N° 569

SÉNAT

SESSION ORDINAIRE DE 2018-2019

Enregistré à la Présidence du Sénat le 12 juin 2019

AVIS

PRÉSENTÉ

au nom de la commission des affaires étrangères, de la défense et des forces armées (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 M. Pascal ALLIZARD,

Sénateur

(1) Cette commission est composée de : M. Christian Cambon, *président ;* MM. Pascal Allizard, Bernard Cazeau, Robert del Picchia, Mme Sylvie Goy-Chavent, MM. Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Cédric Perrin, Gilbert Roger, Jean-Marc Todeschini, *vice-présidents ;* M. Olivier Cigolotti, Mme Joëlle Garriaud-Maylam, M. Philippe Paul, Mme Marie-Françoise Perol-Dumont, *secrétaires ;* MM. Jean-Marie Bockel, Gilbert Bouchet, Michel Boutant, Olivier Cadic, Alain Cazabonne, Pierre Charon, Mme Hélène Conway-Mouret, MM. Édouard Courtial, René Danesi, Gilbert-Luc Devinaz, Jean-Paul Émorine, Bernard Fournier, Jean-Pierre Grand, Claude Haut, Mme Gisèle Jourda, MM. Jean-Louis Lagourgue, Robert Laufoaulu, Ronan Le Gleut, Jacques Le Nay, Rachel Mazuir, François Patriat, Gérard Poadja, Ladislas Poniatowski, Mmes Christine Prunaud, Isabelle Raimond-Pavero, MM. Stéphane Ravier, Hugues Saury, Bruno Sido, Rachid Temal, Raymond Vall, André Vallini, Yannick Vaugrenard, Jean-Pierre Vial, Richard Yung.

Voir les numéros :

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

Sénat : **454** (2018-2019)

SOMMAIRE

Pages

Les technologies de la cinquième génération de standards techniques pour les réseaux de téléphonie mobile, dite « 5G », permettront de développer des applications nouvelles et parfois disruptives, auxquelles tant les industries et entreprises utilisatrices que les fournisseurs de solutions doivent se préparer. La création de tout un écosystème est en jeu, dont le potentiel reste difficile à évaluer tant de nombreux usages restent à inventer.

En même temps, elles présenteront de nouvelles vulnérabilités du fait de leur architecture, de la présence massive des technologies informatiques et de traitements des données comme des modes d'organisation des réseaux de télécommunications qu'elles induiront.

Cette évolution revêt donc un enjeu de sécurité et de défense nationale à un double titre :

- comme les réseaux de distribution d'électricité, désormais indispensables au fonctionnement de l'ensemble des réseaux et des services qui en irriguent les activités économiques et la vie quotidienne sont devenus « supercritiques ». La résilience de cet ensemble présente un intérêt vital pour la défense et la sécurité nationale,

- d'autre part, les forces de sécurité intérieure et les armées utiliseront ces réseaux pour certaines de leurs activités propres.

La présente proposition de loi, adoptée par l'Assemblée nationale, en créant un nouveau régime d'autorisation préalable à l'installation de certains matériels et logiciels critiques, permettra d'assurer une meilleure sécurité des réseaux de télécommunications. Elle constitue une réponse partielle aux multiples facteurs de risques, y compris de souveraineté qui accompagnent cette rupture technologique, dont certains ne pourront d'ailleurs être abordés efficacement qu'à l'échelle européenne.

I. UNE RÉPONSE AUX ÉVOLUTIONS TECHNIQUES DANS LE DOMAINE DES TÉLÉCOMMUNICATIONS ET À LEURS CONSÉQUENCES POUR LA SÉCURITÉ NATIONALE

A. LES RÉSEAUX DE TÉLÉCOMMUNICATIONS SONT DEVENUS DES RÉSEAUX « SUPERCRITIQUES »

1. Une évolution importante des technologies et des usages

a) Une technologie de rupture

Contrairement aux générations précédentes (3G et 4G) à l'origine de l'avènement du smartphone et de la transformation de la vie des particuliers, la 5G est une technologie de rupture qui devrait permettre la transformation de nombreux secteurs d'activités et concernera en priorité les acteurs économiques. Elle permettra de répondre aux limites de la précédente génération en relevant trois défis principaux que sont :

- l'engorgement des réseaux de communications électroniques face à la massification des usages mobiles ;
- la capacité à fournir un accès aux réseaux et un débit suffisant à une grande quantité d'objets connectés (individuels, domotiques ou industriels) ;
- enfin, les trop longs délais de latence pour des services innovants qui requerront des temps de réaction à l'échelle de la milliseconde.

Cette technologie constitue un véritable changement d'échelle dans les capacités des réseaux de télécommunications « mobiles » :

- un **accroissement considérable des débits de données (**environ dix fois supérieurs à la 4G), qui pourraient atteindre, dès 2020, un gigabyte par seconde, et davantage encore ultérieurement ;
- une **réduction des temps de latence** dans les communications. La latence d'une connexion 5G serait d'environ 5 millisecondes, contre 100 millisecondes pour une connexion 4G, ce qui accroit la fiabilité et la stabilité des connexions même en mobilité ;
- un **accroissement de la densité des flux**, qui pourront être concentrés de façon souple et dynamique en fonction des besoins et permettre la création de tranches de réseaux à la demande avec des capacités personnalisées.[1]

---

[1] *Cette technologie permet d'affecter les flux de transmission à telle ou telle application en fonction de son caractère prioritaire et des besoins de l'utilisateur (network slicing), tout en réaffectant ces capacités lorsque l'application n'en a pas besoin. Ainsi de multiples réseaux virtuels adossés à un seul et même ensemble d'équipements physiques de réseau, peuvent cohabiter et fonctionnant par réallocation permanente des ressources.*

En outre, le caractère décentralisé de son architecture permet par la présence de fonctionnalités jusqu'ici uniquement concentrées dans les cœurs de réseau sur chacune des antennes, d'opérer une partie du traitement des données à la périphérie, sans que celles-ci transitent par un *data center* éloigné (*edge computing).*

Enfin, elle permet de déployer les applications de *cloud computing* (fonctionnalités assurées via le *cloud* et donc indépendantes de la performance du terminal – téléphone, ordinateur etc.) tout en maintenant une utilisation régulière du réseau pour des fonctions de base.

b) De nouveaux usages

La diffusion de cette technologie ouvre la voie à des applications et des usages variés et nouveaux. Elle va permettre le déploiement massif de l'internet des objets qui jouera un rôle essentiel dans le domaine de la mobilité (véhicules autonomes), de la domotique, de la réalité augmentée, de la production industrielle ou encore des réseaux énergétiques et des « villes intelligentes ».

