le traitement des nouvelles demandes (d'autorisation) nécessitera un* ***renfort de deux personnels dédiés au traitement administratif*** » des demandes au sein du bureau des contrôles réglementaires. Leur analyse technique devrait pouvoir être assurée sans requérir de moyens supplémentaires spécifiques, compte tenu du renforcement déjà prévu des compétences techniques de l'Anssi dans le domaine de la 5G.

L'Anssi s'attend à une volumétrie du même ordre de grandeur que celui actuellement observé dans le cadre du régime d'autorisation des équipements en vigueur, soit **au plus un millier de demandes annuelles**. Elle estime que cette volumétrie sera probablement plus faible au cours des premières années de mise en œuvre du dispositif, dans la mesure où les premiers déploiements de la 5G relèveront de la version dite « *non-standalone* » de cette technologie.

C. ... IL EST APPARU NÉCESSAIRE DE PROCÉDER À UN CERTAIN RÉÉQUILIBRAGE DU TEXTE

Le rapporteur et la commission sont **favorables à l'idée de rehausser le niveau de contrôle de la sécurité des réseaux de télécommunications « mobiles »** pour faire face aux nouvelles vulnérabilités identifiées dans la 5G et ainsi mieux protéger les « *intérêts de la défense et de la sécurité nationale* ».

Avec ce texte, la France sera le **premier pays européen à se doter d'un cadre juridique clair et propre à la sécurisation des réseaux 5G**, alors que la question se pose dans l'ensemble des pays du monde.

Le choix d'un dispositif d'autorisation préalable apparaît pertinent dans la mesure où il **permettra aux opérateurs d'effectuer leurs investissements de façon éclairée** et évitera une remise en cause *a posteriori* des installations.

Afin que les opérateurs ne ratent pas le virage de la 5G, le rapporteur estime ainsi nécessaire de déterminer rapidement un cadre juridique clair à l'établissement de ces réseaux. Il accueille donc favorablement le fait que le Gouvernement travaille sur les textes réglementaires « en temps masqué », c'est-à-dire en même temps que les travaux législatifs : les projets de décret et d'arrêté d'application ont

d'ailleurs fait l'objet de plusieurs échanges avec les opérateurs et ont été transmis au rapporteur. L'objectif du Gouvernement est que, dès la promulgation de la proposition de loi, les textes d'application puissent être transmis aux organismes à consulter.

Cependant, un tel régime d'autorisation **porte**, en soi, **atteinte aux libertés économiques** (liberté d'entreprendre, liberté contractuelle). Toute atteinte à ces libertés doit être, selon la jurisprudence du Conseil constitutionnel, liée à des exigences constitutionnelles ou justifiée par l'intérêt général, et proportionnée au regard de l'objectif poursuivi – en l'espèce, la protection des intérêts de la défense et de la sécurité nationale.

Dans cet objectif, au regard du dispositif proposé et après avoir entendu toutes les parties prenantes, le rapporteur, suivi par la commission, a souhaité :

– trouver un juste équilibre entre les impératifs de sécurité et les besoins des entreprises et des usagers de la 5G ;

– simplifier son articulation avec le droit en vigueur ;

– en préciser la portée et le contenu.

1. Les propositions de la commission

a) Rééquilibrer

La commission a ainsi exigé du Premier ministre qu'il **proportionne les effets de ses décisions à leurs impacts potentiels sur les déploiements déjà effectués et sur les futurs déploiements de la 5G, en termes de rythme et de coûts**. Le **service rendu aux usagers ne saurait être dégradé** du fait d'un refus d'autorisation, sauf si des circonstances particulièrement graves devaient le justifier.

Dans le même esprit, elle a affirmé la possibilité, pour le Premier ministre, de ne pas se limiter à « oui » ou « non », en **autorisant l'exploitation des équipements concernés sous condition** – autrement dit, il pourra également dire « oui, mais ».

Constatant que le flou n'était toujours pas dissipé sur la question de l'« approche géographique » que pourrait retenir l'Anssi dans son analyse, la commission a également supprimé la mention du périmètre géographique d'exploitation dans le dossier de demande. Il s'agit de **s'assurer que l'État ne dicte pas aux opérateurs leur politique d'achat**.

b) Préciser

La commission a entendu **apporter un certain nombre de précisions au texte** afin d'en encadrer la portée et le contenu.

Elle a ainsi affirmé que la **portée du texte se limiterait à la 5G et aux générations ultérieures**, soumis le décret d'application à l'examen du Conseil d'État, ou encore précisé – même si cela reste subsidiaire – que le niveau de sécurité des équipements concernés devrait être considéré par le Premier ministre dans l'analyse globale de la sécurité des réseaux.

Enfin, afin de renforcer le caractère non discriminatoire du texte, elle a adopté un amendement précisant que le Premier ministre devra prendre en considération le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un **État étranger plutôt que d'un État non membre de l'Union européenne**.

c) Simplifier

Afin d'éviter que les opérateurs concernés par la présente proposition de loi ne se trouvent confrontés à deux dispositifs d'autorisation se chevauchant – l'une au titre de la détention d'un équipement concerné par l'autorisation prévue par le code pénal, l'autre au titre de l'exploitation d'un équipement concerné par la proposition de loi – la commission a adopté un amendement fusionnant les deux demandes d'autorisation en supprimant la nécessité de déposer une demande au titre du code pénal lorsque l'équipement est également couvert par la proposition de loi. Cette **mesure de simplification permet donc de passer de deux autorisations à une seule.**

2. L'extension aux « verticaux » ne semble pas nécessaire à ce jour

La question ayant été fortement débattue à l'Assemblée nationale, à tel point qu'une seconde délibération a dû être effectuée, le rapporteur s'est interrogé sur le point de savoir s'il n'était pas nécessaire d'inclure dans le champ du texte l'exploitation d'équipements dans le cadre de réseaux propres à certains « verticaux ». Il est en effet souvent estimé que, avec la 5G, les « verticaux » pourraient souhaiter déployer leurs propres réseaux pour leurs besoins ou au profit de tiers.

Ayant auditionné quelques-uns de ces verticaux, le rapporteur rejoint l'analyse du Gouvernement : **à ce stade, il ne semble pas justifié de soumettre ces opérateurs verticaux aux mêmes obligations que les opérateurs de télécommunications concernés par la proposition de loi**.

En effet, l'impact des potentielles vulnérabilités des réseaux qu'ils pourraient déployer n'est pas équivalent à celui des opérateurs de

communications électroniques d'importance vitale, de sorte qu'il n'est pas établi que cet impact serait un enjeu de sécurité nationale. En conséquence, il semble davantage proportionné de considérer que, pour ceux des « verticaux » qui seraient d'importance vitale, les mesures qui leur sont imposées en matière de sécurisation de leurs systèmes d'information apparaissent suffisantes.

Il convient cependant de noter que, si des « verticaux » d'importance vitale venaient à ouvrir leurs réseaux au public, ils entreraient *de facto* dans le champ d'application du dispositif de la proposition de loi. La commission a d'ailleurs adopté un amendement assurant une meilleure disponibilité du dispositif sur ce point : dès lors qu'un équipement serait mutualisé pour l'utilisation d'un réseau propre et d'un réseau ouvert au public, le dispositif de la proposition de loi serait bien applicable.

EXAMEN DES ARTICLES

Article 1er
(chapitre II du titre Ier du livre II du code des postes et des communications électroniques)

Autorisation préalable à l'exploitation des équipements de réseaux radioélectriques et pouvoir d'injonction

Objet : cet article soumet à autorisation préalable, en vue de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des équipements des réseaux « mobiles » qui, par leurs fonctions, présentent un risque pour la sécurité des réseaux. Ce régime ne concernerait que les opérateurs de communications électroniques d'importance vitale dans le cadre de l'exploitation d'un réseau ouvert au public. Cet article détermine également les conditions d'octroi ou de refus de l'autorisation par le Premier ministre et confie à celui-ci un pouvoir d'injonction.

I. Le droit en vigueur : la sécurité des réseaux « mobiles » est aujourd'hui assurée grâce à différents outils mobilisant l'Agence nationale de la sécurité des systèmes d'information.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) est au cœur des trois principaux dispositifs concernant la sécurité des réseaux actuellement en vigueur. Les deux premiers mettent des obligations particulières à la charge des opérateurs. Le troisième est centré sur la sécurité des équipements et concerne aussi bien les équipementiers que les opérateurs.

L'Agence nationale de la sécurité des systèmes d'information

Créée il y a moins de dix ans[1], l'Anssi est un service à compétence nationale rattaché (sans personnalité morale) au Secrétariat général de la défense et de la sécurité nationale, lui-même rattaché au Premier ministre, qu'il assiste dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Chargée de mettre en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information, les missions de l'Agence s'organisent autour de deux pôles : « sensibilisation et prévention », destiné à informer les acteurs publics des menaces présentes dans le cyberespace et des moyens de s'en protéger ; « réaction aux attaques », dans lequel le centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la réponse de l'État en termes de défense.

[1] *Décret n° 2009-834 du 7 juillet 2009.*

En raison de l'importance de ses missions dans un monde toujours plus connecté, l'Agence bénéficie d'une croissance non négligeable de ses effectifs, passés de 122 équivalents temps pleins en 2009 à 568 agents en 2018.

Les opérateurs de communications électroniques ont aujourd'hui des relations régulières avec l'Anssi en raison des trois principaux dispositifs qui permettent, aujourd'hui, de s'assurer de la sécurité de nos réseaux. Au-delà, ils se fréquentent également dans le cadre de l'article 34 de la loi de programmation militaire[1], qui prévoit des dispositions relatives au renforcement des capacités de détection des attaques informatiques.

A. Être opérateur en France signifie respecter des obligations de sécurité portant sur les réseaux déployés et, pour ceux qui sont d'importance vitale, sur leurs systèmes d'informations

1. Les obligations pesant sur les opérateurs en matière de sécurité des réseaux.

En France, selon l'article L. 33-1 du code des postes et des communications électroniques, **l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles sur la sécurité des réseaux et de leurs usages**.

Édictées dans la partie réglementaire du même code, elles portent sur la permanence, la qualité et la disponibilité[2], sur la confidentialité, la sécurité et l'intégrité des réseaux[3], sur les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique[4] et sur l'acheminement des appels d'urgence[5] et des communications des pouvoirs publics destinées au public pour l'avertir de dangers imminents ou atténuer les effets de catastrophes majeures[6].

S'agissant plus particulièrement de l'intégrité et de la sécurité des réseaux, les opérateurs ont notamment l'obligation de **prendre toutes les mesures appropriées** pour assurer ces exigences, de **se conformer aux prescriptions techniques** adoptées par arrêté et **d'informer le ministre de l'intérieur de toute atteinte à la sécurit**é ou perte d'intégrité ayant un impact significatif sur le fonctionnement de ses réseaux ou de ses services.

Selon l'article L. 33-10 du code des postes et des communications électroniques, le ministre chargé des communications électroniques peut

---

[1] *Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, dont la déclinaison réglementaire figure aux articles R. 9-12-1 et suivants du code des postes et des communications électroniques.*
[2] *Article D. 98-4 du code des postes et des communications électroniques.*
[3] *Article D. 98-5 du code des postes et des communications électroniques.*
[4] *Article D. 98-7 du code des postes et des communications électroniques.*
[5] *Article D. 98-8 du code des postes et des communications électroniques.*
[6] *Article D. 98-8-7 du code des postes et des communications électroniques.*

imposer à tout opérateur de soumettre ses installations, réseaux ou services à un **contrôle de leur sécurité** et de leur intégrité effectué par l'Anssi, par un service de l'État ou par un organisme qualifié indépendant[1]. En principe, un seul contrôle peut être engagé par année civile pour un même réseau ou un même service. Les opérateurs ont confirmé au rapporteur avoir déjà fait l'objet de tels types de contrôles.

2. Les obligations pesant sur les opérateurs d'importance vitale en matière de sécurité des systèmes d'information.

Les opérateurs de communications électroniques reconnus comme d'importance vitale (OIV)[2] au titre du code de la défense sont soumis à des obligations particulières.

Les systèmes d'information des OIV[3] – ou systèmes d'information d'importance vitale (SIIV) – présents dans ce secteur font l'objet de règles précisées par un arrêté du 28 novembre 2016[4].

Cet arrêté impose notamment la définition d'une politique de sécurité des systèmes d'information, de règles d'homologation des systèmes, la mise en place d'une cartographie des systèmes. D'une manière générale, il édicte un certain nombre de **règles techniques et organisationnelles en vue de garantir la sécurité de ces systèmes d'information**.

Ce régime comporte également une obligation de **déclaration en cas d'incident** ainsi que la **soumission à un processus de contrôle et d'audit**.

C'est l'Anssi qui est en charge de sa mise en œuvre.

---

[1] *Articles 9-7 et suivants du code des postes et des communications électroniques.*

[2] *Selon l'article L. 1332-1 du code de la défense,* « Les 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, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste ». *La liste précise des opérateurs est un document classifié. En revanche, l'annexe de l'arrêté du 2 juin 2006 reconnaît expressément le secteur des communications électroniques comme d'importance vitale.*

[3] *Ce régime figure aux articles L. 1332-6-1 et suivants du Code de la défense ainsi qu'aux articles R. 1332-41-1 et suivants du même code.*

[4] *Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Communications électroniques et Internet » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.*

B. Les équipements télécoms sont actuellement soumis à une autorisation qui concerne aussi bien les équipementiers que les opérateurs et qui permet à l'État de les contrôler au regard du risque d'atteinte au secret des correspondances et à la vie privée.

1. Un régime d'autorisation visant à encadrer le commerce d'équipements pouvant porter atteinte au secret des correspondances, qui concerne aussi bien les opérateurs que les équipementiers.

Afin de protéger le secret des correspondances et la vie privée, le code pénal[1] exige l'obtention d'une **autorisation préalablement** à la fabrication, l'importation, l'acquisition, la détention, l'exposition, l'offre, la location ou la vente de certains **équipements conçus ou permettant d'y porter atteinte**.

En pratique, ce régime concerne à la fois le fabriquant, c'est-à-dire **l'équipementier**, que l'exploitant du dispositif – c'est-à-dire **l'opérateur**. On distingue ainsi l'autorisation requise pour « *la fabrication, l'importation, l'exposition, l'offre, la location ou la vente* » – prévue à l'article **R. 226-3** du code pénal (sorte d'autorisation de mise sur le marché), de celle requise pour « *l'acquisition ou la détention* », prévue à l'article **R. 226-7** du même code. Selon les éléments transmis au rapporteur, environ **1 200 autorisations** sont délivrées à ce titre chaque année, la moitié au titre de l'article R. 226-3 et l'autre au titre de l'article R. 226-7.

Ce régime autorise l'Anssi à **analyser la sécurité** et à **encadrer le commerce** d'équipements considérés comme sensibles, qui permettent notamment aux opérateurs de communications électroniques de satisfaire à leurs obligations en matière d'**interceptions judiciaires ou de sécurité**. Au-delà de la nécessité de détenir une autorisation pour commercer, ce régime organise une forme de système de **traçabilité** :

– chaque équipement autorisé doit porter la référence du type correspondant à la demande d'autorisation et un numéro d'identification individuel[2] ;

– et le titulaire d'une autorisation de mise sur le marché doit tenir un registre standardisé par arrêté et retraçant l'ensemble des opérations relatives à ces matériels[3].

[1] *Article 226-3 et R. 226-1 et suivants du code pénal.*
[2] *Article R. 226-6 du code pénal.*
[3] *Article R. 226-10 du code pénal.*

2. Actuellement limité aux équipements de « cœur de réseau », ce régime s'appliquera aux « stations de base » à compter d'octobre 2021.

Les « appareils et dispositifs techniques » soumis à ce régime sont **listés par un arrêté du Premier ministre**[1]. Ce champ d'application matériel va, en raison de la vocation même du régime, bien au-delà des équipements utilisés pour les réseaux télécoms *stricto sensu*.

Cependant, certains équipements télécoms sont bien concernés. Actuellement, il s'agit des **équipements** dits de « **cœur de réseau** ». Selon les éléments transmis au rapporteur, environ 500 autorisations sont délivrées chaque année aux opérateurs au titre de la détention d'équipements. Une part significative de ces autorisations porte sur des tests réalisés par les opérateurs en amont de potentiels déploiements.

Afin de prendre en compte les évolutions technologiques amenant au développement des « antennes intelligentes », la loi de programmation militaire de 2013[2] a étendu la portée du dispositif aux **éléments de desserte radio des réseaux mobiles** (« stations de base »). Ces équipements pourraient en effet être amenés à porter certaines des fonctions d'interception légale.

La modification effectuée par la loi de programmation militaire de 2013

Initialement limité aux équipements « *conçus pour réaliser les opérations* » pouvant constituer une infraction en matière d'interception de correspondances, le régime de l'article 226-3 du code pénal concerne désormais les **équipements qui, sans être spécifiquement conçus pour permettre les interceptions de communications, sont « *de nature à permettre* »** des interceptions.

En conséquence, l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal a été modifié en 2016 en vue d'intégrer les éléments de desserte radio des réseaux mobiles définis comme « *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* ». On remarquera que le nouvel article L. 34-11 du code des postes et des communications électroniques issu de la présente proposition de loi en est assez largement inspiré.

Cette modification **n'entrera en vigueur qu'en octobre 2021** afin, comme le relevait l'Arcep dans son avis sur l'arrêté de 2016, de « *permettre aux différents acteurs d'anticiper au mieux leurs stratégies de déploiement d'équipements de réseau et* ***d'organiser le remplacement****, d'ici l'échéance du*

[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] *Article 23 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.*

1er juillet 2021, des équipements actuellement exploités par les opérateurs qui sont susceptibles de faire l'objet d'un refus d'autorisation », ce remplacement pouvant concerner « *plusieurs milliers d'équipements* ».

Il n'y aura donc aucun « effet d'aubaine » sur ce point dans la mesure où les stations de base 5G qui pourraient être déployées par les opérateurs avant le 1er octobre 2021 devront bien faire l'objet, à compter de cette date, de demandes d'autorisation. Le Gouvernement a cependant précisé au rapporteur que, dans l'hypothèse où de graves défauts de sécurisation seraient constatés dans un équipement déployé à très grande échelle, une autorisation temporaire serait plus vraisemblablement prononcée qu'un refus, même si celui-ci était justifié, afin de permettre la correction des défauts ou le remplacement des équipements sans obérer le fonctionnement des réseaux.

Selon le Gouvernement, les antennes intelligentes devraient se généraliser avec le déploiement de réseaux 5G dits « *standalone* », anticipé au plus tôt en France à compter de 2021 voire 2022.

Une autorisation est-elle nécessaire en cas de mise à jour ?

Le régime de l'article 226-3 du code pénal concerne aussi bien les équipements matériels que les logiciels. Dans les précédentes générations de réseaux radioélectriques, les évolutions résultaient de changements d'équipements. Aujourd'hui, les réseaux sont modifiés par de simples mises à jour logicielles, ce qui pose la question de savoir quand il s'agit d'un nouvel équipement soumis à autorisation.

L'ensemble des équipementiers dans le domaine des télécommunications distinguent, dans leurs conventions de version :

– des évolutions **mineures** (apportant en général des corrections de vulnérabilités ou de dysfonctionnements, sans ajout de nouvelles fonctionnalités) ;

– et des évolutions **majeures** (évolutions du périmètre fonctionnel, par exemple support de nouveaux protocoles ou de nouvelles révisions des normes).

Cette distinction est généralement reprise dans les procédures de déploiement des opérateurs, qui déploient les mises à jours mineures après un ensemble de tests relativement réduit, mais prévoient des campagnes d'expérimentation prolongées avant toute mise à jour majeure.

Les **mises à jour mineures ne modifiant pas l'analyse de sécurité, elles ne donnent pas lieu à une nouvelle demande d'autorisation**.

En revanche, **en l'absence de conventions de version unifiées**, la définition précise de ce qui constitue une version majeure ou mineure est spécifique à chaque équipementier, voire à chaque gamme d'équipement. Ericsson a, par exemple, adopté un modèle dit « *one track* », c'est-à-dire sans version, ce qui ne permet plus de distinguer entre mise à jour majeure et mineure. Les modalités de gestion de ces « versions » sont alors arrêtées au **cas par cas** dans les conditions associées à chaque autorisation.

3. L'instruction de la demande est effectuée par l'Anssi, selon des délais variés.

La demande d'autorisation doit être déposée auprès du directeur général de l'**Anssi** et comporter, entre autres, les opérations pour lesquelles l'autorisation est demandée et, le cas échéant, la description des marchés visés, l'objet et les caractéristiques techniques du type de l'appareil ou du dispositif technique, accompagnés d'une documentation technique[1].

L'instruction de la demande est effectuée par le bureau des contrôles réglementaires de l'Anssi – qui s'appuie au besoin sur les équipes d'audit ou d'assistance technique ou ses laboratoires. Elle exige de recueillir l'**avis obligatoire d'une commission consultative** présidée par le directeur général de l'Agence et composée de représentants des administrations intéressés (ministères en charge de la justice, de l'intérieur, de la défense, des douanes, de l'industrie, des télécommunications, Agence nationale des fréquences), d'un représentant de la Commission nationale de contrôle des techniques de renseignement et de deux personnalités qualifiées désignées par le Premier ministre[2].

Dans les faits, cette commission se réunit tous les deux mois. Hors cas d'urgence opérationnelle avérée, **l'Anssi requiert en général que les demandes soient déposées au plus tard un mois et une semaine avant la tenue d'une commission**, afin de permettre leur analyse par les différents services représentés au sein de cette commission.

Le décret n° 2014-1266 du 23 octobre 2014 relatif aux exceptions à l'application du principe « silence vaut acceptation » prévoit que **le silence gardé par l'administration durant 9 mois vaut décision de refus**.

Toutefois, comme précisé par le Gouvernement dans sa réponse au rapporteur, le **délai effectif de traitement des demandes est très dépendant de la nature des appareils concernés** :

– les renouvellements d'autorisations antérieures ou les nouvelles demandes portant sur des évolutions de gammes d'équipements déjà analysées par l'Anssi font généralement l'objet d'une décision lors de leur premier passage en commission ;

– en revanche, des appareils présentant une rupture technologique significative par rapport aux équipements antérieurement étudiés, ou des facteurs de complexité particuliers (nouvel équipementier, architecture technique particulièrement complexe…), peuvent faire l'objet de plusieurs ajournement successifs par la commission, et d'importants délais d'analyse. Les causes de ces délais peuvent être multiples : nécessité de compléter la demande d'autorisation par des informations techniques complémentaires, de planifier des tests au sein de plateformes techniques mises à disposition

[1] *Article R. 226-4 du code pénal.*
[2] *Article R. 226-3 du code pénal.*

par les opérateurs ou équipementiers, voire de réaliser des évolutions des appareils analysés suite à l'identification de faiblesses de sécurité.

La grande variété des types d'appareils examinés ne permet pas de fournir des délais moyens représentatifs, mais des **délais de l'ordre de six mois, voire un an pour les dossiers les plus complexes, ne sont pas exceptionnels**. La planification anticipée des demandes et des phases de test associées avec les principaux équipementiers et opérateurs permet cependant, en général, de limiter significativement tant ces délais que leur impact sur les déploiements.

Le Gouvernement a précisé au rapporteur qu'une demande d'autorisation au titre de l'article R. 226-7 du code pénal ne nécessite généralement pas d'instruction approfondie dès lors qu'une autorisation R. 226-3 a déjà été accordée.

4. L'autorisation est délivrée pour trois à six ans, mais peut être retirée.

L'autorisation concernant **les équipementiers** est **délivrée pour six ans**[1] par le Premier ministre. Elle **peut fixer les conditions** de réalisation de l'opération et le nombre des appareils ou des dispositifs techniques concernés[2].

L'autorisation concernant les **opérateurs** ne peut être délivrée que pour une durée maximale de **trois ans**[3]. Elle peut subordonner l'utilisation des appareils ou des dispositifs techniques à des conditions destinées à en éviter tout usage abusif.

Le code pénal prévoit que ces autorisations peuvent être **retirées** dans certaines conditions[4] (en cas de fausse déclaration ou de faux renseignement, en cas de modification des circonstances au vu desquelles l'autorisation a été délivrée, lorsque le bénéficiaire de l'autorisation n'a pas respecté les dispositions réglementaires ou les obligations particulières prescrites par l'autorisation, ou lorsque le bénéficiaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation). Le retrait ne peut intervenir, sauf urgence, qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations.

Les autorisations prennent fin de plein droit en cas de condamnation du titulaire pour infraction à la vie privée ou atteinte au secret des correspondances.

En cas de **retrait** comme d'**expiration** de l'autorisation, les titulaires disposent d'un délai d'**un mois pour procéder à la destruction des appareils**

---

[1] *Article R. 226-5 du code pénal. Elle est accordée de plein droit aux services de l'État désignés par arrêté du Premier ministre pour la fabrication d'appareils ou de dispositifs techniques.*
[2] *Article R. 226-5 du code pénal.*
[3] *Articles R. 226-7, R. 226-8 et R. 226-9 du code pénal.*
[4] *Article R. 226-11 du code pénal.*

ou pour les vendre ou les céder à une personne titulaire de l'une des autorisations[1].

5. Les équipements radioélectriques mis sur le marché européen doivent également respecter certaines exigences essentielles.

Pour mémoire, on rappellera également que la mise sur le marché des équipements radioélectriques[2] est soumise au respect de la directive dite « RED »[3]. En application de ce texte, ces équipements ne peuvent être mis sur le marché, connectés à un réseau ouvert au public, mis en service ou utilisés que si leur conformité aux exigences essentielles a été **évaluée préalablement, selon des procédures d'évaluation interne ou par un organisme extérieur**.

Ces **exigences essentielles** portent sur de très nombreux aspects, tels que la santé et la sécurité des personnes, la protection des biens, la compatibilité électromagnétique, l'utilisation efficace des fréquences, la protection des réseaux et la protection de la vie privée des utilisateurs[4].

Les lacunes du droit en vigueur pour assurer la sécurité des réseaux 5G ont été décrites dans l'exposé général.

II. La proposition de loi initiale : un nouveau dispositif d'autorisation préalable à l'exploitation de certains équipements par les opérateurs de communications électroniques d'importance vitale en vue d'assurer la sécurité des réseaux 5G.

La proposition de loi introduit une section 7 intitulée « *régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques* » au sein du chapitre II du titre Ier du livre II du code des postes et des communications électroniques, consacré au régime juridique des communications électroniques.

---

[1] *Article R. 226-12 du code pénal.*

[2] *Au sens du 11° de l'article 32 du code des postes et des communications électroniques.*

[3] *Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE, transposée par l'ordonnance n° 2016-493 du 21 avril 2016 relative à la mise sur le marché d'équipements radioélectriques et le décret n° 2017-599 du 21 avril 2017 relatif à la mise à disposition sur le marché des équipements radioélectriques.*

[4] *Voir le 12° de l'article 32 du code des postes et des communications électroniques et les articles R. 20-1 et suivants du code des postes et des communications électroniques.*

L'article 1er crée quatre nouveaux articles établissant les principes applicables à ce nouveau dispositif d'autorisation administrative préalable à l'exploitation[1] d'équipements de réseaux radioélectriques.

Le régime d'autorisation préalable est le plus restrictif des libertés en matière économique par rapport aux deux autres régimes que sont la déclaration préalable et le régime de liberté sous réserve du respect de certaines exigences, sous peine de sanction pénale. Il est cependant justifié en l'espèce par le motif d'intérêt général que constitue la préservation de la défense et de la sécurité nationale.

Il convient de noter que, dans le silence des dispositions de nature législative et réglementaire relatives à ce régime *ad hoc*, c'est le régime de droit commun issu du code des relations entre le public et l'administration qui s'appliquera à cette nouvelle autorisation.

A. Un champ d'application limité à l'exploitation d'équipements des réseaux « mobiles » ouverts au public déployés par des opérateurs d'importance vitale, amené à être précisé par voie réglementaire.

Le I- du nouvel article L. 34-11 poserait le principe d'une autorisation préalable à l'exercice d'une activité consistant à exploiter certains appareils et en déterminerait le champ d'application.

1. Les « appareils » concernés.

Plutôt que de faire référence aux équipements, le texte reprend la terminologie de l'arrêté du 4 juillet 2012 et vise les « ***appareils, à savoir tous dispositifs matériels ou logiciels*** »[2].

Le nouveau régime ne s'appliquerait **qu'aux appareils composant les « réseaux radioélectriques**[3] **mobiles »**. Cette terminologie exclut les équipements des réseaux filaires (cuivre, câble ou fibre optique) et les réseaux *wi-fi*.

Seuls les **appareils « *permettant de connecter les équipements de clients au réseau radioélectrique* *qui*, *par leurs fonctions*, *présentent un risque* *pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau* ».

[1] *Le terme d'exploitation a été choisi par le Gouvernement par référence aux articles du code des postes et des communications électroniques, qui mentionne à de nombreuses reprises l'exploitation des réseaux, notamment dans la définition des opérateurs figurant au 15° de l'article L. 32 du code.*

[2] *Si l'article 226-3 du code pénal mentionne les « appareils ou dispositifs techniques », l'arrêté fixant la liste de ces appareils et dispositifs, définit les appareils comme étant des « dispositifs matériels ou logiciels ». Cette tournure, estimée plus claire par le Gouvernement, a été reprise pour la présente proposition de loi.*

[3] *Pour mémoire, selon l'article L. 32 11° du code des postes et des communications électroniques, un réseau est qualifié de radioélectrique* « lorsqu'il utilise intentionnellement des fréquences radioélectriques, en émission ou en réception, pour la propagation des ondes en espace libre, à des fins de radiocommunication ou de radiorepérage ».

Selon le Gouvernement, cette terminologie vise à faire entrer dans les champs du contrôle les différents **composants « actifs »** ou « intelligents » du réseau impliqués dans :

– l'acheminement des communications des équipements terminaux, entre eux ou à destination de réseaux tiers ;

– les différentes fonctions contribuant à cet acheminement, telles que l'authentification des terminaux, le routage des flux, ou le contrôle d'accès.

Elle exclurait les fonctions du réseau qui ne contribuent pas à cet acheminement (par exemple, la facturation) et qui ne constituent par conséquent pas *a priori* un enjeu de sécurité nationale.

Le **Premier ministre doit déterminer la liste précise appareils concernés par arrêté.**

La question de savoir si **les mises à jour des logiciels** seront considérées comme des dispositifs logiciels soumis à autorisation est souvent revenue lors des débats autour de cette proposition de loi. Reprenant l'approche adoptée dans le cadre de l'article 226-3 du code pénal, le Gouvernement a confirmé au rapporteur que « *les mises à jour mineures ne devraient pas être soumises à autorisation* », ce point faisant l'objet d'une précision dans le projet de décret d'application.

Sont, en revanche, exclus du champ d'application du dispositif les **appareils installés « chez les clients »**. Cela vise à exclure des équipements dont l'exploitation ne se fait pas *stricto sensu* sous la responsabilité de l'opérateur qui les a déployés ou mis à disposition de ses clients, et qui ne sont en tout état de cause pas associés à un enjeu sécuritaire à portée systémique, à savoir :

– les équipements terminaux (tels que les téléphones intelligents) ;

– les équipements de desserte locale à très courte portée déployés au profit d'un utilisateur particulier (comme les « *femtocells* »).

2. Seuls les opérateurs d'importance vitale exploitant des réseaux ouverts au public sont visés.

Le texte ne vise que les **opérateurs de communications électroniques d'importance vitale**. Cela exclue les opérateurs de communications électroniques qui ne sont pas considérés d'importance vitale. L'objectif d'une telle délimitation du champ est de centrer le dispositif sur les seuls opérateurs porteurs d'une mission critique pour la sécurité nationale, c'est-à-dire, par construction, ceux qui ont été désignés opérateurs d'importance vitale en vertu des réseaux qu'ils opèrent.

Cette précision exclue également les équipementiers. Cela se justifie car ce n'est pas la vulnérabilité des équipements eux-mêmes que le régime d'autorisation vise à évaluer mais la vulnérabilité des réseaux utilisant ces

équipements. Le Gouvernement estime, du reste, qu'un mécanisme de sanction applicable aux producteurs d'équipements en cas de vulnérabilité de ces derniers serait extrêmement complexe à mettre en place, notamment du fait de la quasi-impossibilité, sur le plan technique, de démontrer le caractère intentionnel d'une telle vulnérabilité. Enfin, une extension du régime de la proposition de loi aux équipementiers risquerait de mettre en péril le régime d'autorisation prévu à l'article R. 226-3 du code pénal, dont l'efficacité a jusqu'ici été démontrée.

Seuls les équipements insérés dans le **réseau ouvert au public** de ces opérateurs seront concernés. Cela exclut les réseaux professionnels d'entreprises (ou réseaux « PMR[1] ») qui pourraient être utilisés par des industriels en dehors du secteur des télécoms, dès lors qu'ils reposeront sur des infrastructures dédiées, et non mutualisées avec les réseaux publics. Les évolutions technologiques apportées par la 5G (en particulier, le *slicing*, permettant de construire plusieurs réseaux virtuels sur une même infrastructure) permettent néanmoins d'envisager à terme des réseaux professionnels adossés aux réseaux publics, et qui en partageraient les éléments d'infrastructure. Dans ce cas, les éléments d'infrastructure mutualisés au contrôle seront soumis au régime d'autorisation.

3. L'autorisation porte sur l'activité d'exploitation, directe ou par l'intermédiaire de tiers fournisseurs.

C'est bien **l'activité d'exploitation** des équipements qui est visée par l'obligation de disposer d'une autorisation et non l'équipement en lui-même.

Cette activité nécessitera d'obtenir une autorisation, qu'elle se fasse **directement ou par l'intermédiaire de tiers fournisseurs**. Cette précision vise à prendre en compte le fait que, comme évoqué dans l'exposé général, selon le Gouvernement, les possibilités accrues de virtualisation des infrastructures réseaux qui accompagnent la 5G rendent envisageables de nouvelles répartitions des rôles entre les différents acteurs économiques de la chaîne de valeur des réseaux.

B. Une autorisation que le Premier ministre peut accorder pour huit ans, renouveler, et refuser uniquement en cas de risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale.

L'autorisation serait délivrée par le Premier ministre – et instruite, dans les faits, par l'Anssi.

Le II- de l'article L. 34-1 et les nouveaux articles L. 34-11-1 et L. 34-11-2 préciseraient les conditions d'octroi de l'autorisation.

[1] *Pour* Private Mobile Radiocommunications.

Le II- de l'article L. 34-11 préciserait que l'autorisation ne serait octroyée que pour un certain **périmètre défini dans le dossier de demande**. Celui-ci doit ainsi définir :

– un **périmètre technique** – c'est-à-dire le ou les modèles et le ou les versions de dispositifs matériels ou logiciels dont il demande l'autorisation ;

– un **périmètre géographique** d'exploitation.

Le II- de l'article L. 34-1 précise que l'autorisation peut être octroyée pour une **durée maximale de huit ans**. Cette durée de huit ans semble correspondre à la durée d'amortissement des équipements matériels aujourd'hui déployés dans les réseaux mobiles. La durée du cycle d'innovation des logiciels est, en revanche, beaucoup plus courte (une fois par an à prévoir pour les mises à jour « majeures » de la 5G). La durée maximale de huit ans apparaît donc particulièrement protectrice pour les demandeurs au regard des appareils auxquels elle s'appliquera d'une part, et en comparaison avec le régime de l'article 226-3 du code pénal d'autre part.

Selon le nouvel article L. 34-11-1, l'autorisation pourrait être **renouvelée sur demande de son bénéficiaire**. Il devrait alors formuler cette demande au moins deux mois avant l'expiration de l'autorisation initiale.

Les modalités de l'autorisation, la composition du dossier de demande d'autorisation et du dossier de demande de renouvellement seraient **fixées par décret**.

L'article L. 34-11-2 préciserait les motifs de refus opposables par le Premier ministre et évoquerait certains éléments de fait qu'il pourrait prendre en compte au soutien de sa décision.

S'agissant des motifs de refus, le Premier ministre ne pourrait arguer que d'un **risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale**, ce risque étant **caractérisé par l'absence de garantie du respect des règles applicables aux opérateurs de communications électroniques**[1] **«** *en particulier l'intégrité, la sécurité et la continuité de l'exploitation des réseaux et services de communications électroniques* ».

Le texte précise que, pour l'appréciation de ces critères, le Premier ministre peut notamment[2] prendre en considération des éléments d'ordre technique et des éléments d'ordre non technique.

S'agissant des **éléments d'ordre technique**, le texte dispose que le Premier ministre pourra prendre en compte les **modalités de déploiement et d'exploitation mises en place par l'opérateur**. Cet élément s'appuie, à nouveau, sur le constat selon lequel la liberté accrue que conférera la 5G aux

[1] *Ces règles sont mentionnées aux a, b et e du I de l'article L. 33-1.*

[2] *L'adverbe n'est pas présent dans le texte mais cela va de soi puisqu'il s'agit d'assurer, dans le texte, que le Premier ministre pourra légalement se prévaloir de ces éléments de fait pour refuser l'autorisation.*

opérateurs dans leurs choix de déploiement et de mise en œuvre de leurs réseaux, qui pourrait s'accompagner d'un recours plus important à la sous-traitance, constitue un des principaux facteurs de vulnérabilité de la 5G.

Selon le Gouvernement, l'analyse du Premier ministre portera en particulier sur les **opérations de configuration et de supervision** réalisées sur les appareils soumis au contrôle, et **sur les sous-traitants** impliqués dans ces opérations.

Les « *modalités de déploiement* » concerneraient la conception des réseaux avant leur activation. Elles amèneraient l'Anssi à vérifier notamment la bonne activation des options de sécurité, l'existence d'une architecture limitant l'exposition aux attaques, la mise en place d'une redondance ou encore de protections périmétriques.

La mention des « *modalités d'exploitation* » renverrait aux actions des opérateurs sur les réseaux une fois ceux-ci activés. L'Anssi pourrait ainsi s'assurer du caractère sécurisé de l'administration du réseau, des modalités de contrôle de l'accès des exploitants aux opérations sensibles, des modalités de supervision ou encore de l'existence de procédures efficaces de déploiement des correctifs.

Parmi les éléments techniques, même si cela n'est pas mentionné dans le texte, le Gouvernement a précisé au rapporteur que l'Anssi prendrait également en compte les **propriétés techniques intrinsèques des différents composants des réseaux 5G** (mise en œuvre des bonnes pratiques de sécurisation, suivi et correction efficace des vulnérabilités, mécanismes de défense en profondeur permettant de tolérer certaines vulnérabilités, possibilité d'évaluation de la sécurité par des tiers…).

Le texte précise, par ailleurs, que le Premier ministre pourra également prendre en compte des **éléments non techniques**. Ainsi, le fait que **l'opérateur ou ses prestataires** – fournisseurs d'équipements, intégrateurs ou sous-traitants impliqués dans les opérations de maintenance et d'exploitation des réseaux des opérateurs –, **soit ou non sous le contrôle ou soumis à des actes d'ingérence** d'un État non membre de l'Union européenne, pourra être pris en compte. Il s'agit, selon le Gouvernement, de traiter du cas d'ingérence d'un État disposant d'un pouvoir de contrainte vis-à-vis de ces acteurs, notamment du fait de dispositions légales qui leur sont applicables en vertu de leur nationalité, ou des liens financiers qu'ils entretiennent avec ces États.

Ces éléments non techniques pourront être apportés dans l'instruction par le Secrétariat général de la défense et la sécurité nationale, en se fondant notamment sur les analyses auxquelles il est associé dans le cadre du dispositif national de d'information stratégique et de sécurité économique.

Comme vu dans l'exposé général, il est possible d'identifier deux États particulièrement concernés par ce critère, à savoir les États-Unis et la

Chine, notamment à travers le *Cloud Act* pour l'un et la loi sur le renseignement de 2017 pour l'autre. En conséquence, sur le marché des équipements, il est probable que le recours, par les opérateurs, à Huawei et Cisco, fasse l'objet d'une attention particulière.