Quelques nouveaux usages envisageables

« Avec l'utilisation entre autres de l'*edge computing* et de l'intelligence artificielle (*machine learning* et *deep learning)*, les opérateurs seront en mesure de proposer de nouvelles offres de services au grand public et aux industriels (assistance à la maintenance via la réalité augmentée, modification en temps réel de l'outil de production – développement des fermes de robots industriels –, services de pilotage des véhicules autonomes, virtualisation de l'offre de gaming, etc.).

Dans l'industrie, elle ouvre la possibilité pour un « client » (une application, une entreprise, etc.) de demander directement des ressources réseau virtuelles adaptées à ses besoins spécifiques (débit, latence, etc.). À titre d'exemple, un opérateur de mobilité pourrait obtenir des ressources réseau dédiées, afin de garantir la stabilité de la connexion et une très faible latence dans le cadre du déploiement d'une flotte de véhicules autonomes[1].

Par ailleurs, certains *business models* évolueront, en se tournant vers des services à forte valeur ajoutée. Ceci est dû au fait que la production de biens matériels sera transformée par l'émergence de moyens de production mutualisés, flexibles et plus réactifs. Par exemple, les constructeurs automobiles se concentreront sur le développement et la conception des services à la mobilité quand la production d'automobiles se trouvera profondément modifiée par le développement de la 5G. En effet, celle-ci permettra demain l'émergence de plateformes réagençant en temps réel les chaînes de production automobile et capable de créer des modèles à la demande.

Dans la société civile, la 5G permettra d'apporter des réponses aux enjeux de connectivité des territoires et d'accès aux services publics.

[1] *Des usages critiques tels que les véhicules connectés (qui auraient besoin d'une latence de l'ordre de 10ms), ou des réseaux d'objets connectés dont la densité pourrait atteindre un million d'équipements par km2 (dans une grande gare ou un stade).*

Sous réserve d'un niveau suffisant de pénétration et d'adoption de cette technologie, les nouveaux réseaux de télécommunications permettront de s'affranchir des contraintes d'implantation physique et géographique, pour apporter un service à plus forte valeur ajoutée sur l'ensemble du territoire, par exemple dans les domaines de la santé ou de l'éducation. À l'aide d'outils de réalité augmentée, rendus performants grâce à la 5G, nous pouvons imaginer que les professionnels de santé implantés dans les territoires réalisent des actes complexes nécessitant une expertise particulière, via une supervision à distance par des experts dans des centres régionaux. »

Source : Institut Montaigne « L'Europe et la 5G, passons la cinquième » *mai 2019*

Un exemple de réflexion prospective sur l'usage de la 5G : la SNCF

SNCF comprend que la 5G trouvera difficilement sa rentabilité dans des usages grand public. Elle trouverait plutôt son essor dans les services aux verticaux, ou entre verticaux, entre systèmes, à condition que les exigences de sécurités soient respectées.

Cette conviction est fortement partagée avec la Deutsche Bahn avec qui elle travaille de plus en plus étroitement, afin de construire une démarche d'écosystème commun autour de cette expérience numérique. L'intégration des transports en commun dans les villes intelligentes passe par la collecte et la gestion de données multiples (horaires, géolocalisation, nombre de voyageurs, points de départ, points d'arrivée, correspondances, etc.), pour optimiser les flux de circulation et les mettre à disposition de l'ensemble des usagers.

La connectivité est au service de la mobilité collective et du désenclavement des territoires. SNCF dans ses missions d'aménagement numérique de la mobilité, a besoin d'apporter au travers de ses 3000 gares, de ses 30 000 km de continuité territoriale et de lignes, de son patrimoine immobilier et de ses 300 emprises industrielles des éléments de solutions à ce désenclavement.

La connectivité est un vecteur critique de compétitivité :

L'accès à la 5G permet d'envisager la modernisation technologique du système ferroviaire, et la satisfaction de nouveaux usages couvrant l'ensemble des domaines de SNCF, en France, comme à l'international :

- nouveaux services d'expérience de voyage à bord ou en gare (travail, loisir, vie pratique) ;
- service de sécurité au bénéfice des agents et des voyageurs à bord et au sol;
- information en gare et à bord des trains ou en intermodalité ;
- gestion opérationnelle des circulations ferroviaires ;
- exploitation ferroviaire en gare, triage et atelier ;
- maintenance prédictive de nos installations ;
- surveillance des infrastructures et conduite de chantiers d'infrastructures ;
- usages télécoms, notamment tertiaires, communs à l'ensemble des métiers SNCF.

Pour les services comme pour les opérations, pour la compétitivité comme pour l'aménagement du territoire, les futurs réseaux 5G, opérés grand public ou privatifs, seront ainsi un actif stratégique.

SNCF met en place un programme 5G SNCF pour mieux comprendre et anticiper ces changements. Le programme comprend un volet de compréhension (veille stratégique, pédagogie, communication), d'expérimentations (conception des cas d'usage, mise en place de plateformes de test).

Il est probable que le groupe SNCF se dote d'un réseau privatif 5G au moins pour ses opérations ferroviaires et industrielles les plus sensibles (…).

Dans le cadre des autres activités, toutes les options sont possibles mais nécessitent au préalable des phases d'expérimentations importantes.

Il est également certain que le groupe SNCF fasse usage des réseaux 5G ouvert à des opérateurs publics pour répondre à certains besoins, ou pour y répondre dans certaines zones géographiques.

La mutualisation ou le partage d'infrastructure, passives ou actives, avec d'autres acteurs, qu'ils soient des verticaux ou des opérateurs télécoms semble un élément incontournable pour résoudre les problèmes de couverture.

Source : réponse au questionnaire parlementaire

c) Un déploiement progressif

Son déploiement sera progressif, avec la mise à disposition :

• dans un premier temps, de réseaux 5G *(non stand alone)* qui permettront, courant 2020, de répondre aux besoins de capacités des réseaux actuels, sans apporter l'ensemble des fonctionnalités 5G et qui continueront à s'appuyer sur les réseaux de quatrième génération ; ce qui suppose une interaction forte entre les deux équipements et pourrait inciter les opérateurs à retenir le même équipementier que pour les générations antérieures ;

• dans un second temps, de réseaux 5G *(stand alone)*, couvrant l'ensemble des usages attendus à travers une faible latence, une grande stabilité et une connectivité massive.

2. Un enjeu économique essentiel

En raison des capacités de ces technologies, du bouleversement des usages, de la révolution des processus de production industrielle et l'apparition de nouveaux services qu'elles induisent, l'entrée dans un nouveau cycle économique se profile qui, dans un environnement de concurrence mondialisée, bénéficiera aux États et aux entreprises qui maitriseront ces développements.

Pour certains observateurs, ce nouveau cycle pourrait être marqué par une amplification de la redistribution de la richesse au profit des grandes entreprises du secteur des nouvelles technologies qui, fort de leur capacité de calcul distribuée et faute de réglementation spécifique, pourraient obtenir une position dominante. Aujourd'hui ces services sont dominés par des acteurs étrangers (*IBM, Google, Microsoft, Amazon Web Service* et pour l'Asie, *Alibaba et Huawei*).

Cela pose des questions relatives à la souveraineté des États quant à la maîtrise de la donnée générée sur leur territoire, mais également concernant la capacité des opérateurs à assurer la sécurité de leurs réseaux.

La souveraineté de l'Europe et de la France dépendra de leur capacité à se mobiliser rapidement pour favoriser le développement des nouveaux réseaux et de la façon dont elles pourront s'assurer que les conditions du développement de l'écosystème des usages et des applications sont remplies.

Dans un premier temps, celles-ci reposent sur une capacité d'expérimentation afin de faire progresser et d'affiner tant les fonctionnalités que les usages.

Les enjeux d'investissement et de coordination à l'échelle européenne sont primordiaux. Les économies chinoises et américaines bénéficient d'un marché domestique suffisamment large pour permettre à leurs champions nationaux de développer ces activités et de prendre dès aujourd'hui une avance considérable. Tout retard pris dans le déploiement de la connectivité des territoires retardera d'autant le développement de l'écosystème 5G par les acteurs européens.

Le déploiement rapide des réseaux 5G constitue donc un enjeu majeur de compétitivité de nos industries, nos infrastructures et nos territoires et, en conséquence, un véritable enjeu de politique publique.

3. Un enjeu de politique publique

a) Un enjeu de souveraineté économique

En Europe, les États prennent conscience des enjeux mais réagissent à ce stade en ordre dispersé. Or, l'émergence d'acteurs alternatifs de cet écosystème est certainement l'une des conditions essentielles pour garantir notre souveraineté. La commission européenne a défini les principaux objectifs stratégiques dans le document *« Europe connectée : objectif 2025 »*.[1]

En France, le gouvernement a dessiné, en juillet 2018, *« une feuille de route ambitieuse pour la 5G »*[2], afin de développer le plus rapidement possible les usages industriels et ceux liés aux infrastructures. Cette feuille de route identifie quatre chantiers : libérer et attribuer les fréquences radioélectriques pour les réseaux 5G ; favoriser le développement de nouveaux usages, notamment industriels ; accompagner le déploiement des infrastructures de la 5G ; assurer, enfin, la transparence et le dialogue sur le déploiement de la 5G et l'exposition du public.

---

[1] « *Europe connectée : objectif 2025* » *Rapport d'information n° 389 (2016-2017 par MM. Pascal Allizard et Daniel Raoul au nom de la commission des affaires européennes du Sénat* http://www.senat.fr/rap/r16-389/r16-389_mono.html

[2] https://www.economie.gouv.fr/files/files/Actus2018/Feuille_de_route_5G-DEF.pdf

b) Un enjeu de sécurité nationale

Les sociétés modernes sont dépendantes du bon fonctionnement des réseaux de télécommunications. La résilience de ces derniers est devenue un enjeu de défense et de sécurité nationale, à deux titres au moins :

- la sécurité de ces réseaux revêt une importance vitale. Une interruption majeure de service constituerait une catastrophe économique et sociale et une atteinte à la sécurité nationale.

- compte tenu des capacités de ces réseaux et du coût qu'impliqueraient la mise en place de réseaux dédiés, les armées et les forces de sécurité intérieure ont commencé et utiliseront de plus en plus les réseaux civils de télécommunications.

Les enjeux de sécurité présentent une acuité particulière en particulier avec l'apparition de nouveaux usages critiques liés à la 5G.

C'est à ce titre que la commission des affaires étrangères, de la défense et des forces armées a été saisie pour avis de la présente proposition de loi.

En outre, compte tenu des investissements financiers importants nécessaires à leur déploiement, ces réseaux constituent des actifs économiques substantiels dont la dégradation serait très préjudiciables, à raisons de choix techniques inappropriés. Garantir la sécurité de ces réseaux procède donc de l'intérêt économique à long terme de l'économie nationale.

B. DES VULNÉRABILITÉS CROISSANTES

1. Des vulnérabilités intrinsèques aux nouvelles technologies

Par la combinaison d'une infrastructure physique et d'une infrastructure logicielle, les réseaux 5G seront capables de s'adapter aux usages clients. La structure d'un réseau 5G est construite sur la séparation entre les différents systèmes constituant l'infrastructure réseau physique (relais, antennes, etc.) et l'architecture logicielle[1].