C. Un pouvoir d'injonction en cas d'exploitation sans autorisation

Le I du nouvel article L. 34-11-3 conférerait au Premier ministre le pouvoir d'enjoindre à un opérateur d'importance vitale exploitant en France des appareils sans autorisation ou avec une autorisation expirée :

– de **déposer une demande d'autorisation** ou de renouvellement ;

– ou de **faire rétablir à ses frais la situation antérieure**, dans un délai qu'il fixe.

Afin d'assurer le caractère contradictoire de la procédure, ces injonctions ne peuvent intervenir qu'une fois l'opérateur **mis en demeure de présenter des observations** dans un délai de quinze jours, sauf en cas d'urgence, de circonstances exceptionnelles ou d'atteinte imminente à la sécurité nationale.

D. La sanction civile de l'absence d'autorisation : la nullité des conventions

Le II du nouvel article L. 34-11-3 établirait une sanction civile : la **nullité** de tout engagement juridique[1] d'exploitation des appareils concernés sans autorisation. Cela recouvrirait tout contrat de sous-traitance – qui pourrait porter sur l'administration et la configuration distante ou la supervision – ou de prestation de services relative à l'exploitation des appareils concernés – comme la fourniture de mises à jour ou les prestations de soutien par l'équipementier.

Interrogé sur ce point par le rapporteur, le Gouvernement estime que les nouvelles obligations qui incomberont aux opérateurs pourront certainement être répercutées par ces derniers, à leur initiative, dans les cadres contractuels qui les lient à leurs fournisseurs ou sous-traitants, par exemple sous la forme d'une obligation de compensation en cas de refus d'autorisation imputable au fournisseur.

[1] *Les termes « engagements, convention ou clause contractuelle » figurant dans le texte ont été repris de l'article L. 151-4 du code monétaire et financier relatif au dispositif applicable aux investissements étrangers en France.*

E. Les clarifications obtenues par le rapporteur

1. Sur la durée d'instruction de la demande

Lors de son audition en commission, la secrétaire d'État auprès du ministre de l'Économie et des Finances a confirmé que le Gouvernement retiendrait le principe selon lequel le silence gardé par l'administration pendant deux mois vaut décision de rejet. En application du 4° de l'article L. 231-4 du code des relations entre le public et l'administration[1], le Gouvernement sera donc contraint d'adopter un décret en Conseil d'État.

Il convient de noter que, dans ces cas, l'obligation de motivation s'exerce dans des conditions différentes. En effet, par hypothèse, une décision implicite de rejet n'est pas motivée. C'est pourquoi l'article L. 232-4 du code des relations entre le public et l'administration, les motifs de toute décision implicite de rejet peuvent être communiqués à l'intéressé s'il en formule la demande dans les délais du recours contentieux. L'administration doit alors transmettre les motifs de l'acte dans le mois suivant cette demande. Dans ce cas, le délai du recours contentieux contre la décision est prorogé jusqu'à l'expiration de deux mois suivant le jour où les motifs lui auront été communiqués.

2. Une possibilité d'abrogation, mais pas de retrait

S'agissant des modalités d'abrogation et de retrait de la décision, la ministre a précisé lors des débats à l'Assemblée que c'est le **droit commun** qui s'appliquerait. Autrement dit, c'est le régime de l'abrogation et du retrait des actes administratifs individuels créateurs de droit, tels que défini par le code des relations entre le public et l'administration, qui s'appliquerait. Une abrogation ou un retrait ne pourraient donc avoir lieu que si l'autorisation initiale est illégale et si l'abrogation ou le retrait intervient dans le délai de quatre mois[2]. Une abrogation resterait possible sans délai si l'autorisation était subordonnée à une condition qui n'est plus remplie[3].

Le Gouvernement a précisé au rapporteur qu'il n'envisage aucunement d'édicter des dispositions spécifiques au retrait, contrairement au régime applicable au titre de l'article 226-3 du code pénal, afin de sécuriser les opérateurs quant à leurs plans d'investissements. Il considère en effet que la possibilité d'un retrait de l'autorisation d'exploitation d'équipement de réseaux, d'une part, ferait courir une menace financière

---

[1] *Selon lequel* « Par dérogation à l'article L. 231-1, le silence gardé par l'administration pendant deux mois vaut décision de rejet : (…) Dans les cas, précisés par décret en Conseil d'État, où une acceptation implicite ne serait pas compatible avec le respect des engagements internationaux et européens de la France, la protection de la sécurité nationale, la protection des libertés et des principes à valeur constitutionnelle et la sauvegarde de l'ordre public ».

[2] *Article L. 242-1 du code des relations entre le public et l'administration (CRPA).*

[3] *Article L. 242-2 du CRPA.*

importante pour les opérateurs au regard des coûts d'investissement que représentent ces réseaux (cela ne serait pas de nature à encourager les investissements), d'autre part, risquerait de perturber gravement et peut-être même de manière irrémédiable (risque de décès) la vie économique et sociale de l'ensemble des personnes concernées par le fonctionnement de ces réseaux.

S'agissant de la possibilité d'abroger une décision, il a également précisé au rapporteur que « *l'autorité administrative devra veiller à la proportionnalité de ses décisions notamment lorsque les réseaux seront déjà installés. Une décision d'abrogation d'autorisation pourrait remettre en cause sur une zone donnée du territoire l'accès à l'ensemble des technologies* ».

3. Aucune modalité de contrôle spécifique n'est prévue.

Le Gouvernement a précisé au rapporteur qu'il n'entend pas mettre en place de modalités de contrôles spécifiques à ce régime d'autorisation. En revanche des contrôles pourront être réalisés par le biais d'audits de sécurité, réalisés par l'Anssi ou pour un organisme tiers à la demande du ministre chargé des communications électroniques, selon les modalités prévues par l'article L. 33-10 du code des postes et communications électroniques déjà évoqué.

III. Les modifications apportées par l'Assemblée nationale : l'obligation pour le Gouvernement de consulter certains organismes avant d'adopter les dispositions d'application de la loi.

Outre des amendements rédactionnels et d'amélioration de la rédaction du texte (suppression de la « mise à jour » de la liste des appareils par le Premier ministre, référence aux « utilisateurs finaux » plutôt qu'aux « clients »…), les députés ont inséré la **consultation obligatoire de l'Arcep** sur le projet d'arrêté listant les appareils entrant dans le champ d'application de l'autorisation et celle de l'Arcep et de la **Commission supérieure du numérique et des postes** (CSNP) – dont sont membres, pour la commission des affaires économiques, Mmes Patricia Morhet-Richaud et Denise Saint-Pé – sur le projet de décret d'application.

Afin de ne pas rallonger excessivement les délais de publication du décret, l'amendement adopté précise que l'Arcep et la CSNP se prononcent dans un **délai d'un mois à compter de leur saisine** sur le décret d'application.

IV. La position de la commission : un juste équilibre entre les impératifs de sécurité et les besoins des entreprises et des usagers de la 5G.

La position de la commission sur cet article se résume en quatre axes : proportionner l'impact du texte aux enjeux, sécuriser le texte juridiquement, ne pas discriminer tel ou tel prestataire, préciser autant que possible ses dispositions.

1. Proportionner l'impact du texte sur les déploiements aux risques de sécurité.

a. Restreindre le champ d'application du texte au strict nécessaire

Le champ d'application du texte apparaît, en l'état, particulièrement large et il conviendra que les textes d'ordre réglementaire en précisent bien la portée. Le Gouvernement a précisé au rapporteur qu'il souhaite « *un dispositif clair et plutôt étroit, mais qui puisse permettre au Gouvernement de s'adapter aux évolutions technologiques* ».

Interrogé sur la question de savoir si, conformément à ses déclarations, le Gouvernement entendait que le texte ne s'applique qu'aux équipements 5G, il a assuré au rapporteur que, « *même si ce point n'apparaît pas explicitement dans le texte législatif, le nouveau dispositif ne concernera effectivement que les réseaux 5G (et, à terme, des générations ultérieures). Ce point est précisé dans le projet d'arrêté listant les types d'appareils dont l'exploitation devra faire l'objet d'une autorisation* ».

Sur proposition du rapporteur, la commission a estimé qu'il convenait d'effectuer une telle précision dans le dispositif de la proposition de loi (**COM-20**).

De même, afin de limiter le champ d'application du texte au strict nécessaire, la commission a également adopté des amendements tendant à exclure les équipements identifiés *ab initio* comme non risqués ou dont l'inclusion dans le champ serait disproportionné (**COM-1 rect. ter et COM-11 rect.**). En effet, les dispositifs passifs et non configurables sont dénués d' « intelligence » et ne présentent, en conséquence, aucun enjeu de sécurité. Quant aux dispositifs non spécialisés, tels que les serveurs informatiques « grand public », ils s'inscrivent, pour les opérateurs, dans une logique d'achat sur étagère plutôt que dans le cadre d'un grand contrat avec un équipementier. En conséquence, les intégrer au dispositif rendrait ce dernier extrêmement lourd pour eux, alors que ces éléments « banalisés » ne nécessitent pas une analyse de sécurité spécifique, dans la mesure où leurs propriétés sont bien connues de l'Anssi, qui saura au besoin intégrer cette connaissance dans l'analyse des modalités de déploiement.

b. Exiger que le Premier ministre prenne en compte les risques sur le rythme et le coût des déploiements ainsi que sur l'accès des utilisateurs aux services.

Dans son avis rendu en février, l'Arcep soulignait que « *de nouvelles dispositions qui auraient pour effet de remettre en cause des investissements passés et conduirait au remplacement anticipé d'équipements déjà en service pourraient avoir un effet notable sur l'activité des opérateurs* ». Elle appelait ainsi le Premier ministre à évaluer, lors de l'instruction des demandes, « *les éventuels effets rétroactifs (même indirects) des décisions prises dans le cadre de ce dispositif sur les déploiements passés* ».

Le rapporteur estime que **la proposition de loi ne devrait pas avoir pour effet de remettre en cause la dynamique des déploiements engagés sur la 4G** dans le cadre du « *New Deal* » mobile et accompagnés par le législateur dans le cadre de la loi dite « ELAN »[1].

De même, il est **impératif que la France ne prenne pas de retard en matière de 5G**.

Il est donc **crucial que le Premier ministre proportionne sa décision au risque, en prenant en compte les effets que sa décision pourrait avoir sur le rythme et le coût des déploiements à venir ainsi que sur l'accès des utilisateurs finaux aux services sur lesquels s'appuient les équipements déjà déployés**.

C'est pourquoi la commission a adopté, sur proposition du rapporteur, un amendement qui oblige le Premier ministre à prendre en compte ces éléments (**COM-24**). Cet amendement rehausse le niveau de l'exigence de proportionnalité des décisions que prendra le Premier ministre afin d'éviter qu'il ne « *tire sur les moineaux à coups de canon* »[2].

c. Permettre au Premier ministre d'accepter sous conditions.

Au cours des débats parlementaires, la secrétaire d'État auprès du ministre de l'Économie et des finances a, à plusieurs reprises, affirmé que l'approche du Premier ministre ne sera pas binaire. Celui-ci pourrait en effet autoriser, refuser, mais également autoriser sous conditions. Autrement dit, il pourrait dire « oui », « non » et « oui, mais ». Cependant, la possibilité d'édicter de telles conditions d'autorisation n'est, à ce stade, pas mentionnée dans le texte.

En conséquence, sur proposition du rapporteur, la commission a adopté un amendement affirmant que le Premier ministre pourrait assortir son autorisation de conditions, dont le non-respect pourrait faire l'objet

---

[1] *Loi n° 2018-1021 du 23 novembre 2018 portant évolution du logement, de l'aménagement et du numérique.*

[2] *Selon l'expression du juriste allemand Fleiner dans un commentaire d'une décision de justice publié en 1912 relatif au principe de proportionnalité (cité par B. Stirn dans* « Vers un droit public européen »*, 2015).*

d'une injonction du Premier ministre (**COM-22**, **COM-25**). Ainsi, le Premier ministre pourra proportionner sa décision aux enjeux de sécurité et, plutôt que de devoir refuser, octroyer une autorisation sous conditions.

d. S'assurer que l'État ne dicte pas aux opérateurs leur politique d'achat.

Le débat sur l'« **approche géographique** » est né du rapport pour avis de l'Assemblée nationale, qui pouvait être interprété comme permettant à l'Anssi de s'assurer d'une parfaite hétérogénéité des fournisseurs sur l'ensemble des plaques géographiques de déploiement. Ce qui pourrait conduire à ce que le Premier ministre empêche un opérateur d'utiliser les équipements d'un fournisseur sur une zone géographique donnée si un autre opérateur a déjà choisi ce même fournisseur sur la même zone.

Lors de son audition par la commission, la secrétaire d'État auprès du ministre de l'économie et des finances a affirmé : « *je ne crois pas qu'il appartienne à l'Anssi de définir la politique achat des opérateurs télécom, ce que l'agence reconnaît d'ailleurs* ».

De même, dans ses réponses écrites, le Gouvernement a confirmé que « ***la mise en œuvre de ce texte ne doit pas aller jusqu'à ce qui semble être l'interprétation du rapporteur Gassilloud, à savoir que le Premier ministre exigerait que l'on dispose d'une grande diversité d'équipementiers sur chaque plaque. L'objectif du Gouvernement, à travers la mise en œuvre de ce dispositif n'est pas d'imposer aux opérateurs le choix de leurs équipementiers par zone géographique.*** *Avec seulement trois équipementiers à ce jour en France, cela obérerait les marges de négociation des opérateurs et augmenterait les coûts de déploiement. Au demeurant, la situation actuelle des déploiements 2G/3G/4G des quatre principaux opérateurs offre d'ores et déjà une bonne diversité de choix d'équipementiers, et la situation dans laquelle tous les opérateurs s'appuieraient sur le même équipementier ne pourrait se produire qu'à condition d'une évolution majeure des choix d'équipementiers de plusieurs de ces opérateurs* ».

Les opérateurs ont souligné que, s'il existe aujourd'hui une règle non écrite, pour certains matériels sur une zone géographique donnée, elle est motivée par le caractère sensible de certaines installations civiles et militaires sur la zone en cause et non par un principe de diversité des équipementiers sur une même zone.

Ils estiment que « l'approche géographique » telle que décrite dans le rapport pour avis de l'Assemblée nationale serait discutable d'un point de vue technique dans la mesure où, en dehors des appels d'urgence, les opérateurs ne prévoient pas techniquement la possibilité d'écouler le trafic de leurs clients en utilisant les réseaux des autres opérateurs. Ainsi, en cas de panne du réseau d'un opérateur, les réseaux des autres opérateurs ne seraient pas suffisamment dimensionnés pour prendre en charge le trafic

supplémentaire. Au contraire, cela pourrait entraîner un déni de service également chez les autres opérateurs.

Ils soulignent surtout le caractère discutable des effets d'une telle approche sur le marché : elle pourrait renforcer la position des fournisseurs autorisés et générer, pour les opérateurs, l'obligation de s'entendre sur les déploiements.

Par ailleurs, elle pourrait en particulier mettre en difficulté un opérateur comme Free qui n'a, jusqu'ici, eu recours qu'à Nokia pour la quasi-totalité de ses équipements.

Comme déjà évoqué, la diversité des équipementiers présents en France résulte actuellement d'une logique de marché, dans la mesure où cela apparaît raisonnable d'un point de vue économique. Il ne faudrait pas que cela résulte d'une forme de planification résultant du dispositif d'autorisation établi par la présente proposition de loi.

Constatant une forme d'ambigüité persistante sur ce sujet, sur proposition du rapporteur, la commission a donc **supprimé la référence au périmètre géographique dans le dossier de demande d'autorisation**, afin de s'assurer que l'État ne dicte pas aux opérateurs leur politique d'achat (**COM-30 rect.** et **COM-13 rect.**).

2. S'assurer de la sécurité juridique du dispositif.

Comme évoqué dans l'exposé général du présent rapport, le Gouvernement a fait preuve, dans la gestion de la discussion parlementaire de ce texte, d'une certaine précipitation. Cela a privé le Parlement d'une étude d'impact mais aussi de l'avis du Conseil d'État.

Afin d'éviter de reproduire la même erreur au stade des textes d'application, la commission a adopté, sur proposition du rapporteur, un amendement exigeant que le décret d'application soit adopté en Conseil d'État (**COM-22**). Cela constitue une garantie quant à la sécurité juridique du dispositif retenu pour les textes d'application. Au demeurant, une telle exigence se retrouve dans de nombreux autres dispositifs d'autorisation préalable (régime de l'article 226-3 du code pénal, autorisation des moyens de cryptologie, accès et produits d'utilisation du service public réglementé de radionavigation par satellite, régime d'autorisation des investissements étrangers…). Enfin, le Gouvernement y sera tenu en application du code des relations entre le public et l'administration s'il souhaite, comme cela a pu être affirmé à plusieurs reprises au cours des débats parlementaires, déroger au principe selon lequel le silence gardé par l'administration pendant deux mois vaut accord : il eût donc été malvenu qu'il ne soumette au Conseil d'État que ce volet des mesures d'application nécessaires.

3. Le souhait de ne pas discriminer

Sur proposition du rapporteur, la commission a adopté un amendement précisant que le Premier ministre devra prendre en considération le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'**ingérence d'un État étranger plutôt que d'un État non membre de l'Union européenne** (**COM-24**).

S'il est évident que les États membres de l'Union européenne partagent avec la France des valeurs et des normes qui rendent peu probables des actes d'ingérence sur un opérateur ou un prestataire de nature à susciter un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale, il est plus raisonnable et conforme à l'esprit non discriminatoire du texte que de viser tout État étranger.

4. Préciser certains éléments du texte

La commission a adopté, sur proposition du rapporteur, un amendement qui insère **le niveau de sécurité des appareils utilisés** parmi les éléments à prendre en compte par le Premier ministre pour prendre sa décision, dans la mesure où cela constitue de fait l'un des éléments – même subsidiaire – à prendre en compte, avant les modalités d'exploitation et de déploiement ou le risque d'ingérence d'un État étranger (**COM-24**). L'Anssi pourra donc analyser les éventuels défauts avérés de sécurisation des équipements, qui seraient soit identifiés dans le cadre de l'instruction soit connus *a priori*, et évaluer leur impact concret compte tenu des modalités de déploiement et d'exploitation – qui peuvent apporter des contre-mesures à de tels défauts. Si l'Anssi pourra, la plupart du temps, s'appuyer sur les éléments recueillis auprès des équipementiers dans le cadre de l'instruction de l'autorisation exigée par l'article R. 226-3 du code pénal, pour les cas résiduels ne rentrant que dans le champ d'application de la présente proposition de loi, elle a confirmé au rapporteur être en mesure de demander aux équipementiers de plus amples informations pour s'assurer de leur sécurité. Si un dispositif de certification devait être établi au niveau européen sur les équipements 5G, cela pourrait également constituer une source d'information utile à l'instruction.

Sur proposition de la commission des affaires étrangères, de la défense et des forces armées, la commission a adopté un amendement insérant les obligations des opérateurs relatives aux communications d'urgence dans la liste des obligations dont le manque de garantie pourrait motiver une décision de refus du Premier ministre sur le fondement d'un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale (**COM-8**).

Afin d'assurer une **meilleure lisibilité du dispositif**, et comme l'Autorité de régulation des communications électroniques et des postes

avait pu le suggérer dans son avis n° 2019-0161 sur ce qui était alors un amendement dans le cadre de la loi « Pacte », la commission a adopté, sur proposition du rapporteur, un amendement précisant que sont exclus les équipements dédiés exclusivement à un réseau indépendant au sens du code des postes et des communications électroniques (**COM-20**). En revanche, dès lors qu'ils seront utilisés, exclusivement ou pas, pour l'exploitation d'un réseau ouvert au public, le régime de la présente proposition de loi sera applicable.

Sur proposition de la commission des affaires étrangères, de la défense et des forces armées, la commission a adopté un amendement alignant le régime de **motivation** du texte sur celui du code des relations entre le public et l'administration (**COM-9**). Ainsi, en cas de risque d'atteinte à un secret protégé, et notamment au secret de la défense nationale, les motifs de la décision ne pourront être communiqués au demandeur.