Intrinsèquement les technologies 5G offrent des capacités de sécurité importantes comme le cryptage des données utilisateur, mais comme elles reposent sur des équipements de plus en plus virtuels et des architectures de réseaux de plus en plus déconcentrées, elles portent de nouvelles vulnérabilités.

[1] *Voir* Institut Montaigne « *L'Europe et la 5G, passons la cinquième* » mai 2019

a) Leur architecture va passer de systèmes centralisés à des systèmes distribués

Les réseaux de 5G seront des réseaux maillés à la configuration évolutive.

Dans les réseaux classiques, les antennes-relais ne servent qu'à retransmettre de façon assez passive les flux de données entre les terminaux des utilisateurs et les cœurs de réseaux qui assurent l'essentiel des fonctions. Avec la 5G, des fonctions sophistiquées de traitement des flux seront intégrées aux stations de base des antennes augmentant significativement le caractère sensible de ces équipements.

Ce changement exposera une plus grande surface de vulnérabilité à d'éventuelles attaques en raison de la grande ramification des réseaux, la multiplication des antennes, des capteurs et des nœuds informationnels qu'elle implique et les efforts de sécurisation qui portaient jusqu'à présent essentiellement sur les cœurs de réseau devront donc être étendus à ces nouveaux équipements pour assurer une sécurité de bout en bout.

b) Leur architecture va reposer toujours davantage sur des logiciels

La 5G devrait être le vecteur de la généralisation de réseaux virtualisés. Certains équipements physiques seront remplacés par des solutions logicielles déployées dans le *cloud*[1]. Ce transfert accroîtra la vélocité et la résilience des réseaux mais il ne sera pas exempt de failles d'un nouveau genre.

La part plus importante de logiciels dans les équipements de 5G crée de nouveaux risques d'erreur de configuration et confère aux modalités de déploiement retenues par chaque opérateur une importance considérable dans l'analyse de sécurité.

Avec le *cloud*, l'extension des liaisons entre les utilisateurs et les cœurs de réseaux accroît les risques d'interception ce qui rend nécessaire un contrôle renforcé. Là où un dispositif technique particulier, telle une « porte dérobée » (*backdoor*) est nécessaire pour intercepter un flux d'information, la détention des codes d'administrateur pour accéder aux logiciels et aux *clouds* des réseaux de 5G sera suffisante.

C'est donc par son architecture même, davantage que par la nature des équipements, que la 5G présentera des vulnérabilités nouvelles[2].

---

[1] *Actuellement les fonctionnalités des équipements de réseau reposaient à 70 % à 80 % sur des logiciels, mais ceux-ci étaient disséminés dans les équipements. Avec la 5G, ces logiciels ne seront plus nécessairement physiquement installés et exclusivement asservis au fonctionnement de tel ou tel équipement. Ils seront disséminés, dans un premier temps vers des centres serveurs, puis dans un second temps vers des clouds qui agrégeront les fonctions logicielles de réseaux, permettant de réorienter les ressources du réseau en fonction des besoins observés sur le territoire.*

[2] *Voir* Institut Montaigne « *L'Europe et la 5G, passons la cinquième* » mai 2019

c) La diversité des usages induit également de nouvelles vulnérabilités

Les menaces proviendront également de la croissance exponentielle des appareils ou systèmes connectés[1], qui eux-mêmes ne pourront garantir un niveau de sécurité infaillible[2].

Des secteurs d'activités complets et des nouveaux usages seront fortement dépendants de la disponibilité du réseau et offriront des capacités nouvelles aux cyber-attaquants. Afin d'éviter la prise de contrôle de ces objets ou services par des cyber-attaquants et la paralysie de systèmes vitaux de fonctionnement d'entreprises (notamment dans les secteurs sensibles ou présentant des risques de sécurité ou de services publics (« villes connectées », réseaux de distribution d'eau et d'énergie…), il deviendra primordial d'assurer un niveau adéquat de sécurité.

2. Ces évolutions pourraient préfigurer une redistribution des rôles entre les opérateurs.

La 5G ne sera probablement pas sans impact sur la structure même de l'industrie des télécommunications. Pour des raisons diverses stratégiques ou financières, les opérateurs traditionnels n'ont pas toujours pu réaliser avec leurs seuls moyens internes la montée en puissance nécessaire pour maîtriser de bout en bout et de façon autonome les capacités techniques de leurs équipements.

En outre, la 5G sera également source d'une évolution de la stratégie des opérateurs dits « verticaux ».

a) Un recours plus important à la sous-traitance

Il n'est pas exclu que les technologies nouvelles entraînent une réorganisation de l'écosystème industriel des télécommunications.

Les opérateurs ont avec la virtualisation une liberté et une responsabilité accrues dans les choix de déploiement des équipements. Cette évolution les conduit naturellement à un recours accru à la sous-traitance, tant pour la définition et l'implémentation des choix initiaux de déploiement (prestataires intégrateurs), que potentiellement pour la mise en œuvre des équipements eux-mêmes (prestataires d'infogérance, voire d'hébergement).

D'ores et déjà, les sous-traitants (intégrateurs ou fabricants de matériels et de logiciels) ont étoffé leurs offres de prestations d'installation, de maintenance, voire de gestion de l'exploitation des réseaux.

---

[1] *Selon Cisco, le monde comptera plus de 12 milliards d'appareils mobiles et d'objets connectés en 2022 (contre 9 milliards en 2017), et la 5G sera le support de 422 millions de connexions mobiles (3 % des connexions mobiles) avec une progression des connexions 5G exponentielle.*

[2] *Celles-ci pourront être dirigées vers l'objet lui-même, ou en détourner la finalité les transformant en vecteurs d'actions malveillantes. Le domaine des objets connectés souffre d'un manque de maturité qui se traduit par une insuffisance de normes et l'absence de sécurité by design.*

Le passage d'infrastructures matérielles à des infrastructures logicielles rend les opérations de mise à jour plus faciles, donc plus fréquentes et, partant, le suivi des différentes versions d'un même équipement devient plus complexe. Certains équipementiers en viennent à proposer à leurs clients d'acquérir un service de mise à jour en permanence effaçant la notion de versions des logiciels. Rien n'empêcherait, en outre, que ces mises à jour soient réalisées à distance sans intervention physique des opérateurs sur les équipements eux-mêmes et donc complètement sous-traitées, avec un contrôle technique a posteriori des opérateurs.