Partant du constat selon lequel l'utilité d'inscrire dans le texte que le Premier ministre peut prendre en considération tel ou tel élément apparaît limitée, la commission, sur proposition du rapporteur et de la commission des affaires étrangères, de la défense et des forces armées, s'est assurée que le Premier ministre prendra en compte les éléments mentionnés dans le texte dans la caractérisation du risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale (**COM-10 et COM-23**).

Par ailleurs, la commission a précisé, sur proposition du rapporteur, que le dispositif prévu par la présente proposition de loi s'appliquera sur l'ensemble du territoire national (**COM-26**).

Enfin, la commission a procédé à plusieurs modifications d'ordre rédactionnel (**COM-21**, **COM-25**).

La commission a adopté l'article 1er ainsi rédigé.

Article 2
(articles L. 39-1-1 [nouveau], L. 39-6, L. 39-10 et L. 42-1 du code des postes et des communications électroniques)

Sanctions pénales

Objet : cet article punit de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de ne pas détenir d'autorisation ou de ne pas se conformer à une injonction du Premier ministre. Il prévoit également des peines complémentaires.

I. Le droit en vigueur

S'agissant du régime d'autorisation établi par l'article 226-3 du code pénal, le fait de fabriquer, importer, détenir, exposer, offrir, louer ou vendre les appareils concernés, y compris par négligence, **en l'absence d'autorisation ou sans respecter les conditions fixées par celle-ci[1],** est puni de **cinq ans d'emprisonnement et de 300 000 euros d'amende**.

S'agissant des obligations pesant sur les opérateurs de communications électroniques en application de dispositions du code, l'Arcep peut imposer les **sanctions administratives** édictées à l'article L. 36-11 du code des postes et des communications électroniques.

II. La proposition de loi initiale

L'article 2 complète le chapitre V du livre II du code des postes et des communications électroniques, relatif aux sanctions pénales applicables en matière de communications électroniques.

Il créerait un article L. 39-1-1 en vue de compléter le dispositif d'autorisation mis en place par l'article 1er par une sanction pénale.

Le fait d'exploiter les appareils sans autorisation ou de ne pas exécuter, totalement ou partiellement, une injonction du Premier ministre en la matière serait ainsi puni :

– d'**un an d'emprisonnement ;**

– et de **150 000 euros d'amende**.

---

[1] *Il punit des mêmes peines le fait de réaliser une publicité en faveur de ces appareils lorsqu'elle constitue :*
- une incitation à commettre une infraction d'atteinte à la vie privée (sur le fondement de l'article 226-1 du code pénal) ou au secret des correspondances (sur le fondement de l'article 226-15, second alinéa, du code pénal) ;
- une incitation à en faire un usage frauduleux lorsque le dispositif a pour objet la captation des données informatiques.

Les **peines complémentaires** définies par l'article L. 39-6 du code des postes et des communications électroniques seraient également applicables. Le tribunal pourrait, en conséquence, prononcer :

– la **confiscation** des matériels et installations constituant le réseau ou permettant la fourniture du service ou en ordonner la **destruction** aux frais du condamné ;

– et **l'interdiction** de trois ans maximum **d'établir** un réseau ouvert au public **ou de fournir** au public un service de communications électroniques.

Enfin, les **personnes morales** déclarées responsable pénalement du fait d'exploiter un appareil sans autorisation ou de ne pas respecter une injonction seraient exposées aux peines complémentaires suivantes :

– **l'interdiction**, pour une durée de cinq ans au plus, **d'exercer** directement ou indirectement **l'activité** professionnelle dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;

– **l'affichage de la décision** prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

III. Les modifications apportées par l'Assemblée nationale

En commission, les députés ont adopté un amendement permettant à l'Arcep de **refuser l'octroi de fréquences à un opérateur qui aurait été condamné** pour exploitation d'appareils sans autorisation ou de non-exécution partielle ou totale des injonctions, comme cela existe déjà pour les sanctions administratives infligées par l'Arcep ou pour les autres infractions pénales prévues par le code (exercice non déclaré de l'activité d'opérateur de communications électroniques, perturbations ou utilisations répréhensibles des fréquences, obstacle aux enquêtes).

En séance publique, les députés ont **augmenté**, sur proposition de Mme Laure de La Raudière, **le quantum des peines principales**, afin de les aligner sur celles applicables au titre de l'article 226-3 du code pénal. La **peine d'emprisonnement passerait d'un à cinq ans et l'amende, de 150 000 à 300 000 euros**.

IV. La position de la commission

Ces sanctions apparaissent suffisamment dissuasives tout en état proportionnées à l'objectif poursuivi.

Dans la suite de ceux insérés à l'article premier, la commission a adopté un amendement du rapporteur établissant que le **non-respect des conditions figurant dans l'autorisation** pourrait également faire l'objet des

sanctions prévues au nouvel article 39-1-1 du code des postes et des communications électroniques, sur le modèle de ce qui existe aujourd'hui à l'article 226-3 du code pénal (**COM-27**).

Enfin, la commission a précisé, également sur proposition du rapporteur, et comme à l'article premier, que le nouvel article 39-1-1 du codes des postes et des communications électroniques **s'appliquera sur l'ensemble du territoire national** (**COM-28**).

La commission a adopté l'article 2 ainsi rédigé.

Article 3

Entrée en vigueur du régime d'autorisation préalable et délai d'adoption des dispositions d'ordre réglementaire

Objet : cet article précise les conditions d'entrée en vigueur du régime d'autorisation préalable, en exigeant l'obtention d'une autorisation pour les équipements installés dès le 1er février 2019. Il fixe également un délai de deux mois au Gouvernement pour adopter les textes d'application de la proposition de loi.

I. Le droit en vigueur

Dans le cadre du régime d'autorisation prévu à l'article 226-3 du code pénal, l'article R. 226-12 prévoit que les personnes concernées par l'obligation d'être titulaire d'une autorisation au moment de l'entrée en vigueur du dispositif disposent d'un **délai de trois mois** à compter de la publication de l'arrêté listant les équipements concernés **pour déposer leur demande d'autorisation**.

II. La proposition de loi initiale

L'article 3 de la proposition de loi détermine ses conditions d'entrée en vigueur. Il prévoit qu'une autorisation sera nécessaire pour **l'exploitation d'appareils installés à compter du 1er février 2019**.

Afin de régulariser la situation des équipements déjà déployés entre le 1er février et l'entrée en vigueur des textes réglementaires d'application de la loi, l'article précise que les opérateurs qui exploitent, à la date d'entrée en vigueur de la loi, de tels équipements, **devront déposer une demande d'autorisation dans un délai de deux mois** à compter d'une date que le texte ne précise pas.

III. Les modifications apportées par l'Assemblée nationale

Les députés ont complété cet article du texte via deux principaux apports.

Le premier – issu d'un amendement du Gouvernement en commission rectifié en séance publique par un amendement du rapporteur – **précise la date à partir de laquelle courrait le délai de deux mois** pour déposer une demande d'autorisation concernant un équipement déjà installé. Il **courrait à compter de la plus tardive des dates suivantes** :

– la **publication du dernier texte réglementaire d'application** de la loi (c'est-à-dire de l'arrêté définissant la liste des appareils concernés et le

décret sur les modalités de l'autorisation et la composition du dossier de demande) ;

– la **fin du deuxième mois suivant la publication de la loi**.

Un amendement du rapporteur adopté en séance publique précise également que ce sont les équipements exploités à la date de la publication de la loi et non à la date d'entrée en vigueur de la loi qui seront concernés par l'obligation de déposer une demande dans un délai de deux mois.

Sur proposition du rapporteur, les députés ont également adopté en séance publique un amendement qui fixe le **délai de publication des textes réglementaires à deux mois à compter de la publication de la loi**.

IV. La position de la commission

Initialement étonné par l'application du texte aux équipements installés dès le 1er février 2019, le rapporteur approuve désormais la logique retenue par le Gouvernement : elle consiste à inclure dans le dispositif l'ensemble des équipements déployés dans le cadre des expérimentations actuellement en cours à partir du moment où l'intention de légiférer du Gouvernement sur ce sujet était connue. Il n'est, en effet, pas exclu que les appareils déployés dans ce cadre soient laissés en place à l'issue des expérimentations et, à terme, intégrés aux réseaux ouverts au public.

Les apports des députés apparaissent bienvenus : ils tendent à sécuriser le dispositif et à en accélérer l'entrée en vigueur, afin que les opérateurs puissent rapidement disposer d'un cadre clair pour leurs déploiements.

La commission a adopté l'article 3 sans modification.

Article 4 (nouveau)
(article 226-3 du code pénal)

Articulation des deux régimes d'autorisation

Objet : cet article fusionne le régime d'autorisation applicable aux équipements utilisés par les opérateurs de communications électroniques d'importance vitale au titre de la présente proposition de loi avec celui qui leur est déjà applicable au titre de l'article R. 226-7 du code pénal.

I. Le droit en vigueur

Bien que le droit en vigueur ait été décrit au commentaire de l'article premier, il convient de rappeler que, en pratique, les opérateurs de communications électroniques détenant ou acquérant un équipement entrant dans le champ d'application matériel de l'article 226-3 du code pénal sont soumis à l'autorisation prévue à l'article R. 226-7 du même code. Cette autorisation est distincte de celle applicable aux équipementiers, prévue à l'article R. 226-3.

La présente proposition de loi établit un nouveau régime d'autorisation dont le champ d'application – s'agissant des équipements – peut être commun à celui de l'article 226-3 du code pénal.

En conséquence, dans cette situation, les opérateurs de communications électroniques d'importance vitale pourraient se retrouver dans trois types de situations :

– lorsqu'ils détendraient un appareil entrant uniquement dans le champ de l'article 226-3 du code pénal, seule une autorisation au titre de l'article R. 226-7 du code pénal devrait être sollicitée ;

– s'ils venaient à détenir puis exploiter un appareil entrant dans le champ d'application de l'article 226-3 du code pénal et de la présente proposition de loi, ils devraient déposer une demande d'autorisation au titre de l'article R. 226-7 du code pénal et une autorisation au titre de la présente proposition de loi ;

– enfin, s'ils devaient exploiter des équipements ne relevant que du champ de la présente proposition de loi, seule l'autorisation à ce titre serait nécessaire.

Comparaison des appareils concernés par les deux régimes d'autorisation

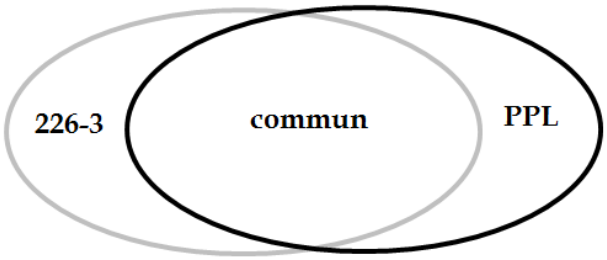
S'agissant des équipements concernés par les deux dispositifs, le **champ d'application du régime de l'article 226-3 du code pénal ne recoupe pas totalement celui de la proposition de loi**.

Comme cela a pu être décrit dans le commentaire de l'article 1er, l'article 226-3 va au-delà des équipements télécoms et concerne au premier chef les dispositifs de renseignement et d'enquête. Un équipement télécom concerné par le régime du code pénal pourrait ne pas tomber dans le champ de la proposition de loi : c'est le cas des équipements des réseaux mobiles des générations antérieures à la 5G et des réseaux fixes.

En revanche, il est peu probable qu'un équipement 5G relevant de l'article 226-3 ne soit pas également dans le champ de la proposition de loi, puisqu'un tel équipement sera forcément sensible, de sorte qu'**un champ d'application commun substantiel est à prévoir**.

Inversement, certains appareils pourraient entrer dans le champ d'application de la proposition de loi et ne pas être concernés par le régime de l'article 226-3 du code pénal. Il ira probablement ainsi des « stations de base », jusqu'à octobre 2021. Il pourrait également en aller ainsi s'agissant, selon le Gouvernement, des fonctions de *slicing* ou d'acheminement des flux vers des réseaux tiers.

Champ d'application des deux régimes d'autorisation



II. La position de la commission.

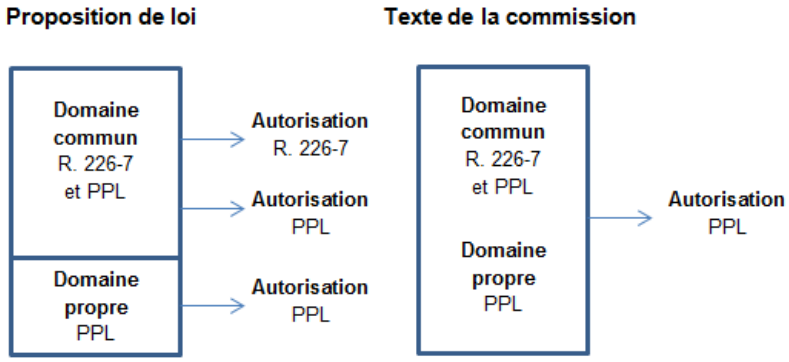
Le rapporteur estime que le manque d'articulation entre les deux régimes d'autorisation (R. 226-7 du code pénal et proposition de loi) n'est pas satisfaisant car cela exigerait des opérateurs d'importance vitale qu'ils obtiennent deux autorisations pour le même équipement lorsque celui-ci entrerait dans le champ des deux régimes.

C'est pourquoi, **en vue de simplifier le dispositif de la présente proposition de loi**, la commission a adopté un amendement proposé par le rapporteur qui **fusionne**, dans le cas d'un équipement qui entre dans le champ d'application des deux régimes, **les deux autorisations** pour ne laisser subsister que celle exigée par la proposition de loi (**COM-29, COM-7 rect. ter et COM-19 rect.**).

L'Anssi a indiqué au rapporteur qu'une telle fusion ne posera pas de difficulté dans la mesure où, la plupart du temps, l'équipement aura été analysé dans le cadre de l'article R. 226-3 et que, dans le cas inverse, elle a

confirmé au rapporteur être en mesure de demander aux équipementiers de plus amples informations pour s'assurer de la sécurité de leurs équipements.

La simplification opérée par cet amendement se résume par le schéma suivant :



La commission a adopté l'article 4 ainsi rédigé.

TRAVAUX EN COMMISSION

I. AUDITION DE MME AGNÈS PANNIER-RUNACHER, SECRÉTAIRE D'ÉTAT AUPRÈS DU MINISTRE DE L'ÉCONOMIE ET DES FINANCES – MARDI 4 JUIN 2019

Réunie le 4 avril 2019, la commission a entendu Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances, dans le cadre de l'examen de la proposition de loi n° 454 (2018-2019) 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.

Mme Sophie Primas, présidente. – Nous recevons aujourd'hui Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances, sur la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, dite « PPL 5G » ou, parfois, de façon plus médiatique, « PPL Huawei ».

Sa rédaction initiale reprenait le dispositif d'un amendement déposé par le Gouvernement au Sénat dans le cadre de l'examen en première lecture du projet de loi relatif à la croissance et la transformation des entreprises (Pacte). Suivant l'avis de la commission spéciale émis en séance par notre collègue rapporteure Élisabeth Lamure, le Sénat avait rejeté cet amendement, estimant qu'un tel sujet méritait davantage qu'un simple amendement.

Cette proposition de loi part du constat qu'il est nécessaire que le Gouvernement se dote d'un cadre juridique renforcé pour garantir la sécurité des réseaux 5G, dont l'architecture serait plus vulnérable que les précédentes générations de réseaux, et les usages, comme le véhicule connecté ou l'usine connectée, plus critiques. Il s'agit en quelque sorte du volet sécuritaire de la feuille de route du Gouvernement en matière de 5G, publiée en juillet 2018.

Cette proposition de loi crée ainsi un nouveau régime d'autorisation préalable à l'exploitation de certains équipements de réseaux mobiles, qui seraient listés par arrêté. Seuls les opérateurs de communications électroniques d'importance vitale seraient concernés. Ce régime d'autorisation qui, juridiquement, porte atteinte aux libertés économiques, se justifie par l'objectif de protection des intérêts de la défense et de la sécurité nationale.

Il s'ajoute au régime d'autorisation actuellement en vigueur, dit « régime du R. 226-3 », et qui porte sur certains équipements de télécommunications en vue de protéger le secret des correspondances et la vie privée – auquel le Sénat est particulièrement attaché.

Préservant l'économie générale du texte, les députés ont durci les sanctions, exigé la consultation de l'Autorité de régulation des communication électroniques et des postes (Arcep) sur les textes d'ordre réglementaire, et fixé au Gouvernement un délai de deux mois pour l'adoption de ces textes.

Le Gouvernement a pour objectif de rester dans la course de la 5G par un déploiement rapide des infrastructures, afin que nos entreprises puissent profiter des gains en compétitivité qui devraient en résulter, mais cette proposition de loi pourrait affecter la poursuite de cet objectif.

Avez-vous procédé, madame la ministre, à une évaluation de son impact potentiel sur le rythme des déploiements de la 5G ? La question peut également être posée pour la 4G, alors que les opérateurs se sont engagés, dans le cadre du *New Deal*, à accélérer les déploiements. En effet, même si l'esprit de la proposition de loi, pour le Gouvernement, ne concerne que la 5G, ce n'est pas le cas de sa lettre. Et quand bien même les textes réglementaires se limiteraient aux équipements strictement nécessaires à la 5G, le refus opposé à un équipement 5G pourrait entraîner la nécessité, pour un opérateur, de procéder au remplacement d'équipements 4G déjà installés. Nous commençons tout juste à rattraper notre retard sur la 4G, il serait particulièrement malvenu d'enrayer cette dynamique et de prendre le risque d'être en retard sur la 5G…

Dès juillet 2018, le Gouvernement faisait état, dans sa feuille de route, de réflexions sur la sécurité des réseaux. Alors que les opérateurs doivent être en mesure de réaliser leurs plans d'affaires pour pouvoir candidater à l'attribution des fréquences 5G, pouvez-vous nous dire quel nouveau calendrier entraîne cette proposition de loi ?

Mme Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'économie et des finances. – Je suis très heureuse de commencer l'examen au Sénat de cette proposition de loi sur le déploiement de la 5G et la sécurité de nos réseaux. C'est un sujet important pour notre économie, la qualité de nos services et notre souveraineté.

Un mot d'abord sur les grandes orientations défendues par le Gouvernement, qui n'ont pas varié depuis nos premiers échanges – à la faveur de cet amendement que vous avez jugé cavalier… La première consiste à déployer rapidement la 5G sur tout notre territoire. Nous sommes entrés dans une course mondiale au déploiement de la 5G : les premiers États qui en développeront massivement l'usage sont susceptibles de prendre une avance technologique sur les grandes innovations industrielles. Il faut donc se donner les moyens de déployer la 5G en France et, surtout, de développer les usages tant industriels que dans les services pour renforcer notre compétitivité – il ne suffit pas d'avoir la technologie, nous devons avoir l'intelligence qui va avec.

Ce déploiement doit se faire dans de bonnes conditions : c'est l'objectif de la feuille de route 5G que nous avons tracée l'été dernier. Ce déploiement doit permettre à tous les territoires d'avoir accès à la 5G et à ses usages spécifiques dans un calendrier raisonnable. Il se fera en préservant la concurrence entre opérateurs, de façon à ce que le rapport qualité-prix des offres reste compétitif, comme c'est le cas en comparaison avec nos voisins européens. Enfin, ce déploiement doit répondre aux besoins des industriels, en permettant à de nouveaux usages de se développer. Les nouveaux titulaires de fréquences devront donc y donner accès aux nouveaux fournisseurs de services que seront les prestataires de voitures connectées ou de télémédecine, en particulier dans les zones peu denses du territoire où ces services apporteront beaucoup de valeur.

Deuxième orientation : expérimenter pour accélérer l'innovation. Les industriels doivent avoir accès aux infrastructures dans de bonnes conditions, mais ils doivent aussi pouvoir expérimenter la 5G facilement. C'est pourquoi, avec l'Autorité de régulation des communications électroniques et des postes (Arcep), nous encourageons la création de bacs à sable de tests sur la 5G, c'est-à-dire de plateformes d'expérimentation sur lesquelles toute entreprise pourra tester son produit en situation réelle. Les modalités en sont simples : pendant trois ans, ces plateformes seront autorisées à utiliser des fréquences 26 GHz et les innovations pourront être testées en s'affranchissant en partie du cadre réglementaire. C'est à la faveur de ces tests que des micro-déploiements d'équipements 5G seront possibles ; nous fixons donc une date d'entrée en vigueur au 1er février, afin de traiter leur déploiement sur des réseaux ouverts. Nous sommes, avec l'Allemagne, les seuls à retenir une telle démarche, qui vise à gagner du terrain et acquérir une avance technologique. Je me permets toutefois d'indiquer à la représentation nationale – afin qu'elle pousse nos entreprises, surtout nos PME et nos entreprises de taille intermédiaire à se lancer dans des expérimentations – que l'Allemagne est plus active que nous en la matière.

Troisième orientation : préserver la sécurité de nos réseaux et de nos communications. C'est l'objectif du texte que nous examinons. La 5G va apporter de nouvelles opportunités technologiques, mais celles-ci constituent aussi de nouveaux facteurs de risques, qui vont au-delà de la confidentialité des correspondances. Il faut donc compléter notre arsenal juridique pour contrôler efficacement les équipements de réseaux 5G. Le contrôle renforcé passe par une mesure concrète : soumettre à autorisation préalable du Premier ministre l'exploitation des nouveaux équipements d'antenne mobile pour les opérateurs télécom qui sont opérateurs d'importance vitale. Ce dispositif de contrôle est fondé sur des motifs de sécurité et de défense nationale ; il permettra d'assurer le respect du principe de précaution dans le déploiement de la 5G. Il complète des dispositifs déjà en place, tel l'article R. 226 du code pénal sur la protection du secret des correspondances. La mécanique de contrôle des équipementiers et des opérateurs, elle, existe déjà : elle est exercée par l'Agence nationale de la

sécurité des systèmes d'information (Anssi), placée sous la responsabilité du Premier ministre, avec le Secrétariat général de la défense et de la sécurité nationale. Il n'est évidemment pas question de retarder le déploiement de la 5G ni de la 4G.

Quatrième orientation : ne pas discriminer les équipementiers. Tous, sans distinction, seront soumis aux mêmes règles. D'une part, car une vulnérabilité ou une faille de sécurité est rarement le propre d'un équipementier : elle peut les concerner tous. D'autre part, car les actionnariats et les stratégies de demain sont encore inconnus. Cette nouvelle protection ne doit pas retarder l'innovation et la réussite de la 5G.

Vous le voyez, les orientations du Gouvernement n'ont pas changé. Ce qui a changé depuis février en revanche, c'est la situation internationale. De nouvelles mesures de protection ont été mises en place aux États-Unis, qui peuvent avoir un impact sur le paysage concurrentiel et nos entreprises. Le 15 mai dernier en effet, un décret du Président américain a interdit l'installation d'équipements susceptibles de soulever un risque pour la sécurité des communications américaines. Concrètement, ce texte prive Huawei de la possibilité de collaborer avec des entreprises américaines et donc de se fournir en composants électroniques aux États-Unis ou d'y exporter des équipements. Cette décision pourrait avoir des conséquences – que nous sommes en train d'évaluer – sur les entreprises françaises des filières microélectronique et télécoms. Je recevrai dans les prochains jours les entreprises affectées par ces mesures, et nous travaillerons en transparence avec la représentation nationale sur ces questions.

Devons-nous faire évoluer notre position à la suite de cette décision ? Nous ne le pensons pas. Nos orientations sont mesurées ; elles protègent, sans entraver l'innovation et sans discriminer. La France ne veut pas entrer dans le jeu d'une escalade protectionniste qui nuirait à tous. Nous garderons cette position équilibrée. Nous ne sommes d'ailleurs pas seuls à avoir opté pour cette solution : l'Allemagne a récemment présenté un projet de renforcement des exigences de sécurité applicables aux opérateurs de télécommunications. Des différences techniques le séparent de notre projet, mais il suit *grosso modo* les mêmes grandes orientations : évaluer les risques plutôt qu'interdire, et renforcer les contrôles des modalités de déploiement et d'exploitation. L'Union européenne s'est également saisie de la question, en invitant les États membres à se doter de dispositifs pour répondre aux risques inhérents au déploiement de la 5G. Elle souhaite une stratégie de coordination et d'harmonisation des approches nationales, qui s'inscrit dans la ligne et le calendrier que nous avons défini à l'échelle nationale. Les règles du jeu sur la 5G sont une compétence nationale, mais il importe d'avoir un système cohérent sur l'ensemble de l'Union européenne et de protéger nos réseaux de télécommunications de manière commune.

Les orientations du gouvernement que j'ai mentionnées en introduction sur le déploiement 5G ont été transmises à l'Arcep, qui est en

train d'avancer avec les opérateurs – de les tester, en quelque sorte – sur l'écriture du cahier des charges. Cela explique peut-être un certain bruit de fond, assez classique dans ces situations. Le cahier des charges sera livré à la fin de l'été ou au début de l'automne ; nous le validerons et lancerons les enchères avec l'objectif d'attribuer les fréquences en début d'année prochaine. L'Union européenne fixe l'objectif de déploiement dans une ville d'ici 2020 ; nous souhaitons aller plus loin, pour expérimenter des usages de services plus importants, au-delà des grandes villes.

Mme Catherine Procaccia, rapporteur. – Merci, madame la ministre, d'avoir confirmé que cette proposition de loi ne comporterait pas d'éléments discriminatoires et respecterait les règles de concurrence. Merci aussi d'avoir évoqué la guerre commerciale entre les États-Unis et la Chine ; ce n'est pas la nôtre, mais elle peut en effet avoir des incidences sur le marché des composants électroniques et des équipements. Nous ne souhaitons pas nous mêler de choix diplomatiques, nous nous intéressons uniquement à l'importance de la 5G pour nos entreprises et notre compétitivité. En matière d'écoutes téléphoniques et de fuites de données, nous avons du reste peu de conseils à recevoir du pays où a éclaté l'affaire Snowden.

Nous garantissez-vous que la procédure d'octroi des autorisations ne laissera pas ouverte la possibilité de prendre, par des moyens détournés, des mesures discriminatoires ?

La présidente Sophie Primas l'a rappelé : nous n'avons pas eu de véritable débat sur ces questions dans le cadre de la loi Pacte. Nous nous réjouissons de pouvoir nous rattraper avec cette proposition de loi, mais le choix d'un tel véhicule nous prive hélas d'étude d'impact et de l'avis du Conseil d'État.

Vous travaillez en temps masqué sur les mesures réglementaires d'application. Or le champ d'application de la proposition de loi est très vaste. Comment comptez-vous associer le Parlement à la préparation de ces textes, qui devront être prêts très vite ?

Pourquoi ne pas avoir fait le choix, plutôt que d'introduire des dispositions nouvelles, d'élargir et de muscler la portée du régime d'autorisation existant à l'article R. 226 du code pénal ?

Pourquoi la proposition de loi ne vise-t-elle que les opérateurs, et non les équipementiers ? Les opérateurs ont durci le ton récemment, et vous n'avez manifestement pas encore réussi à les rassurer sur la portée du dispositif. Un point en particulier les inquiète : l'approche dite géographique que pourrait retenir l'Anssi dans l'instruction des dossiers, en vue de garantir l'hétérogénéité des équipements déployés sur chaque plaque de déploiement. Cela se comprend du point de vue de la sécurité nationale et de la sécurité des utilisateurs, mais n'est-ce pas aller trop loin ? Le respect des règles de concurrence n'est-il pas menacé ?

L'Anssi remplit actuellement ses missions dans de bonnes conditions, mais ces dispositions vont alourdir sa charge de travail, en particulier le contrôle des mises à jour. Vous avez certes précisé à l'Assemblée nationale que toutes les mises à jour n'étaient pas critiques, mais l'Anssi aura-t-elle les moyens de répondre rapidement aux demandes concernant tel équipement ou tel logiciel ?

La proposition de loi dispose que le Premier ministre pourra prendre en considération le fait que l'opérateur « est sous le contrôle ou soumis à des actes d'ingérence d'un État non membre de l'Union européenne » : cela vise un équipementier particulier… Mais tel équipementier peut toujours être racheté par un autre ! Cette disposition doit-elle évoluer pour ne pas apparaître discriminatoire ? Par parenthèse, lorsque j'ai organisé une table ronde des équipementiers et des opérateurs, tous ont demandé que l'on cesse d'appeler ce texte « PPL Huawei »…

Pouvez-vous nous assurer que la boîte à outils lancée par l'Union européenne ne vous obligera pas à venir nous présenter, dans quelques mois, des ajustements au régime que vous nous proposez aujourd'hui ?

Enfin, afin de rétablir le climat de confiance qui semble avoir disparu, seriez-vous favorable à des ajustements qui tendraient à apporter des garanties supplémentaires aux opérateurs ?

Mme Agnès Pannier-Runacher, secrétaire d'État. – Non, les autorisations ne sont pas un moyen détourné de prendre des mesures discriminatoires. Les parts de marché des équipementiers sont respectivement de 30 %, 30 % et 40 % : on peut considérer qu'il n'y a pas de discrimination aujourd'hui, et l'on ne souhaite pas qu'il y en ait demain. Cela dit, le marché va évoluer. Samsung en est pour l'instant absent, et il a décidé de faire de la 5G un axe de développement stratégique. En déplacement en Corée du Sud il y a deux semaines, j'ai constaté que Samsung était présent dans tous les premiers développements de 5G qui ont eu lieu dans le monde. Cet acteur peut aussi offrir une diversification des usages et contribuer à l'innovation. Comme Huawei, il investit massivement dans la 5G.

Les textes d'application sont effectivement en discussion avec les opérateurs. Je précise que l'amendement soumis au Parlement dans le cadre de la loi Pacte procédait aussi d'un travail conjoint avec les opérateurs. La vivacité des réactions de certains fait partie du jeu de la négociation. Pour avoir assisté au G7 numérique sur la partie 5G, je peux vous dire que ces questions sont abordées par l'ensemble des pays, qui poursuivent tous le même objectif de conciliation entre innovation rapide et recherche de garanties.

Dès qu'ils seront disponibles, les textes seront soumis à l'Arcep et à la commission supérieure du numérique et des postes (CSNP), par laquelle vous serez associés au processus. Je ne vois pas d'obstacle au partage de ces

informations. Sur ce terrain nouveau, nous gagnerions à partager l'intelligence de ces questions.

Nous n'avons pas retenu l'extension du R. 226 car le sujet est ici différent. Il ne s'agit plus seulement de confidentialité des correspondances. Dès lors que notre souveraineté est en jeu, associer les parlementaires à la décision et ne pas se limiter à des dispositions d'ordre réglementaire ne paraît pas insensé. L'article R. 226-3 du code pénal porte essentiellement sur des caractéristiques techniques sans évoquer les modalités de déploiement des équipements retenues par les opérateurs. Chacun joue son rôle : les équipementiers mettent à disposition les équipements ; les opérateurs choisissent le mode de déploiement, choisissent de développer les compétences en interne ou de s'appuyer sur des compétences externes pour la maintenance et les mises à jour, et choisissent de conduire leurs propres contrôles de sécurité. Il est important que les opérateurs s'emparent de la question de leur propre résilience sur le réseau. Nous avons donc un système à plusieurs étages : les équipements sont autorisés au moyen du R. 226-7 ; les opérateurs bénéficient de la validation préalable des équipements par l'Anssi, et doivent expliquer les modalités de leur maintien – quand, comment, intervention ou non de sous-traitants…

Vous évoquez la question géographique. Chaque opérateur a six ou sept plaques géographiques sur lesquelles il dispose d'une unité d'équipementiers. Certains, comme Free, n'ont qu'un seul équipementier ; d'autres en ont deux, de manière à conserver un peu de concurrence dans leur propre stratégie achat. Je ne crois pas qu'il appartienne à l'Anssi de définir la politique achat des opérateurs télécom, ce que l'agence reconnaît d'ailleurs.

L'Anssi recevra en effet un surcroît de travail. Mais l'agence, qui compte 570 collaborateurs, vient d'en recruter quarante : c'est un signal considérable de soutien qui lui est adressé dans le contexte actuel, alors que d'autres services, comme la direction générale des entreprises ou celle de la concurrence, de la consommation et de la répression des fraudes, perdent des effectifs.

Nous mentionnons des pays qui n'appartiennent pas à l'Union européenne car nous réalisons le travail de coordination entre pays européens que j'évoquais à l'instant. Mais au fond, l'origine des équipementiers est assez indifférente. La vraie question est celle des pays qui prévoient des lois ayant des dimensions d'extraterritorialité ou permettant une immixtion dans la gestion. Deux exemples viennent facilement à l'esprit – si Cisco n'est pas un fournisseur immédiat, il fait partie du paysage : la législation chinoise oblige depuis 2017 ses opérateurs à communiquer des données par tout moyen technologique ; le droit américain autorise le Président à prendre des décrets, ou *executive orders,* qui ont un impact sur l'ensemble des pays, comme l'a montré l'exemple du décret en date du 15 mai dernier. Les autorisations délivrées par le Gouvernement ne se

contenteront pas de dire oui ou non, elles préciseront pour quoi faire, dans quel ressort géographique, selon quelles modalités de déploiement et de contrôle, et pour une durée maximale de huit ans.

L'Union européenne a indiqué qu'il s'agissait d'une compétence nationale. Nous n'attendons donc aucun ajustement législatif. En revanche, nous partagerons avec les autres États membres les bonnes pratiques et les informations, y compris sur la sécurité des équipements.

Pour restaurer le climat de confiance, je recommande de laisser les négociations se poursuivre. Nous maintenons un juste équilibre entre le souci de sécurité et celui d'être armé pour les années à venir. Ne connaissant pas les risques auxquels nous serons exposés, nous proposons un dispositif législatif laissant de la latitude au pouvoir réglementaire. Une garantie est également donnée par notre engagement de déploiement de la 4G – le *New Deal* – et de la 5G – dont nous faisons un élément important de notre compétitivité. Si je rends visite à Samsung, c'est aussi pour anticiper toute forme de coopération avec les leaders mondiaux, quelle que soit leur nationalité, et comprendre leur stratégie.

M. Alain Duran. – Au-delà des questions de sécurité et de souveraineté numérique, je souhaiterais revenir sur un point plus concret pour le quotidien de nos administrés : la télémédecine, pour laquelle la 5G pourrait être une véritable révolution. Nous examinons d'ailleurs en ce moment en séance publique le projet de loi relatif à l'organisation de notre système de santé. La télémédecine pourrait être une réponse pragmatique et efficace à la déprise médicale qui frappe un nombre important de nos territoires – surtout ruraux. Encore faudrait-il que les infrastructures puissent absorber de telles évolutions. Dans l'Ariège, selon l'Arcep, 93 % des bâtiments sont couverts par la 4G mais le débit internet n'est supérieur à 500 Mbit/s que dans 3,2 % des foyers, contre 48 % à Paris !

Afin de ne pas renouveler les erreurs commises dans le passé, quelles dispositions entendez-vous prendre afin de veiller à une couverture homogène et sans zone blanche de l'ensemble du territoire national en 5G, compte tenu de ce problème d'infrastructures, mais aussi de ce régime d'autorisation préalable ? Le délai de huit ans est-il le plus indiqué pour donner de la lisibilité aux opérateurs, qui ont de lourds investissements à réaliser ?

Mme Élisabeth Lamure. – Nous avions en quelque sorte rendez-vous, madame la ministre, depuis la loi Pacte… Je rappelle que l'amendement du Gouvernement a été repoussé pour des questions de méthode, compte tenu de la précipitation avec laquelle il avait été déposé, non en raison de son contenu. Le fait d'avoir choisi une proposition de loi nous prive de l'étude d'impact attachée aux projets de loi, hélas car, même lacunaires, ces études servent nos analyses. Votre choix de procéder par

proposition de loi est-il guidé seulement par le souci de la rapidité, alors que quatre mois se sont écoulés depuis l'examen de la loi Pacte ?

Je suis étonnée de la rétroactivité de la mesure. Y aura-t-il des conséquences financières pour les équipementiers et les opérateurs – du démontage de matériel, par exemple ? Je serais étonnée que le délai de déploiement – de la 4G – n'en soit pas retardé.

Mme Patricia Morhet-Richaud. – Les nouvelles perspectives que permettra la nouvelle génération de communication 5G sont très diverses et concerneront de nombreux secteurs : la santé, l'agriculture, l'industrie, la mobilité, etc. Nous devons relever l'énorme défi du numérique si nous voulons exister sur la scène internationale. L'intelligence artificielle est également une ambition nationale et, pour mener à bien cette stratégie, tous les acteurs doivent être mobilisés. S'il est bien entendu nécessaire de sécuriser les parties sensibles du réseau et de se protéger du risque d'exploitation malveillante ou criminelle, il est aussi nécessaire de s'engager au plus tôt dans le déploiement de la 5G. Les délais prévus à l'article 3 de cette proposition de loi peuvent-ils être revus à la baisse ? Qui aujourd'hui est chargé de piloter la mise en œuvre de la stratégie pour l'intelligence artificielle en France ? Le Gouvernement a-t-il lancé des démarches pour mobiliser les acteurs économiques dans la normalisation de l'intelligence artificielle ?

Mme Viviane Artigalas. – Nous comprenons tous l'importance du déploiement rapide de la 5G pour la compétitivité de nos entreprises et le développement de nos territoires – ruraux en particulier. Une étude d'impact nous aurait servi, il est vrai. Le modèle économique de la 5G n'est pas stabilisé. L'expérimentation que vous proposez permettra-t-elle de mieux l'anticiper, et d'affiner le coût pour les opérateurs ? Ceux-ci ont déjà pris pour la 4G des engagements avec les équipementiers qui pourraient servir pour la 5G, sauf si des mesures de sécurité les poussaient à en changer… Cette proposition de loi n'augmentera-t-elle pas les coûts, retardant ainsi le développement de la 5G ?

La 5G est essentiellement fondée sur des logiciels impliquant des mises à jour régulières qui, avec ce texte, ne seraient pas toutes soumises à autorisation. Or nous savons que les évolutions technologiques seront importantes. L'autorisation de huit ans, qui vaut aussi pour les logiciels, est-elle dès lors judicieuse ?

M. Xavier Iacovelli. – Il est devenu clair que les opérateurs nationaux n'étaient pas de fervents soutiens de cette proposition de loi, qui, selon eux, introduit une planification excessive du marché au regard de son objectif officieux – la lutte contre la domination du géant chinois de la 5G. Au-delà de la méthode, cet objectif peut faire débat, puisque le Président de la République avait affirmé ne pas vouloir combattre directement Huawei. Plutôt que la coercition des opérateurs, ne devrions-nous pas chercher à

favoriser les équipementiers européens – les deux grands étant le suédois Ericsson et le finlandais Nokia ? Une telle stratégie économique serait cohérente avec la volonté affichée par la France de s'appuyer sur les autres pays et entreprises européens, voire de créer un géant européen afin d'affronter la concurrence internationale et les rivalités stratégiques.

Une telle volonté n'est bien entendu pas incompatible avec la création de mécanismes de contrôle tels que celui mis en place par cette proposition de loi. Pensez-vous qu'il soit possible, dans le cadre des négociations en cours avec les opérateurs nationaux, de proposer une telle politique ? Le système issu de ce texte favorisera à terme des équipementiers européens ; quel est votre sentiment sur l'idée d'un système alliant bâton et carotte ?

Mme Anne-Catherine Loisier. – En raison des exigences de sécurité renforcées sur la 5G, les services de police et de justice pourraient ne plus avoir accès à certaines données, du fait de l'adoption des techniques de chiffrement de bout en bout. En définitive, la 5G ne serait-elle pas plus poreuse, plus vulnérable que les générations précédentes ?

Le Gouvernement a indiqué vouloir valoriser au mieux le patrimoine de l'État – objectif que nous partageons tous. Cela signifie-t-il la fin d'une logique du *New Deal*, qui privilégie les déploiements sur tout le territoire aux recettes de l'État ?