En outre, une technologie nouvelle appelle en règle générale dans sa phase de déploiement des modifications nombreuses opérées à un rythme soutenu, à mesure qu'apparaissent des problèmes et notamment pour palier des failles de sécurité. On peut donc s'attendre avec la 5G à une phase assez longue d'expérimentations et de corrections avant que le réseau ne se stabilise. Ceci accroît les risques liés à l'utilisation de technologies encore immatures et au temps d'adaptation nécessaire pour élever le niveau de protection.

De même, à côté des acteurs traditionnels des télécommunications que sont les équipementiers et les opérateurs, émergent des entreprises qui proposent aux opérateurs des services d'ingénierie afin de configurer les réseaux de nouvelles générations et d'intégrer certaines fonctionnalités[1].

Ce recours à la sous-traitance est naturellement porteur de risques, tant du fait de la possible méconnaissance des obligations de sécurité par les prestataires concernés, qu'au regard de leur soumission potentielle à des formes d'ingérence. Ces risques devront être appréciés lors de l'examen des modalités d'exploitation des appareils soumis à autorisation.

b) Le développement de nouveaux opérateurs

La 5G permettra le développement des services de cloud en augmentant la performance du réseau. Il n'est pas exclu que des entreprises avancées dans l'ingénierie logicielle, notamment les acteurs du secteur du *cloud computing* qui ont développé des outils de mise en œuvre des infrastructures de stockage massives, sur lesquelles les acteurs du secteur des réseaux mobiles devront s'appuyer pour créer les cœurs « 5G », prennent une place importante au détriment des opérateurs traditionnels, remettant en cause la nature incontournable de ces opérateurs.

Comme le souligne la récente étude de l'Institut Montaigne[2], « *le recours aux technologies utilisant le cloud pose la question de la sécurisation des données qui y transitent, y sont stockées et traitées. À ce jour, et en dehors des dispositions prises en Europe, notamment en matière de traitement des données privées via le Règlement général sur la protection des données (RGPD), il n'existe*

[1] *Une entreprise comme Cap Gemini propose des services de cette nature.*
[2] Institut Montaigne « *L'Europe et la 5G, passons la cinquième* » mai 2019

pas d'encadrement réglementaire concernant ces activités et l'usage qui est fait des données collectées. Il n'existe pas non plus de normalisation sur la façon dont les implémentations technologiques (containers, API…) doivent être effectuées de sorte à rendre interopérables les offres des différents leaders du marché. Sur un marché dominé par des acteurs étrangers (principalement Amazon Web Services, Microsoft et Google), et avec la mise en place de dispositifs judiciaires comme le Cloud Act, l'Europe et la France pourraient théoriquement rapidement se trouver dans une situation de dépendance et de vulnérabilité ».

c) Une évolution possible de la stratégie des opérateurs verticaux et l'apparition de nouveaux opérateurs de ce type

Il n'est pas exclu, dans l'attribution des fréquences utiles à la 5G, que les enchères puissent intéresser d'autres acteurs que les seuls opérateurs de télécommunications et notamment ceux qui, en soutien ou en complément d'une activité principale autre que les télécommunications, développent pour leur propre compte un réseau de télécommunication. On notera que l'Allemagne a réservé une part du spectre hertzien utile à la 5G aux opérateurs verticaux.

En France, des acteurs comme la SNCF, EDF ou les sociétés concessionnaires d'autoroutes ou d'aéroports qui utilisent déjà des réseaux PMR, et sont à ce titre qualifiés d'opérateurs « verticaux » seraient en mesure de se porter eux aussi acquéreurs de licences d'utilisation de fréquences 5G, pour améliorer les performances de leurs réseaux privatifs. Des réflexions sont en cours[1], mais une alternative pourrait venir des capacités offertes par les réseaux des opérateurs de télécommunication à travers l'affectation à une entreprise de capacités correspondant à ses besoins (en débit, en latence, en continuité : *slicing)* sans qu'elle soit obligée de se doter de sa propre infrastructure.

Avec la 5G et ses multiples applications au-delà de la seule téléphonie mobile, les opérateurs verticaux pourraient ainsi prendre une part croissante dans le marché des télécommunications.

3. L'évolution économique du secteur des télécommunications offre également des risques de vulnérabilité accrue

Une évolution tendancielle des acteurs et de la répartition de la chaîne de valeurs - les opérateurs traditionnels investissant davantage vers l'aval vers la gestion de leurs abonnés et de leur marque et la fourniture de services et d'applications alors qu'ils sous-traiteraient davantage la partie amont -constituerait une difficulté supplémentaire en termes de contrôle de la sécurité des réseaux par les pouvoirs publics, d'autant que les activités de certains de ses nouveaux acteurs ne sont pas nécessairement localisées sur le

[1] *Voir l'encadré supra p.9 s'agissant de la SNCF*

territoire national, ni sur celui de l'Union européenne, et ne relèvent pas toujours de la législation française ou communautaire.

L'objectif de la proposition de loi qui soumet à autorisation l'installation de certains équipements sous la responsabilité des opérateurs de télécommunications a aussi pour objectif de soutenir leur implication dans la sécurité de leurs réseaux dont la criticité est absolue.

4. Ces nouvelles vulnérabilités apparaissent dans un contexte marqué par le développement de la cybercriminalité.

a) Une augmentation tendancielle de la cybercriminalité

Comme votre Commission le remarquait dans son rapport pour avis sur les crédits de l'ANSSI[1], la menace ne cesse de s'accroître en intensité et en sophistication :

- le rapport Symantec[2] donne des statistiques précises sur les cyberattaques et classe la **France désormais au 9ème rang mondial (et au 4ème rang européen) des pays où la cybercriminalité est la plus active.**
- le domaine cybernétique est reconnu comme un nouvel espace de conflictualité dans les doctrines militaires, ce qui se traduit par la création de structures de forces dans la plupart des grandes puissances, France incluse.
- enfin la dépendance croissante aux systèmes numériques couplée à une insuffisante prise en compte des enjeux de cybersécurité dans leur architecture et leur développement accroît leur vulnérabilité.

Le rapport de l'ANSSI[3] pour 2018 identifie cinq catégories de menaces et leur évolution (voir encadré ci-dessous) : *si les opérations de sabotage restent les plus visibles, l'espionnage est sans doute le risque qui pèse le plus fortement sur les organisations. Il a été une préoccupation majeure pour l'ANSSI en 2018. Discrets, patients et bénéficiant de ressources importantes, certains attaquants semblent préparer les conflits de demain en s'intéressant à des secteurs particulièrement critiques (défense, santé, recherche, etc.). L'exploitation des relations de confiance entre partenaires en vue de mener des attaques indirectes constitue également un champ de préoccupation majeur ».*

b) *Un enjeu démultiplié*

Le recours croissant de pans de l'économie (industrie, transports, santé, etc.) et de nos sociétés, à ces technologies devenues, dans certains cas,

---

[1] *Sénat (2018-2019) Avis n°149 – Tome IX Loi de finances pour 2019 Direction de l'action du Gouvernement : coordination du travail gouvernemental – rapport pour avis de MM. Olivier Cadic et Rachel Mazuir p.19* http://www.senat.fr/rap/a18-149-9/a18-149-94.html#toc85

[2] Symantec *Internet Security Threat Report (ISTR)* https://www.symantec.com/fr/fr/security-center/threat-report

[3] *Exfiltration de données stratégiques, attaques indirectes, opérations de déstabilisation ou d'influence, génération de crypto monnaies et fraude en ligne* https://www.ssi.gouv.fr/uploads/2019/04/anssi_rapport_annuel_2018.pdf *p.6*

indispensables, leurs évolutions et l'apparition massive des objets connectés va accroître très fortement la surface d'exposition aux attaques.

Les conséquences de ces attaques pourraient s'avérer catastrophiques et coûteuses en cas de déni de fonctionnement des réseaux de communication desservant des nombreux systèmes d'informations (risques d'accident industriel, arrêts de production de biens et de services, arrêts de services publics essentiels ou du secteur de la grande distribution, paralysie des transports….).

La menace à laquelle doit répondre le nouveau dispositif est celle de l'exploitation d'une faiblesse des infrastructures 5G, afin de porter atteinte à la sécurité nationale. La faiblesse considérée pourrait résulter d'un défaut de conception, volontaire ou non, de la part du producteur de ces équipements, ou d'une erreur de configuration dans leur déploiement par les opérateurs, ou encore d'actions illégitimes ou d'erreurs des opérateurs ou de leurs sous-traitants dans le cadre de la maintenance et de l'administration de ces équipements. De telles faiblesses pourraient être exploitées par un acteur, étatique ou non, qui en aurait connaissance.

Nature de finalités recherchées par les attaquants

- **espionnage des communications électroniques** transitant par les équipements concernés – cette préoccupation sera étendue par la 5G à un ensemble plus vaste d'équipements constitutifs du réseau, du fait de la déconcentration accrue des fonctions avancées dans cette technologie ;
- **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 ; leur impact serait particulièrement significatif dès lors que les réseaux 5G serviront de support à d'autres usages que les seules communications électroniques grand public, et entraîner des atteintes tant à la sécurité des biens et des personnes (objets connectés) qu'à la continuité de l'action de l'État (réseaux régaliens de la sécurité intérieure ou civile) ;
- **attaque informatique d'autres infrastructures numériques** : un attaquant ayant pris le contrôle d'un équipement au sein du réseau d'un opérateur pourrait se servir de celui-ci comme relai, pour injecter des logiciels malveillants dans les flux transitant par cet équipement, et infecter les systèmes d'information de ses clients. La mise en œuvre de cette technique sur les réseaux 5G pourrait avoir un impact d'autant plus important que ceux-ci donneront indirectement accès à de nombreuses autres infrastructures critiques.

Dans l'appréciation des risques, il convient d'intégrer tant les propriétés techniques intrinsèques des différents composants des réseaux 5G (qualité d'implémentation, 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, etc.) que les garanties apportées à travers les modalités de déploiement (bonne activation des options de sécurité, architecture limitant l'exposition aux attaques,

redondance, protections périmétriques) et d'exploitation (administration sécurisée, contrôle de l'accès des exploitants aux opérations sensibles, supervision, procédures de déploiement efficace des correctifs).

Outre ces facteurs techniques, l'analyse de sécurité doit également intégrer les possibilités d'ingérence d'États tiers, disposant d'un pouvoir de contrainte vis-à-vis de certains acteurs (fournisseurs d'équipements de télécommunication, intégrateurs, ou sous-traitants impliqués dans les opérations de maintenance et d'exploitations des réseaux des opérateurs), notamment du fait de dispositions légales applicables à ces acteurs en vertu de leur nationalité, ou des liens financiers qu'ils entretiennent avec ces États.

C. UN ENJEU DE DÉFENSE ET DE SÉCURITÉ NATIONALE

L'évolution des technologies va renforcer encore la place des réseaux de télécommunications dans notre société. Le renforcement de la surveillance et la résilience de ces réseaux est un enjeu majeur de défense et de sécurité nationale.

1. La résilience des réseaux : un enjeu d'intérêt vital

Ce secteur est déjà reconnu comme d'importance vitale au titre du code de la défense. Les opportunités offertes par les nouvelles technologies et leurs conséquences en matière de vulnérabilité rendent leur résilience et leur protection d'autant plus indispensables.

Au-delà du seul secteur des communications électroniques, l'utilisation des nouvelles technologies peut également concerner d'autres opérateurs dits « verticaux » qui disposent d'ores et déjà de réseaux de radioélectriques privatifs pour exploiter un certain nombre de leurs activités. Ces réseaux utilisent des fréquences attribuées aux opérateurs et des infrastructures propriétaires. Il pourrait concerner à l'avenir d'autres activités.