M. Fabien Gay. – Nous sommes tous d'accord sur la nécessité de déployer la 5G pour notre politique industrielle et le développement de notre territoire, mais je m'étonne que nous parlions d'une proposition de loi déposée par le groupe La République en Marche plutôt que d'un projet de loi. Nous n'analysons ici le sujet que sous l'angle de la sécurité. Or nous aurions eu besoin d'un projet de loi abordant tous les autres aspects ! Par exemple, le fait que le territoire n'est pas même totalement couvert par la 4G, et les territoires ruraux ne sont pas les seuls exclus : ma rue, en Seine-Saint-Denis, est aussi concernée ! Ne craignez-vous pas que les inégalités numériques s'accroissent ? Il n'y a rien non plus dans le texte sur les hautes fréquences et la santé publique ; rien sur la sécurité des consommateurs ; rien sur la protection de l'environnement, alors que les *data centers* sont très énergivores.

Comment pensez-vous rattraper notre faiblesse industrielle, notamment sur les opérateurs, alors que votre gouvernement prône un retrait de l'État interventionniste ? Je regrette notamment, comme peut-être un certain nombre de mes collègues, qu'on ait démantelé Alcatel, qui aurait servi une vision à long terme dans le déploiement de la 5G.

Mme Agnès Pannier-Runacher, secrétaire d'État. – Oui, madame Lamure, la rapidité d'adoption de ces dispositions est un objectif, car nous devons être équipés et faire savoir les règles du jeu aux opérateurs. Or, tant

qu'elles n'ont pas été arrêtées par la représentation nationale, elles sont réputées pouvoir évoluer…

Réaliser une étude d'impact sur cette question aurait été un exercice particulièrement difficile. Nous parlons de quelque chose qui n'existe pas, puisque la 5G dite « *stand alone* » sera lancée en 2021 et probablement déployée en 2022 ! Nous ignorons donc quels usages précis nous pourrons en faire et à plus forte raison ceux qui s'imposeront demain. Il nous faut donc le maximum de retours d'expériences des tentatives de connecter de nombreux objets ensemble dans une usine, un hôpital, une *smart city*…

En matière de télémédecine, distinguons la 4G+, c'est-à-dire la 4G de qualité, du très haut débit ou du très très haut débit : ceux-ci peuvent apporter une réponse aux problèmes des déserts médicaux et de la démographie médicale par la consultation à distance, celle-là pourra peut-être suffire pour la lecture de certains examens. La chirurgie à distance, par exemple, exigera probablement la 5G. Le premier niveau de télémédecine exige d'abord que la 4G soit déployée : c'est tout l'enjeu du *New Deal*. Si ce Gouvernement a bien une caractéristique, c'est cet engagement au service de la cohésion des territoires, porté de façon quasi militante par Julien Denormandie, Cédric O, Jacqueline Gourault et moi-même. Nous sommes convaincus qu'il y a là un moyen évident de réduire les fractures territoriales. En deux ans, nous avons réalisé l'équivalent de cinq années de déploiement ! Les efforts ont également été intensifiés sur la couverture mobile. Et je ne parle pas d'une barre au fond du jardin, mais d'une 4G de bon niveau ; nous avons revu en conséquence les critères d'appréciation de la couverture.

La durée de huit ans est plus longue que celle des autorisations régies par l'article R. 226, et plus élevée que celle des amortissements des équipements : elle est donc appropriée. Madame Artigalas, plusieurs versions des logiciels seront disponibles successivement : seules les transformations majeures feront l'objet d'une nouvelle autorisation.

Oui, madame Morhet-Richaud, il y a une stratégie sur l'intelligence artificielle, portée par le ministère de l'économie et en particulier Cédric O, qui a l'avantage d'avoir piloté cette stratégie dans ses anciennes fonctions et a une conviction forte quant à l'importance de la déployer.

Les deux premiers défis technologiques du fonds d'investissement pour l'innovation et l'industrie concernent l'intelligence artificielle et plus précisément l'audit des algorithmes et l'utilisation de l'intelligence artificielle dans le diagnostic médical. La direction générale des entreprises porte un plan spécifique. C'est aussi un sujet majeur pour l'Union européenne – vous avez certainement entendu parler, outre l'intelligence artificielle, de la batterie électrique ou de la nanoélectronique parmi les chaînes de valeur stratégiques portées à ce niveau. Pour gagner ces batailles, il faut rassembler les forces européennes.

Monsieur Iacovelli, cette proposition de loi n'exerce aucune forme de coercition sur les opérateurs. D'un côté, les équipementiers doivent toujours se soumettre aux autorisations prévues à l'article R. 226 du code pénal. De l'autre, les opérateurs de télécom, qui gèrent des infrastructures vitales, ont à ce titre des responsabilités, qu'ils ont l'habitude d'assumer. Collectivement, nous augmentons le niveau de jeu parce que nous estimons que la technique l'impose. Stratégiquement, c'est aussi l'intérêt des opérateurs que de disposer de cette capacité à analyser leur résilience et d'internaliser des compétences technologiques pour pouvoir auditer et comprendre leurs sous-traitants, le codage des équipements qui leur sont livrés et les offres.

L'interopérabilité n'est pas la priorité des départements de recherche et développement des équipementiers, or elle est possible. Il faut être capable, tant en stratégie d'achat qu'en stratégie technologique, de demander des comptes à ses équipementiers. Vous connaissez l'histoire du traitement de texte, qui a bien fini par fonctionner tant sur PC que sur Mac. Le sujet a été évoqué à Barcelone. Nous devons pouvoir avancer.

Il faut accompagner les entreprises dans la 5G. Je verrai le patron d'Ericsson vendredi et je rencontrerai les responsables de Nokia bientôt. Nous sommes à leurs côtés pour qu'ils investissent plus. Nous étudions ce qui se passe au grand international et sommes aux aguets en matière de veille technologique. Il est intéressant de se positionner par rapport à ceux qui investissent le plus. Ce n'est pas nous qui menons la stratégie des entreprises privées, mais nous sommes capables de les accompagner, de les pousser, d'avoir éventuellement des projets d'innovation. C'est ensemble que cela se joue.

La 5G n'est pas plus poreuse que les générations précédentes, ce sont les usages qui diffèrent. Voir ses communications et ses données interceptées, c'est désagréable ; si, demain, l'opération conduite par un robot s'arrête au milieu ou si quelqu'un d'extérieur prend la main sur l'usine ou sur les voitures autonomes, les conséquences seront d'une autre nature.

La compatibilité entre la 5G et les interceptions légales est une préoccupation de certains services. Toutefois, je rappelle que les opérateurs sont assujettis à des obligations légales en la matière, y compris pour la 5G. L'État participe directement à la normalisation sur ce point – la direction générale des entreprises est encore une fois à la manœuvre. Un plan d'action spécifique à la 5G est mis en œuvre en lien avec l'ensemble des intervenants publics pour garantir la poursuite de ces activités essentielles à la sécurité nationale.

Ce n'est pas la fin du *New Deal*, qui est en œuvre ici et maintenant et doit être livré jusqu'au bout. Je le répète, la 5G porte sur des usages différents. La bande de fréquence mise aux enchères est à ondes courtes. La 5G est optimale pour traiter massivement des données à un point précis,

dans une zone industrielle ou un centre hospitalier par exemple, mais pas entre deux points d'un territoire rural, sauf s'il y a, dans ce territoire rural, un endroit où l'on traite beaucoup de données, par exemple à travers une plateforme de services. Il faut absolument comprendre quels sont les *business models* concernés. Ce sera beaucoup de *business to business*. Même si tout le monde aura le plaisir de profiter de la 5G, elle correspondra à des *business models* de gestionnaires d'infrastructures, des gestionnaires de services ou des responsables industriels qui auront besoin d'une grande puissance de feu pour pouvoir développer un produit, être plus rapide, traiter des données en temps réel.

Il n'est pas question d'approfondir une quelconque fracture numérique. J'appartiens au Gouvernement qui s'est le plus emparé de ce sujet, qu'il s'agisse des équipements ou de l'illectronisme.

L'Agence nationale des fréquences (ANFR) procède à toutes les mesures d'ondes et l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) est saisie de l'impact sur l'environnement et la santé humaine. La technologie de la 5G, ce sont des ondes concentrées qui ne se diffusent pas dans l'atmosphère et n'entraînent pas non plus d'effet micro-ondes. Nous avons mis en place un comité, à la suite de la loi « Abeille », pour échanger avec les usagers. Nous prenons très au sérieux ce sujet sensible. J'ai constaté qu'une petite polémique avait émergé lorsque Bruxelles avait gelé son expérimentation à cause de bisbilles entre deux autorités. Certains ont dit que Bruxelles arrêtait de déployer la 5G en raison de risques sur la santé, or cela n'avait rien à voir. La 5G, comme toute nouveauté, inquiète. Bien malin celui qui peut dire aujourd'hui quel impact elle aura dans cinquante ans sur les personnes exposées. C'est pourquoi nous prenons très au sérieux ce dispositif et sommes très transparents sur nos mesures et les études menées, avec l'ANFR, l'Anses et le comité « Abeille ».

Mme Sophie Primas, présidente. – Dans le cadre du dispositif d'application imaginé, le silence de l'administration vaudra-t-il rejet à l'issue d'un délai de deux mois ?

Mme Agnès Pannier-Runacher, secrétaire d'État. – Oui. Je vous le confirme.

Mme Sophie Primas, présidente. – J'ai été saisie aujourd'hui même par l'entreprise Huawei. Nous serons attentifs aux conséquences sur l'industrie française de la décision américaine concernant la 5G.

Mme Agnès Pannier-Runacher, secrétaire d'État. – Les conséquences de la décision américaine seront plus grandes que celles de cette petite proposition de loi !

Mme Sophie Primas, présidente. – En effet. Nous vous remercions. Je voudrais conclure par un clin d'œil un peu perfide : je salue votre volonté de co-construire le cahier des charges avec les opérateurs. Si vous aviez fait

la même chose sur Aéroports de Paris, vous auriez eu moins de difficultés au Sénat !

II. EXAMEN DU RAPPORT – MERCREDI 19 JUIN 2019

Réunie le mercredi 19 juin 2019, la commission a examiné le rapport et le texte sur la proposition de loi n° 454 (2018-2019), adoptée par l'Assemblée nationale, 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.

Mme Catherine Procaccia, rapporteur. – Avant d'évoquer 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, dite « PPL 5G », je souhaite brièvement revenir sur ce qu'est la 5G. La cinquième génération de standards de télécommunications mobiles est souvent désignée comme une rupture technologique. Elle apportera en effet un changement d'échelle dans les capacités des réseaux - débits multipliés par dix, temps de latence divisés par dix, etc. - et surtout, elle promet le développement de nouveaux usages critiques pour la vie économique d'un pays, usine du futur, véhicule connecté, ville connectée,internet des objets… Une véritable course à la 5G est engagée dans le monde entier car il y va de la compétitivité de nos opérateurs et de nos entreprises. Il faut cependant avoir à l'esprit que la véritable 5G, qui permettra ces nouveaux usages – la 5G dite *stand alone* – ne sera pas disponible avant 2021 ou 2022.

La proposition de loi instaure un régime d'autorisation préalable à l'exploitation, par les opérateurs télécoms, des équipements des réseaux mobiles. Elle confère ainsi le moyen au Premier ministre de protéger les intérêts de la défense et de la sécurité nationale. Elle se distingue d'un autre régime d'autorisation actuellement en vigueur en application de l'article 226-3 du code pénal d'abord en ce qu'elle est centrée sur l'exploitation des équipements, alors que le régime du code pénal est focalisé sur les équipements, ensuite en ce qu'elle vise à protéger les intérêts de la défense et de la sécurité nationale alors que le régime du code pénal entend éviter les atteintes au secret des correspondances et à la vie privée. Enfin, elle ne concerne que les opérateurs télécoms d'importance vitale ; le régime actuel d'autorisation inscrit dans le code pénal concerne à la fois les équipementiers – qui fabriquent les équipements – et les opérateurs télécoms – qui les utilisent.

La nouvelle autorisation préalable vise à garantir la sécurité des réseaux 5G. Selon le Gouvernement, ceux-ci sont porteurs de nouvelles vulnérabilités qui exigent d'analyser la sécurité du réseau dans son ensemble, au-delà de la seule qualité des équipements utilisés. Or, le

Gouvernement estime que ces nouvelles vulnérabilités ne peuvent être tolérées en raison du caractère particulièrement critique des usages promis par la 5G – car la véritable rupture de la 5G proviendra de ses usages. On imagine l'ampleur des conséquences en cas de panne ou de piratage d'un réseau organisant la circulation des véhicules connectés…

Tous les pays du monde réfléchissent actuellement à cette question de la sécurité de la 5G. Certains pensent avoir trouvé la solution en interdisant l'équipementier chinois. Ce n'est pas l'orientation du Gouvernement, et c'est heureux. Je l'ai déjà dit : nous n'avons pas à participer à une guerre commerciale qui n'est pas la nôtre et qui voudrait réduire l'Europe à un simple théâtre d'opérations.

Un mot de l'état d'esprit dans lequel j'ai travaillé : ce texte doit permettre à l'État de protéger la sécurité nationale, sans obstruer les déploiements de la 5G ni obérer la concurrence entre les fournisseurs des opérateurs.

Je partage les deux objectifs poursuivi par le Gouvernement. Car il ne faut pas rater le virage de la 5G : la compétitivité à moyen terme de nos opérateurs et de notre économie en dépend.

Sur le fond, la sécurité des réseaux 5G doit être garantie tant pour des raisons de sécurité que pour des raisons économiques : les acteurs économiques qui bénéficieront des nouveaux usages doivent pouvoir avoir confiance en la sécurité des réseaux.

Sur la forme, dans le calendrier retenu, la France serait l'un des premiers pays à se doter d'un cadre juridique clair tendant à garantir la sécurité des réseaux 5G. Je regrette seulement la méthode utilisée par le Gouvernement : une tentative de « passage en force » lors de la loi Pacte, puis le choix d'un véhicule législatif privant les débats d'étude d'impact et d'avis du Conseil d'État. L'exigence de célérité ne doit pas se faire au détriment de la qualité de la loi, surtout lorsqu'elle est à ce point structurante pour les années à venir.

Je partage les objectifs du Gouvernement. Mais je souhaite aussi éviter une sortie de route dans le virage de la 5G : c'est la préoccupation qui m'a guidée. Cette nouvelle autorisation administrative ne doit pas mettre en péril la rapidité des déploiements, ni en augmenter le coût. Elle ne doit pas avoir pour conséquence une dégradation du service rendu aux usagers, aujourd'hui avec la 4G ou dans le futur. Évitons de sombrer dans le tout sécuritaire et assurons-nous de la proportionnalité du dispositif.

Je vous proposerai des amendements en ce sens, qui pourraient, pour la plupart, se résumer en trois mots : rééquilibrer, simplifier, préciser. Rééquilibrer le texte en encadrant davantage les motifs de refus du Premier ministre et en lui permettant d'autoriser sous conditions : je préfère un « oui mais » à une approche binaire du type « oui ou non ». Je souhaite également m'assurer que l'État ne dictera pas aux opérateurs leur politique d'achat.

Simplifier en fusionnant les procédures d'autorisation applicables aux opérateurs. Et enfin préciser, en particulier indiquer clairement que le dispositif se limite aux équipements 5G.

Mme Sophie Primas. – Merci de cette précision d'analyse et de cette concision !

Mme Viviane Artigalas. – Ce rapport équilibré tient compte des divers enjeux, sécurité, économie, usages personnels. Le sujet aurait mérité plus de discussions : c'est un débat de société ! La 5G ouvre des perspectives intéressantes, mais nous devons nous interroger sur la société dans laquelle nous vivrons dans quelques années. D'abord un amendement à la loi Pacte, ensuite un texte sans étude d'impact ni avis du Conseil d'État : moi aussi je regrette la forme. À nous d'être vigilants. Nous ignorons quels nouveaux usages émergeront, nous manquons de visibilité économique et sociale car le modèle de la 5G n'est pas stabilisé. Nous ne devons pas retarder le déploiement dans les territoires ruraux. Cependant, en tant que parlementaires, nous devons être très vigilants sur la sécurité de l'État, de nos entrepriseset de nos concitoyens… Nous devrons inévitablement y revenir ! C'est pourquoi il conviendra de prévoir une évaluation sans trop tarder.

Mme Élisabeth Lamure. – Notre collègue rapporteur nous propose la voie de la sagesse et de la simplicité, sur un sujet complexe techniquement. Nous avions dénoncé l'absence d'étude d'impact, mais les auditions et le rapport nous fournissent des éléments de réflexion. Nous aurions pris beaucoup de risques à adopter un simple amendement du Gouvernement en discussion de la loi Pacte.

Je m'interroge sur la rétroactivité au 1er février, souhaitée par le Gouvernement. Elle poserait sans doute problème aux opérateurs concernés. Sera-t-elle maintenue ?

Enfin, il est question de la 5G mais qu'en est-il de la 4G et des équipements existants, si les équipementiers ne reçoivent pas du Premier ministre l'autorisation prévue ?

M. Daniel Gremillet. – La 5G pourrait susciter dans les territoires peu favorisés bien des espoirs, concernant l'aménagement du territoire, les déplacements, les créations d'emplois… Nous qui, dans le Grand Est, avons décidé d'apporter la fibre optique jusque chaque habitation, nous le savons bien : ce n'est pas parce qu'elle sera disponible que la 5G sera utilisée. Le phénomène d'exclusion est devant nous… Il y a aussi des enjeux financiers. Des transferts de compétences sont à prévoir, aux dépens du contribuable local. Là encore, nous en avons fait l'expérience : nous avons négocié avec l'Office national des forêts des redevances pour le passage de la fibre optique dans le domaine forestier…

Mme Anne-Catherine Loisier. – Je salue le travail de notre rapporteur sur ce sujet complexe et en perpétuelle évolution. Je partage le propos de Viviane Artigalas, une veille constante s'impose.

Les auditions ont montré combien la sécurisation des réseaux est un travail complexe. Il sera confié à l'Agence nationale de la sécurité des systèmes d'information (Anssi). Celle-ci est-elle dimensionnée, cependant, pour cette charge supplémentaire ?

M. Franck Montaugé. – Je félicite Mme le rapporteur. La question économique est importante. Mais la dimension liée à la défense nationale et à la sécurité est au cœur de ce texte. Ne soyons pas naïfs et songeons à tout ce que permettra la 5G : les forces de sécurité et de cyber défense doivent pouvoir utiliser le réseau civil de 5G, qui est d'une complexité folle. Des garde-fous s'imposent, l'autorisation préalable adossée à une certification des équipements constitue un bon compromis, on n'oblige pas les opérateurs à prendre des fournisseurs sur une liste prédéfinie. Les questions de défense et de sécurité concernent tous nos concitoyens et les opérateurs ne sont pas dispensés de prendre en compte ces impératifs dans leur mode de fonctionnement !

Ce texte est un bon compromis et, assorti sans doute de quelques amendements, il répondra aux attentes des forces de sécurité et de défense.

M. Pierre Louault. – Les technologies et les logiciels évoluent à très grande vitesse. La législation doit à la fois protéger les données des citoyens et les systèmes de transmission : c'est une gageure dans un domaine international, ouvert.

Les intérêts de la défense nationale, ceux de nos entreprises, doivent être protégés. Il y a urgence, car les opérateurs sont maintenus dans un immobilisme qu'ils estiment de plus en plus grave : si une feuille de route n'est pas décidée rapidement, le retard se creusera et sera pour notre pays de plus en plus difficile à rattraper.

M. Laurent Duplomb. – Merci pour ce rapport. Je me bornerai à une question : en cas de problème, y a-t-il un plan ? Combien de temps sera nécessaire pour réparer une panne ? Je m'interroge au regard des délais de réparation des pannes qu'on peut actuellement observer… Quand la grande vitesse d'exécution sera devenue indispensable pour les démarches administratives ou la vie économique, quand tout sera connecté, tout dysfonctionnement pourrait avoir des effets redoutables, s'il dure : un plan de maintenance des lignes et des serveurs sera-t-il en place pour y faire face très rapidement ?