Certaines activités relèvent du régime légal de sécurité des activités d'importance vitale établi par le code de la défense. Ce régime repose sur un ensemble d'obligations faites aux « *opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* », selon l'article L. 1332-1 de ce code.

Les infrastructures critiques comprennent les entités publiques et privées qui fournissent des biens et services indispensables à la Nation ou peuvent présenter un danger grave pour la population. Cette définition recouvre généralement l'approvisionnement en énergie, les communications électroniques, les systèmes de transport, les services financiers, la santé

publique, la gestion de l'eau et les services publics indispensables. La France a ainsi défini douze secteurs d'activité d'importance vitale et identifié plus de 200 opérateurs d'importance vitale (OIV) dont la liste est un document classifié. Le secteur des communications électroniques, de l'audiovisuel et de l'information étant reconnu comme un secteur d'activités d'importance vitale, on peut estimer que les principaux opérateurs de télécommunication, et notamment ceux exploitant des réseaux radioélectriques mobiles, figurent parmi ces OIV.

a) Le cadre législatif et réglementaire

Le dispositif de sécurité des activités d'importance vitale, inséré dans le code de la défense, constitue un cadre législatif et réglementaire permettant d'associer les OIV au système national de protection contre le terrorisme, le sabotage et les actes de malveillance. Il formalise le dialogue permanent entre l'État et ces opérateurs afin d'assurer leur sécurité.

Ces obligations peuvent porter sur la limitation de l'accès et sur des mesures de protection physique des sites et installations, mais également, depuis les dispositions introduites dans la loi n°2013-1168 du 18 décembre 2013 de programmation militaire sur les règles de sécurité nécessaires à la protection de certains des systèmes d'information des opérateurs d'importance vitale et des opérateurs publics ou privés qui participent à ces systèmes[1].

b) Les modalités d'action de l'État relative à la sécurité des systèmes d'information

Au même titre que la sécurisation des systèmes d'information de l'État, l'amélioration de la protection des organismes d'importance vitale fait partie des champs prioritaires définis par la Stratégie nationale de cyberdéfense de février 2018[2].

Identifiée comme une priorité par les documents stratégiques et les lois de programmation militaires successives depuis 2008, la sécurité des systèmes d'information et de communication contre les risques d'interception ou d'interférence, notamment par des moyens cybernétiques, fait partie intégrante de la stratégie de sécurité nationale et de la politique de défense que le Premier ministre a la charge de définir et de coordonner[3].

Il dispose à cette fin de l'Agence nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de sécurité des systèmes d'information.

Depuis sa création en 2009, l'ANSSI a progressivement renforcé son rôle auprès des OIV. Jusqu'en 2013, à l'exception du secteur des

[1] *Article l 1332-6-1 du code de la défense et suivants*
[2] *http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/*
[3] *Article L 2331-1 et suivants du code de la défense.*

communications électroniques, pour lequel elle était déjà impliquée dans l'agrément des équipements au titre du dispositif de l'article 226-3 du code pénal dont l'objet la protection de la vie privée et du secret des correspondances (*voir infra p.25*), les missions de l'ANSSI se limitaient à la diffusion d'informations et de conseils ou à la réalisation d'audits de sécurité à la demande des opérateurs.

Face à une menace informatique croissante, le législateur, par la loi n°2013-1168 du 18 décembre 2013 de programmation militaire, a imposé des exigences en matière de sécurité informatique aux OIV[1], la France devenant ainsi un des premiers pays à légiférer dans le domaine de la cybersécurité des infrastructures critiques.

À ce titre, le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'informations des OIV, mais aussi des opérateurs publics ou privés qui participent à ces systèmes pour lesquels *« l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population »*[2].

Ces règles élaborées et proposées sont établies par arrêtés du Premier ministre après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernée. Elles peuvent être différentes selon le secteur ou le type d'activité de l'opérateur concerné. Chaque OIV tient à jour une liste des systèmes d'information d'importance vitale y compris ceux des opérateurs tiers qui participent à ces systèmes, auxquels s'appliquent les règles de sécurité. Il communique cette liste ainsi que ses mises à jour à l'ANSSI qui peut solliciter des modifications. Cette liste est couverte par le secret de la défense nationale.

Ces règles peuvent prescrire l'installation de systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale, exploités sur le territoire national par des prestataires de services qualifiés, par l'ANSSI ou par d'autres services de l'État[3].

Elles créent une obligation de déclaration au Premier ministre de tout incident majeur qui affecterait le fonctionnement ou la sécurité de ces systèmes et les bases du dialogue qui intervient alors entre l'opérateur et l'ANSSI[4].

---

[1] *Cette évolution figurait parmi les recommandations du rapport d'information de M. Jean-Marie Bockel au nom de la commission des affaires étrangères de la défense et des forces armées « La cyberdéfense : un enjeu mondial, une priorité nationale » Sénat n° 681 (2011-2012) .*

[2] *Article L. 1332-6-1 du code de la défense*

[3] *Alinéa 2 de l'article L 1332-6-1 et articles R 1332-41-3, R 1332-41-9 du code de la défense*

[4] *Article L. 1332-6-2 et R. 1332-41-10 et R.1332-41-11 du code de la défense*

Elles permettent au Premier ministre de soumettre les opérateurs à un processus de contrôle et d'audit de leurs systèmes d'information d'importance vitale destiné à vérifier leur niveau de sécurité et le respect des règles de sécurité[1].

Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut, en outre, décider des mesures que les OIV doivent mettre en œuvre[2].

Le non-respect de ces règles est passible[3] d'amendes.

Ces mesures ont fait l'objet d'une concertation approfondie avec les opérateurs. Elles sont désormais fixées par arrêtés sectoriels du Premier ministre et revêtent un caractère contraignant. L'ANSSI accompagne les OIV sur le plan technique dans la mise en œuvre de ces arrêtés.