M. Jean-Pierre Moga. – Je félicite à mon tour Mme le rapporteur. Une question sur les risques pour la santé : soixante-dix chercheurs avaient l'an dernier demandé un moratoire au déploiement de la 5G et tiré la sonnette d'alarme sur les effets nocifs pour la santé ; deux cent quarante scientifiques en ont demandé le report. Où en est-on ? Certains affirment à

l'inverse que les ondes 5G pénètrent moins profondément que d'autres ondes magnétiques. En vingt-cinq ans d'utilisation constante des téléphones portables, on n'a observé aucune hausse des tumeurs du cerveau. Ici, dispose-t-on d'études ? Des questions sont posées dans la société.

Mme Anne Chain-Larché. – Ma question porte sur les emplois. L'installation de la fibre a déjà suscité des besoins de formation. Cette proposition de loi est très ambitieuse et la 5G est très certainement porteuse de développement économique dans les territoires. A-t-on mesuré l'impact pour les emplois et les besoins de formation ?

M. Pascal Allizard, rapporteur pour avis de la commission des affaires étrangères. – La commission des affaires étrangères, de la défense et des forces armées a examiné la proposition de loi le 12 juin dernier. Le texte nous paraît strictement suffisant pour assurer la protection des intérêts de la défense et de la sécurité nationale. Il paraît équilibré et pourra faire l'objet d'une application souple, conciliant divers critères d'appréciation du risque, assortissant l'autorisation de conditions d'exploitation, modulant sa durée. Une évaluation de l'application sera nécessaire, notamment au regard de l'évolution des usages et du développement des technologies, afin de garantir la pérennité dans le temps de cette protection. Car on ne mesure pas où tout cela peut nous mener…

Sous réserve de ces observations et des trois amendements techniques, la commission de la défense et des forces armées est favorable à l'adoption de la proposition de loi.

Mme Catherine Procaccia, rapporteur. – Les futurs usages ne sont pas encore connus. Le véritable déploiement de la 5G aura lieu en 2021 ou 2022 : une évaluation pourra alors être conduite… Le passage à la 5G est important pour la vitalité économique – refuser la 5G par crainte des futurs usages, ce serait un peu comme en rester au minitel !

La santé n'est pas comprise dans le périmètre de ce texte. Soit dit en passant, la même inquiétude se renouvelle à chaque apparition d'une nouvelle technologie ! On s'est moins inquiété de la généralisation des micro-ondes…

Merci à Mme Lamure d'avoir avec sagesse refusé un amendement à la loi Pacte : M. Allizard et moi avons entendu un certain nombre de personnes en audition et nous avons aujourd'hui du sujet une vision plus complète qu'au mois de février dernier – comme d'ailleurs probablement les opérateurs et même le Gouvernement. J'espère que ce dernier sera ouvert à nos propositions. Je reviendrai lors de l'examen des amendements sur la question de la rétroactivité.

S'agissant de la question des transferts de compétences et des charges financières qui les accompagnent : ces enjeux existent, mais ne sont pas non plus réellement l'objet du texte. Quoi qu'il en soit je précise que le

déploiement de la 5G doit se faire partout sur le territoire – et pas au détriment de la 4G.

Je remercie la présidente qui m'a confié ce rapport, sur un sujet passionnant et qui n'est pas aussi complexe que je le croyais initialement. L'Anssi estime que ses moyens sont proportionnés à cette nouvelle mission : 30 recrutements ont eu lieu récemment, d'autres suivront. Il ne semble pas y avoir de souci…

Monsieur Montaugé, nos collègues de la commission des affaires étrangères estiment que la défense nationale, la sécurité, les intérêts économiques sont ici bien protégés.

Nous en sommes à la phase d'expérimentation, les questions d'emploi et de formation ne se posent pas encore et l'impact de la 5G n'a pas pu être encore mesuré, mais je ne suis pas certaine qu'il serait très différent de ce qu'on a pu observer avec d'autres technologies nouvelles.

Avant d'en venir aux amendements, je voudrais indiquer que pour apprécier la recevabilité des amendements au regard de l'article 45 de la Constitution, autrement dit le lien des amendements avec le texte, j'ai considéré qu'entraient dans le champ de la proposition de loi les dispositions 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.

Article 1er

Mme Catherine Procaccia, rapporteur. – Mon propos sera un peu long sur les premiers amendements, COM-20, COM-1 rectifié *bis* et COM-11.

Mon amendement COM-20 restreint le champ d'application en faisant explicitement référence aux réseaux de cinquième génération et des éventuelles générations ultérieures ; il aligne la terminologie avec l'alinéa 10 et ajoute une précision. La restriction que j'ai mentionnée se retrouve dans les amendements COM-1 rectifié *bis* et COM-11. Ils réduisent également le champ du texte aux équipements à risque, dans une logique de proportionnalité, ce à quoi je suis favorable.

En revanche, je suis défavorable à une extension aux équipementiers. Cette proposition est *a priori* séduisante, mais elle brouillerait la logique du texte, car le régime d'autorisation porte sur l'exploitation des équipements, non sur les équipements en eux-mêmes. En outre, le régime instauré repose sur des obligations de sécurité imposées aux opérateurs, qui sont différentes de celles imposées aux équipementiers. Enfin et surtout, cette proposition d'extension va de pair avec une fusion de l'autorisation créée avec celle déjà existante dans le code pénal. Si une telle fusion est souhaitable pour les opérateurs concernés par la proposition de loi – c'est l'objet d'un amendement que je vous proposerai – elle ne l'est pas pour les équipementiers. En effet, dans le cadre du régime du code pénal

relatif aux équipements permettant des interceptions de sécurité, l'analyse des équipements est confiée à une commission consultative et le délai réglementaire pour l'instruction des dossiers est de neuf mois. Le régime prévu dans le texte ne comporte aucune consultation et le délai réglementaire d'instruction des dossiers sera, selon le Gouvernement, de deux mois. N'allons pas rendre le nouveau régime incompréhensible, ne vidons pas de son utilité l'autorisation existante. Pourquoi défaire cet article 226-3 qui fonctionne bien ?

Je propose donc aux auteurs des deux amendements identiques de rectifier ceux-ci en conservant seulement la mention de la 5G et des générations ultérieures, et la restriction du champ d'application aux équipements à risque. À défaut, j'émettrai un avis défavorable.

Mme Patricia Morhet-Richaud. – Les propositions du rapporteur me paraissent raisonnables. Je rectifie mon amendement en ce sens.

Mme Sylviane Noël. – Je le rectifie également.

Mme Élisabeth Lamure. – L'autorisation ne porte pas sur les équipements ?

Mme Catherine Procaccia, rapporteur. – Les équipements en eux-mêmes relèvent d'une autre procédure d'autorisation, je l'ai indiqué, plus lourde et plus longue.

Mme Élisabeth Lamure. – Cette procédure d'autorisation n'a pas de rapport avec celle nouvelle autorisation, qui passe exclusivement par les services du Premier ministre ?

Mme Catherine Procaccia, rapporteur. – C'est l'Anssi qui est chargée de l'instruction des demandes d'autorisation dans les deux cas.

Mme Viviane Artigalas. – Cela n'exclut-il pas dès lors les premiers déploiements de 5G, ceux qui s'appuient sur la 4G, au risque de fragiliser le régime ici créé ?

M. Franck Montaugé. – Il se pose une question de fond : durant une longue période, il y aura à la fois de la 4G et de la 5G. Couvre-t-on l'ensemble du sujet, techniquement, en se limitant à la 5G ? Les liens sont forts entre les deux techniques ! Les garanties du texte doivent s'apprécier en tenant compte de cette imbrication entre 4G et 5G…

Mme Catherine Procaccia, rapporteur. – N'ayez pas d'inquiétude. Si nous retreignons le champ à la 5G, c'est qu'il ne faut pas retarder les déploiements de la 4G qui seront, dans un premier temps, utilisés par la 5G, mais uniquement pour les usages existants. Les futurs usages de la 5G n'existent pas encore. Mon amendement ne met pas en danger les équipements ni n'exclut les usages futurs. Ceux-ci n'utiliseront pas les antennes ou d'autres éléments de la 4G.

Mme Sophie Primas, présidente. – Le Gouvernement réserve-t-il un accueil favorable à cet amendement ?

Mme Catherine Procaccia, rapporteur. – Oui, et tout le monde partage la préoccupation de ne pas retarder le déploiement de la 4G. C'est pour cette raison que j'ai voulu infléchir la rédaction.

Les amendements COM-20, COM-1 rectifié ter et le COM-11 rectifié sont adoptés.

Mme Catherine Procaccia, rapporteur. – Les amendements COM-2 rectifié *bis* et COM-12, identiques, visent à préciser le contenu de l'arrêté : les opérateurs souhaitent en effet que la liste des appareils visés par le nouveau régime d'autorisation utilise la terminologie des normes techniques internationales. Cela relève de la rédaction de l'arrêté, je suggère donc aux auteurs de retirer leurs amendements, pour les redéposer en séance : alors, nous pourrons interroger le Gouvernement. Nous demanderons alors l'avis du Gouvernement sur ces deux amendements. À défaut de retrait, mon avis sera défavorable.

Les amendements COM-2 rectifié bis et 12 sont retirés.

Mme Catherine Procaccia, rapporteur. – Mon amendement COM-30 rectifié supprime la mention du périmètre géographique dans la demande d'autorisation : il s'agit de s'assurer que l'État ne dicte pas aux opérateurs leur politique d'achat. Ce n'est pas à lui de choisir les équipementiers… Ce point avait été évoqué lors de l'audition de la secrétaire d'État devant notre commission, or malgré mes assurances de celle-ci, un certain flou subsiste.

Mon amendement COM-21 est rédactionnel.

L'amendement COM-13 supprime également le périmètre géographique, mais poursuit la logique d'extension du dispositif aux équipementiers et de fusion de l'ensemble des régimes d'autorisation. J'ai dit mon opposition sur ce point. Si cet amendement est rectifié et devient identique au COM-30, j'y serai bien sûr favorable. Sinon, avis défavorable.

M. Franck Montaugé. – Quel est le rapport entre le périmètre géographique et l'équipement ? Un opérateur place les équipements autorisés où il le souhaite !

Mme Catherine Procaccia, rapporteur. – Dans le texte initial, c'était l'inverse : il y avait un risque que le Premier ministre n'interdise à un opérateur de placer tel équipement à tel endroit.

M. Franck Montaugé. – Mais ce n'est pas un hasard : il y a une raison à cela ?

Mme Catherine Procaccia, rapporteur. – Reportez-vous à l'intitulé initial de la proposition de loi…

Mme Sophie Primas, présidente. – Il y a une préoccupation militaire sous-jacente.

Mme Viviane Artigalas. – L'idée était aussi que les équipements soient déployés de façon cohérente, et qu'en cas de panne, un autre équipement prenne la relève. Mais cela ne marche pas ! Un expert nous l'a dit, il ne sera pas possible de faire de l'interopérabilité.

Je suis d'accord pour supprimer la validation par le Premier ministre, mais il importe que le dossier soumis à l'Anssi indique où seront situés les équipements. Cela me gêne qu'on ne le prévoie pas.

M. Pascal Allizard. – Je ne suis pas mandaté par ma commission pour répondre, mais c'est un point qui a été évoqué lors de notre discussion. En matière de sécurité, le périmètre géographique est une notion importante. Imaginez que l'on souhaite installer un matériel à proximité d'une zone sensible. Jamais le Premier ministre ne donnera une autorisation tant qu'il n'aura pas de garanties sur le lieu d'implantation.

Le Gouvernement, je le crains, voudra rétablir l'actuelle rédaction.

Mme Sylviane Noël. – Quoi qu'il en soit, je rectifie mon amendement.

Mme Sophie Primas, présidente. – Nous en discuterons en séance publique, la position de la commission évoluera peut-être avec les explications du Gouvernement.

Mme Viviane Artigalas. – Le Premier ministre ne peut imposer les types de matériels et leur localisation. En revanche, il est normal qu'il soit informé de l'implantation.

Mme Catherine Procaccia, rapporteur. – Il faut prendre en compte les intérêts de la défense mais nous prémunir également contre le risque de pressions contre le déploiement d'un équipement.

Les amendements identiques COM-30 rectifié et COM-13 rectifié sont adoptés, ainsi que l'amendement COM-21.

Mme Catherine Procaccia, rapporteur. – L'amendement COM-14 supprime la durée maximale de huit ans prévue pour les autorisations délivrées par le Premier ministre. Or cette durée correspond à celle de l'amortissement des matériels et dépasse de loin celle des équipements logiciels : défavorable.

L'amendement COM-14 est retiré.

Mme Catherine Procaccia, rapporteur. – L'amendement COM-22 soumet le décret d'application à l'avis du Conseil d'État – c'est une garantie quant à la sécurité juridique du texte.

Surtout, il indique que le Premier ministre peut délivrer une autorisation sous conditions : la logique binaire, autorisation ou refus, ne suffit pas pour proportionner la décision aux enjeux.

L'amendement COM-22 est adopté.

Mme Catherine Procaccia, rapporteur. – Deux amendements identiques, le COM-23 que je vous présente et le COM-10 de la commission pour avis, corrigent la rédaction.

Mon amendement COM-24 renforce l'exigence de proportionnalité, car les décisions du Premier ministre auront un impact sur le rythme de déploiement, les coûts et l'accès des utilisateurs finaux aux services fournis grâce aux réseaux. Seul un risque particulièrement caractérisé justifie de telles incidences.

Cet amendement vise également à réduire la portée discriminatoire du texte en visant tout État étranger plutôt que tout État non membre de l'Union européenne – même si, nous le savons bien, les États membres de l'Union européenne partagent avec la France des valeurs et des normes qui rendent peu probables des actes d'ingérence sur un opérateur ou un prestataire. Enfin, pour clarifier le fait que ce régime d'autorisation porte globalement sur l'équipement et ses modalités d'exploitation, ma rédaction précise que le niveau de sécurité de l'équipement fait partie de l'analyse de sécurité.

Les demandes soumises au Premier ministre doivent comporter la garantie qu'un certain nombre d'obligations seront respectées. L'absence d'une telle garantie pourrait motiver une décision de refus du Premier ministre, sur le fondement d'un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale. L'amendement COM-8 de la commission pour avis ajoute parmi les obligations celles relatives aux communications d'urgence : cela complète opportunément le texte. J'y suis favorable.

L'amendement COM-9 de la commission pour avis soumet la motivation au droit commun : quand un secret protégé par la loi est en cause, la communication des motifs est facultative. J'y suis favorable.

Les amendements identiques COM-3 rectifié *bis* et COM-15 mentionnent le secret des correspondances, ajoutent dans les critères à prendre en compte le niveau de sécurité des appareils ; et ils remplacent « les modalités de déploiement et d'exploitation » par la « configuration ».

Le texte mentionne déjà la confidentialité, qui recoupe le secret des correspondances. La question des modalités de déploiement et d'exploitation mériterait sans doute d'être davantage explicitée en séance. Mais il s'agit de l'objectif même du nouveau régime d'autorisation : il ne serait pas avisé de le supprimer ! Je suis donc défavorable à ces amendements.

Mme Viviane Artigalas. – Viser les États étrangers plutôt que les États hors Union européenne ne risque-t-il pas de fermer la porte à toute stratégie européenne ?

Quant à la proportionnalité, nous venons déjà d'exclure les équipements liés à la 4G : il ne faudrait pas transiger avec le « risque sérieux ».

Mme Catherine Procaccia, rapporteur. – Notre rédaction ne fait nullement obstacle à des travaux communs à l'échelle européenne. Mais il s'agit de notre défense nationale et des intérêts étrangers pourraient monter au capital d'un fournisseur européen. Nous ne visons ici que ce que nous pouvons maîtriser, c'est-à-dire le cadre national.

La proportionnalité est importante, car on ne saurait geler tout projet en raison d'un risque faible, ni gêner sans une bonne raison l'activité des opérateurs et le déploiement de la 5G.

Les amendements COM-23 et COM-10 sont adoptés, ainsi que les amendements COM-24, COM-8, COM-9.

L'amendement COM-3 rectifié bis est retiré.

L'amendement COM-15 n'est pas adopté.

Mme Catherine Procaccia, rapporteur. – L'amendement COM-25 complète le COM-22 relatif aux autorisations sous conditions. Il procède également à une modification d'ordre rédactionnel.

Son adoption ferait tomber les amendements COM-4 rectifié *bis* et COM-16 qui poursuivent la logique d'unification des régimes applicables aux équipementiers et aux opérateurs. J'ai dit mon opposition à cette solution. Avis défavorable, donc.

L'amendement COM-25 est adopté. Les amendements COM-4 et COM-16 sont sans objet.

Mme Catherine Procaccia, rapporteur. – Par l'amendement COM-26, nous nous assurons que le texte s'applique sur l'ensemble du territoire, y compris à Wallis-et-Futuna.

L'amendement COM-26 est adopté.

L'article 1er est adopté dans la rédaction issue des travaux de la commission.

Article 2

Mme Catherine Procaccia, rapporteur. – Mon amendement COM-27 prévoit que le non-respect des conditions posées par le Premier ministre sera sanctionné comme une absence d'autorisation. L'adoption de cet amendement ferait tomber les COM-5 rectifié *bis* et COM-17, qui visent à unifier les différents régimes. Avis défavorable pour les raisons déjà évoquées.

L'amendement COM-27 est adopté.

Les amendements Com-5 rectifié bis et COM-17 sont sans objet.

Mme Catherine Procaccia, rapporteur. – L'amendement COM-28 concerne l'application de l'article 2 à Wallis-et-Futuna.

L'amendement COM-28 est adopté.

L'article 2 est adopté dans la rédaction issue des travaux de la commission.

Article 3

Mme Catherine Procaccia, rapporteur. – Les amendements identiques COM-6 rectifié *bis* et COM-18 visent à décaler l'entrée en vigueur de l'article, prévue au 1er février 2019. Je me suis moi-même étonnée de cette date mais les opérateurs que nous avons entendus en audition ne s'en sont pas émus: la législation en cours d'élaboration était annoncée et connue d'eux. Avis défavorable.

Les amendements COM-6 rectifié bis et COM-18 sont retirés.

L'article 3 est adopté sans modification.

Articles additionnels après l'article 3

Mme Catherine Procaccia, rapporteur. – Mon amendement COM-29 procède à une simplification par rapport au texte initial : pour un équipement entrant à la fois dans le champ de l'autorisation prévue à l'article R. 226-7 du code pénal et dans celui de l'autorisation prévue ici, une seule demande d'autorisation pourra être déposée.

Cette idée de simplification est également présente dans les amendements COM-7 rectifié *bis* et COM-19, mais je ne soutiens pas l'extension aux équipementiers : je propose donc aux auteurs de les rectifier dans le sens de mon amendement. J'émettrai alors un avis favorable. À défaut de rectification, l'avis serait défavorable. Je précise que, dans cette hypothèse, les deux amendements deviendront sans objet si le mien est adopté.

Mme Patricia Morhet-Richaud. – Je rectifie l'amendement COM-7 rectifié *bis* pour le rendre identique au COM-29.

Mme Sylviane Noël. – Je fais de même pour le COM-19.

Les amendements identiques COM-29, COM-7 rectifié ter et COM-9 rectifié sont adoptés et deviennent un article additionnel.

La proposition de loi est adoptée dans la rédaction issue des travaux de la commission.

LISTE DES PERSONNES ENTENDUES

Mardi 21 mai 2019

- *Autorité de régulation des communications électroniques et des postes :* **M. Loïc DUFLOT**, directeur Internet et utilisateurs.

Lundi 27 mai 2019

- *Direction générale des entreprises :* **MM. Mathieu WEILL**, chef de service de l'économie numérique, **Jean-Pierre LABE**, chef du bureau de la réglementation des communications électroniques, M**me Mélanie PRZYROWSKI**, conseillère parlementaire.

Mardi 28 mai 2019

- *Agence nationale de la sécurité des systèmes d'information :* **M. Guillaume POUPARD**, directeur général.

Mercredi 29 mai 2019

Table ronde « verticaux » :

- *Vinci Autoroutes :* **Mme Faustine ANTOINE**, directrice des contrats de concession, **M. Fabrice FRAJUT**, directeur des systèmes d'information.

- *SNCF :* **MM. Benoît TIERS**, directeur général Digital et Systèmes d'Information, **Sébastien KAISER**, directeur Connectivité & Réseaux.

Table ronde des opérateurs de communications électroniques :

- *Fédération française des télécoms (FFT) :* **MM. Arthur DREYFUSS**, secrétaire général Altice SFR, président de la FFT, **Michel COMBOT**, directeur général, **Mme Marie-Georges BOULAY**, directrice des affaires réglementaires SFR, **MM. Laurentino LAVEZZI**, directeur des affaires publiques Orange, **Pascal NOURRY**, responsable sécurité des réseaux Orange, **Hervé DE TOURNADRE**, directeur des affaires réglementaires Bouygues Telecom.

- *ILIAD* : **M. Pascal MAYEUX**, directeur des obligations légales, **Mme Ombeline BARTIN**, responsable des relations institutionnelles ILIAD.

Table ronde des équipementiers :

- *CISCO France :* **MM. Laurent DEGRÉ**, directeur général, **Jean-Charles GRIVIAUD**, *chief security officer* France.

- *Ericsson* : **M. Viktor ARVIDSSON**, directeur des relations institutionnelles et de l'innovation.

- *Huawei Technologies France :* **MM. Minggang ZHANG**, directeur général adjoint, **Antoine BOUR**, expert Réseau-Sécurité, **Jean-Christophe AUBRY**, responsable des affaires publiques.

- *Nokia :* **M. Marc CHARRIÈRE**, secrétaire général.

- *Samsung :* **M. Daniel BORRAS**, directeur de la stratégie - Samsung networks Europe, **Mme Florence CATEL**, directrice des relations publiques - Samsung electronics France.

LISTE DES CONTRIBUTIONS ÉCRITES

– EDF

TABLEAU COMPARATIF

___

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
___	___	___	___
	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	**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**	**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**
	Article 1er	**Article 1er**	**Article 1er**
Code des postes et des communications électroniques	Le chapitre II du titre Ier du livre II du code des postes et des communications électroniques est complété par une section 7 ainsi rédigée :	*(Alinéa sans modification)*	Le chapitre II du titre Ier du livre II du code des postes et des communications électroniques est complété par une section 7 ainsi rédigée :
LIVRE II : Les communications électroniques **TITRE Ier : Dispositions générales** **Chapitre II : Régime juridique.**			
	« Section 7	*(Alinéa sans modification)*	*« Section 7*
	« Régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques.	***« Régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques***	***« Régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques***
	« *Art. L. 34-11* – I. – Est soumise à une autorisation du Premier ministre, destinée à préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou	« *Art. L. 34-11.* – I. – Est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou	« *Art. L. 34-11.* – I. – Est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
	logiciels, permettant de connecter les équipements de clients au réseau radioélectrique mobile, qui par leurs fonctions présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau, à l'exclusion des appareils installés chez les clients, par les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ainsi désignés en vertu de leur activité d'exploitant, direct ou par l'intermédiaire de tiers fournisseurs, d'un réseau de communications électroniques ouvert au public.	logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile qui, par leurs fonctions, présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau, à l'exclusion des appareils installés chez les utilisateurs finaux.	logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile <u>de cinquième génération et des générations ultérieures</u> qui, par leurs fonctions, présentent un risque pour l'intégrité, la sécurité<u>, la confidentialité</u> et la continuité de l'exploitation du réseau, à l'exclusion des appareils installés chez les utilisateurs finaux <u>ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils</u>. **Amdts COM-20, COM-1 rect. ter, COM-11 rect.**
		« L'autorisation mentionnée au premier alinéa du présent I n'est requise que pour l'exploitation, directe ou par l'intermédiaire de tiers fournisseurs, d'appareils par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public.	« L'autorisation mentionnée au premier alinéa du présent I n'est requise que pour l'exploitation, directe ou par l'intermédiaire de tiers fournisseurs, d'appareils par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public.
	« Le Premier ministre publie et tient à jour une liste des dispositifs soumis au régime d'autorisation prévu à l'alinéa précédent.	« La liste des appareils dont l'exploitation est soumise à l'autorisation mentionnée au premier alinéa du présent I est fixée par arrêté du Premier ministre, pris après avis de l'Autorité de régulation des communications électroniques et des postes.	« La liste des appareils dont l'exploitation est soumise à l'autorisation mentionnée au premier alinéa du présent I est fixée par arrêté du Premier ministre, pris après avis de l'Autorité de régulation des communications électroniques et des postes.
	« II. – Sauf lorsqu'elle est refusée en application de	« II. – L'autorisation d'exploitation d'un appareil	« II. – L'autorisation d'exploitation d'un appareil

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
	l'article L. 34-11-2, l'autorisation est octroyée pour un ou plusieurs modèles et une ou plusieurs versions de dispositifs matériels ou logiciels, ainsi que pour un périmètre géographique précisés par l'opérateur dans son dossier de demande d'autorisation, pour une durée maximale de 8 ans.	peut être octroyée après examen d'un dossier de demande d'autorisation remis par l'opérateur. Le dossier précise les modèles et les versions des ~~dispositifs matériels et logiciels composant l'appareil ainsi que le périmètre géographique d'exploitation~~ pour lesquels l'autorisation est sollicitée.	peut être octroyée après examen d'un dossier de demande d'autorisation remis par l'opérateur. Le dossier précise les modèles et les versions des appareils pour lesquels l'autorisation est sollicitée. **Amdts COM-30 rect., COM-21, COM-13 rect.**
	« *Art. L. 34-11-1.* – Le renouvellement de l'autorisation prévue à l'article L. 34-11 peut être sollicité par son bénéficiaire, au minimum deux mois avant l'expiration de l'autorisation initiale.	« L'autorisation ~~peut être octroyée~~ pour une durée maximale de huit ans. Le renouvellement de l'autorisation fait l'objet d'un dossier de demande de renouvellement, qui est remis au moins deux mois avant l'expiration de l'autorisation en vigueur.	« L'autorisation est octroyée, le cas échéant sous conditions, pour une durée maximale de huit ans. Le renouvellement de l'autorisation fait l'objet d'un dossier de demande de renouvellement, qui est remis au moins deux mois avant l'expiration de l'autorisation en vigueur. **Amdt COM-22**
	« Les modalités de l'autorisation, la composition du dossier de demande d'autorisation et du dossier de demande de renouvellement sont fixées par décret. »	« Les modalités de l'autorisation ainsi que la composition du dossier de demande d'autorisation et du dossier de demande de renouvellement sont fixées par décret, pris après avis de l'Autorité de régulation des communications électroniques et des postes et de la Commission supérieure du numérique et des postes, qui se prononcent dans un délai d'un mois à compter de leur saisine.	« Les modalités d'octroi de l'autorisation, les conditions dont elle peut être assortie, ainsi que la composition du dossier de demande d'autorisation et du dossier de demande de renouvellement sont fixées par décret en Conseil d'État, pris après avis de l'Autorité de régulation des communications électroniques et des postes et de la Commission supérieure du numérique et des postes, qui se prononcent dans un délai d'un mois à compter de leur saisine. **Amdt COM-22**
	« *Art. L. 34-11-2.* – Le Premier ministre refuse par décision motivée l'octroi de l'autorisation s'il estime, après examen de la demande, qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale en raison de ce que le respect des règles mentionnées	« *Art. L. 34-12.* – Le Premier ministre refuse ~~par décision motivée~~ l'octroi de l'autorisation prévue à l'article L. 34-11 s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale résultant du manque de garantie du respect des	« *Art. L. 34-12.* – Le Premier ministre refuse l'octroi de l'autorisation prévue à l'article L. 34-11 s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale résultant du manque de garantie du respect des règles mentionnées aux *a*,

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
	aux *a*, *b* et *e* du I de l'article L. 33-1, en particulier l'intégrité, la sécurité et la continuité de l'exploitation des réseaux et services de communications électroniques, n'est pas garanti.	règles mentionnées aux *a*, *b* et ~~*e*~~ du I de l'article L. 33-1 relatives à l'intégrité, à la sécurité, à la confidentialité et à la continuité de l'exploitation des réseaux et de la fourniture de services.	b, *e*, *f* et *f bis* du I de l'article L. 33-1 relatives à l'intégrité, à la sécurité, à la confidentialité et à la continuité de l'exploitation des réseaux et de la fourniture de services. Sa décision est motivée sauf lorsque la communication des motifs pourrait être de nature à porter atteinte à l'un des secrets ou intérêts protégés par les dispositions des *a* à *f* du 2° de l'article L. 311-5 du code des relations entre le public et l'administration. **Amdts COM-8, COM-9**
	« Le Premier ministre peut prendre en considération, pour l'appréciation de ces critères, les modalités de déploiement et d'exploitation mis en place par l'opérateur, et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, soit ou non sous le contrôle ou soumis à des actes d'ingérence d'un État non membre de l'Union européenne. »	« Le Premier ministre ~~peut prendre~~ en considération, pour l'appréciation de ~~ces critères~~, ~~les~~ modalités de déploiement et d'exploitation ~~mises en place~~ par l'opérateur et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État ~~non membre de l'Union européenne~~.	« Le Premier ministre prend en considération, pour l'appréciation de ce risque, le niveau de sécurité des appareils, leurs modalités de déploiement et d'exploitation envisagées par l'opérateur et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État étranger. **Amdts COM-23, COM-10, COM-24** « Un tel refus ne peut être décidé que si les risques de ralentissement du rythme de déploiement des appareils sur le territoire national, de renchérissement des coûts de ce déploiement et de remise en cause de l'accès des utilisateurs finaux aux services qui en résultent sont proportionnés au risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale. **Amdt COM-24**
	« *Art. L. 34-11-3.* – I. – Si l'exploitation des	« *Art. L. 34-13.* – I. – Si l'exploitation des	« *Art. L. 34-13.* – I. – Si l'exploitation des

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
	appareils mentionnés au I de l'article L. 34-11 est réalisée en France sans autorisation préalable, le Premier ministre peut enjoindre à l'opérateur de déposer une demande d'autorisation, ou de renouvellement, ou de faire rétablir à ses frais la situation antérieure, dans un délai qu'il fixe.	appareils mentionnés au I de l'article L. 34-11 est réalisée ~~en France~~ sans autorisation préalable, le Premier ministre peut enjoindre à l'opérateur de déposer une demande d'autorisation ou de renouvellement ou de faire rétablir à ses frais la situation antérieure, dans un délai qu'il fixe.	appareils mentionnés au I de l'article L. 34-11 est réalisée sur le territoire national sans autorisation préalable ou sans respecter les conditions fixées par l'autorisation, le Premier ministre peut enjoindre à l'opérateur de déposer une demande d'autorisation ou de renouvellement ou de faire rétablir à ses frais la situation antérieure, dans un délai qu'il fixe. **Amdt COM-25**
	« Ces injonctions ne peuvent intervenir qu'après que l'opérateur a été mis en demeure de présenter des observations dans un délai de quinze jours, sauf en cas d'urgence, de circonstances exceptionnelles ou d'atteinte imminente à la sécurité nationale.	*(Alinéa sans modification)*	« Ces injonctions ne peuvent intervenir qu'après que l'opérateur a été mis en demeure de présenter des observations dans un délai de quinze jours, sauf en cas d'urgence, de circonstances exceptionnelles ou d'atteinte imminente à la sécurité nationale.
	« II. – Est nul tout engagement, convention ou clause contractuelle prévoyant l'exploitation des appareils mentionnés au I de l'article L. 34-11, lorsque cette activité n'a pas fait l'objet de l'autorisation préalable exigée sur le fondement de l'article L. 34-11 ou d'une régularisation dans les délais impartis. »	« II. – Est nul tout engagement, convention ou clause contractuelle prévoyant l'exploitation des appareils mentionnés au I de l'article L. 34-11 lorsque cette activité n'a pas fait l'objet de l'autorisation préalable exigée sur le fondement du même article L. 34-11 ou d'une régularisation dans les délais impartis. ~~»~~	« II. – Est nul tout engagement, convention ou clause contractuelle prévoyant l'exploitation des appareils mentionnés au I de l'article L. 34-11 lorsque cette activité n'a pas fait l'objet de l'autorisation préalable exigée sur le fondement du même article L. 34-11 ou d'une régularisation dans les délais impartis. « *Art. L. 34-14 (nouveau).* – La présente section est applicable dans les îles Wallis et Futuna. » **Amdt COM-26**
Chapitre V : Dispositions pénales.	**Article 2** Le chapitre V du titre I[er] du livre II du code des postes et des communications électroniques est ainsi modifié :	**Article 2** Le livre II du code des postes et des communications électroniques est ainsi modifié :	**Article 2** Le livre II du code des postes et des communications électroniques est ainsi modifié :
	1° Après l'article L. 39-1, il est	1° *(Alinéa sans*	1° Après l'article L. 39-1, il est

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
	inséré un article L. 39-1-1 ainsi rédigé :	*modification)*	inséré un article L. 39-1-1 ainsi rédigé :
	« *Art. 39-1-1*. – Est puni d'un an d'emprisonnement et de 150 000 euros d'amende le fait :	« *Art. 39-1-1*. – Est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait :	« *Art. 39-1-1*. – Est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait :
	« 1° d'exploiter des appareils mentionnés à l'article L. 34-11 sans autorisation préalable ;	« 1° D'exploiter des appareils mentionnés au I de l'article L. 34-11 sans autorisation préalable ;	« 1° D'exploiter des appareils mentionnés au I de l'article L. 34-11 sans autorisation préalable ou sans respecter les conditions fixées par l'autorisation ;
			Amdt COM-27
	« 2° de ne pas exécuter – totalement ou partiellement – les injonctions prises sur le fondement du I de l'article L. 34-11-3. » ;	« 2° De ne pas exécuter, totalement ou partiellement, les injonctions prises sur le fondement du I de l'article L. 34-13. ~~»~~ ;	« 2° De ne pas exécuter, totalement ou partiellement, les injonctions prises sur le fondement du I de l'article L. 34-13. « Le présent article est applicable dans les îles Wallis et Futuna. » ;
			Amdt COM-28
Art. L. 39-6. – En cas de condamnation pour l'une des infractions prévues aux articles L. 39 et L. 39-1, le tribunal pourra, en outre, prononcer la confiscation des matériels et installations constituant le réseau ou permettant la fourniture du service ou en ordonner la destruction aux frais du condamné et prononcer l'interdiction, pour une durée de trois années au plus, d'établir un réseau ouvert au public ou de fournir au public un service de communications électroniques.	2° À l'article L. 39-6, la référence : « L. 39-1 » est remplacé par les références : « L. 39-1 et L. 39-1-1 » ;	2° À l'article L. 39-6, la référence : « et L. 39-1 » est remplacée par les références : « , L. 39-1 et L. 39-1-1 » ;	2° À l'article L. 39-6, la référence : « et L. 39-1 » est remplacée par les références : « , L. 39-1 et L. 39-1-1 » ;
Art. L. 39-10. – Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions	3° Au premier alinéa de l'article L. 39-10, après la référence : « L. 39-1 », est insérée la référence : « L. 39-1-1 ».	3° Au premier alinéa de l'article L. 39-10 et au 4° du I de l'article L. 42-1, après la référence : « L. 39-1 », est insérée la référence : « ,	3° Au premier alinéa de l'article L. 39-10 et au 4° du I de l'article L. 42-1, après la référence : « L. 39-1 », est insérée la référence : « ,

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
définies aux articles L. 39, L. 39-1 et L. 39-3 encourent, outre l'amende suivant les modalités prévues par l'article 131-38 du code pénal : 1° (Abrogé) ; 2° La peine mentionnée au 2° de l'article 131-39 du code pénal, pour une durée de cinq ans au plus ; 3° La peine mentionnée au 9° de l'article 131-39 du code pénal. L'interdiction mentionnée au 2° de l'article 131-39 du code pénal porte sur l'activité professionnelle dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.		L. 39-1-1 ».	L. 39-1-1 ».
TITRE II : Ressources et police **Chapitre I^er^ : Fréquences radioélectriques.** **Section 2 : Dispositions spécifiques aux fréquences radioélectriques dont l'assignation est confiée à l'Autorité de régulation des communications électroniques et des postes.** *Art. L. 42-1*. – I. – L'Autorité de régulation des communications électroniques et des postes attribue les autorisations d'utilisation des fréquences radioélectriques dans des conditions objectives, transparentes et non discriminatoires tenant compte des besoins d'aménagement du territoire. Ces autorisations ne peuvent être refusées par l'Autorité de régulation des communications			

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
électroniques et des postes que pour l'un des motifs suivants : 1° La sauvegarde de l'ordre public, les besoins de la défense nationale ou de la sécurité publique ; 2° La bonne utilisation des fréquences ; 3° L'incapacité technique ou financière du demandeur à faire face durablement aux obligations résultant des conditions d'exercice de son activité ; 4° La condamnation du demandeur à l'une des sanctions mentionnées aux articles L. 36-11, L. 39, L. 39-1 et L. 39-4.			
. . . . .			
	Article 3	**Article 3**	**Article 3** *(Non modifié)*
	L'article 1er est applicable à l'exploitation des appareils, mentionnés à l'article L. 34-11 du code des postes et des communications électroniques, installés depuis le 1er février 2019. Les opérateurs qui exploitent des appareils soumis à autorisation, en vertu de l'article L. 34-11 du code de postes et de télécommunications électroniques, à la date d'entrée en vigueur de la présente loi disposent d'un délai de deux mois pour déposer la demande d'autorisation préalable prévue à ce même article.	L'article 1er est applicable à l'exploitation des appareils mentionnés au I de l'article L. 34-11 du code des postes et des communications électroniques installés depuis le 1er février 2019. Les opérateurs qui, à la date de publication de la présente loi, exploitent des appareils soumis à autorisation en vertu du même article L. 34-11 disposent d'un délai de deux mois pour déposer la demande d'autorisation préalable prévue audit article L. 34-11. Ce délai court à compter de la date de publication la plus tardive de l'arrêté mentionné au I ou du décret mentionné au II du même article L. 34-11, et au plus tard à compter de la fin du deuxième mois suivant la publication de la présente	L'article 1er est applicable à l'exploitation des appareils mentionnés au I de l'article L. 34-11 du code des postes et des communications électroniques installés depuis le 1er février 2019. Les opérateurs qui, à la date de publication de la présente loi, exploitent des appareils soumis à autorisation en vertu du même article L. 34-11 disposent d'un délai de deux mois pour déposer la demande d'autorisation préalable prévue audit article L. 34-11. Ce délai court à compter de la date de publication la plus tardive de l'arrêté mentionné au I ou du décret mentionné au II du même article L. 34-11, et au plus tard à compter de la fin du deuxième mois suivant la publication de la présente

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
		loi.	loi.
		L'arrêté mentionné au I et le décret mentionné au II du même article L. 34-11 sont publiés au plus tard deux mois à compter de la publication de la présente loi.	L'arrêté mentionné au I et le décret mentionné au II du même article L. 34-11 sont publiés au plus tard deux mois à compter de la publication de la présente loi.
			Article 4 *(nouveau)*
Code pénal **Livre II : Des crimes et délits contre les personnes** **Titre II : Des atteintes à la personne humaine** **Chapitre VI : Des atteintes à la personnalité** **Section 1 : De l'atteinte à la vie privée**			
Art. 226-3. – Est puni de cinq ans d'emprisonnement et de 300 000 € d'amende : 1° La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'État, lorsque ces faits sont commis, y compris par			L'article L. 226-3 du code pénal est complété par un alinéa ainsi rédigé :

Dispositions en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée nationale en première lecture	Texte adopté par la commission du Sénat en première lecture
négligence, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret ou sans respecter les conditions fixées par cette autorisation ; 2° Le fait de réaliser une publicité en faveur d'un appareil ou d'un dispositif technique susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure lorsque cette publicité constitue une incitation à en faire un usage frauduleux.			« Le présent article n'est pas applicable à la détention ou à l'acquisition par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, des appareils soumis à une autorisation du Premier ministre en application de la section 7 du chapitre II du titre I^{er} du livre II du code des postes et des communications électroniques.» **Amdts COM-29, COM-7 rect.ter, COM-19 rect.**