Ainsi, les acteurs du secteur des télécommunications sont-ils d'ores et déjà en lien étroit avec le SGDSN et l'ANSSI, dont ils apprécient le haut niveau de compétence technique.

Cependant, la Stratégie nationale de cyberdéfense de février 2018[4] considère que cette étape a apporté des résultats importants mais que des insuffisances demeurent et qu'il convient en conséquence de « *faire évoluer le modèle pour l'adapter davantage aux contraintes et à l'évolution de la cyber menace dans cinq directions : l'adaptation des règles de sécurité informatique aux métiers, le renforcement de la cyber sécurité des opérateurs « supercritiques », l'extension du dispositif réglementaire au traitement des incidents, la prise en compte des particularités des entreprises de services numériq*ues *et le développement de l'offre privée d'assistance technique en cyber sécurité.* »

2. Les forces armées utiliseront ces réseaux pour leurs propres activités

Comme l'indique, en y consacrant des développements importants dans son rapport pour avis au nom de la commission de la défense et des forces armées de l'Assemblée nationale, M. Thomas Gassilloud[5], « *tant les forces de sécurité intérieure que les armées s'appuient aujourd'hui sur les réseaux civils de télécommunications pour leur activité opérationnelle sur le territoire national. Elles sont autant concernées par les opportunités que par les vulnérabilités de la 5G qu'elles utiliseront pour des usages par nature sensibles* ».

---

[1] *Article L .1332-6-3 et R. 1332-41-11 à R. 1332-41-16 du code de la défense*
[2] *Article L .1332-6-4 du code de la défense*
[3] *Article L .1332-7 et R. 1332-41-23 et R.1332-42 du code de la défense*
[4] *http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/ p.60*
[5] *Assemblée nationale - XVème législature - Avis n°1830 http://www.assemblee-nationale.fr/15/rapports/r1830.asp*

a) Forces de sécurité intérieure : un adossement croissant aux réseaux civils.

Les réseaux traditionnellement distincts des réseaux civils (Rubis pour la gendarmerie et l'infrastructure nationale partagée de télécommunications (INPT) pour la police (système Acropol) et les services d'incendie et de secours (Système Antarès) interopérables et couvrant ainsi 95 % à 98 % du territoire en télécommunications à bas débit, mis en place il y a une trentaine d'années restent opérationnels et sont plus résilients que les infrastructures civiles. Mais cette technologie devra faire place à des systèmes à plus haut débit pour répondre aux nouveaux comme le partage de situations tactiques en temps réel[1].

Des réflexions ont donc été conduites jusqu'en 2018 sur la modernisation des communications tactiques, aboutissant à un programme appelé PC-Storm pour lequel, en raison du montant des investissements nécessaires et de la couverture offerte, il a été décidé de s'en remettre à la suite d'un appel d'offres aux services d'un opérateur civil – en l'espèce, Orange –, qui fournira aux forces de sécurité intérieure des services de télécommunications mobiles et leur garantira, en cas de saturation d'une cellule de communications, des moyens propres à assurer la résilience des forces[2].

Les opportunités qu'offre la 5G et les vulnérabilités qu'elle crée sont prises en compte avec le concept de politique de numérisation nomade « *brigade sans fil* », développé par la gendarmerie dont les premières applications sont déployées dans le cadre du programme appelé Néogend qui permet aux brigades dotées de *smartphones* tant d'accéder à nombre d'applications depuis le terrain, sans avoir à consulter les réseaux concernés depuis un poste fixe. Mais le nomadisme a des ambitions plus grandes, dans les domaines de la vidéo, de la biométrie, de l'internet des objets, ou encore de l'exploitation de la domotique pour lesquels l'accroissement des débits permis par la 5G est très attendu.

Le Rapporteur pour avis de l'Assemblée nationale souligne en outre les modalités de traitements des vulnérabilités associés à l'utilisation des réseaux civils, grâce à l'appui de l'ANSSI, aux leviers offerts par le droit des marchés publics de défense et de sécurité, permettant le choix d'un

---

[1] *Les attentats de 2015 ont montré les limites des outils actuels pour le partage de situations tactiques au sein des forces de sécurité intérieure ; à défaut, les opérateurs ont été conduits à utiliser des réseaux civils de téléphonie peu sécurisés voire des applications de messagerie instantanées.*

[2] *L'architecture des communications tactiques des forces de sécurité intérieure reposera donc sur les services d'un fournisseur civil, que compléteront des systèmes projetables de bulles tactiques qui peuvent être déployées en cas de défaillance de l'opérateur et le maintien des bandes 28 et 68 dans la fréquence des 700 MHz, allouées au ministère de l'Intérieur, capacités qui permettront si besoin un moyen de fonctionnement « en mode dégradé ».*

opérateur faisant preuve d'une grande maturité dans la prise en compte des besoins des forces.

b) Des perspectives dans le domaine militaire.

Le Rapporteur pour avis de l'Assemblée nationale expose deux systèmes conçus pour s'adosser – au moins en partie – à des réseaux civils :

- *Auxylium* permet aux militaires, grâce à un téléphone de gamme commerciale utilisant les réseaux civils de télécommunication, relié par Bluetooth à un poste radio, d'accéder à leurs propres réseaux de communication, tout en utilisant les réseaux civils de télécommunication. L'articulation trouvée entre réseaux civils et militaires permet d'utiliser le système pour transmettre des ordres certifiés, y compris des ordres de tir, et géolocaliser les unités.
- *DIPAD* repose en partie sur les réseaux GSM, peut être connecté au réseau *Acropol* (des forces de sécurité intérieure) en basculant d'un réseau d'arrondissement parisien à un autre, tout en étant compatible avec les réseaux militaires et doté d'une fonction de géoréférencement. Il vise à assurer la liaison entre les centres et les hommes sur le terrain.

Ces deux dispositifs ont été utilisés dans le cadre de l'opération Sentinelle.

II. L'INTERVENTION DU LÉGISLATEUR EST NÉCESSAIRE

Plusieurs dispositifs législatifs, obéissant à des finalités différentes sont actuellement applicables aux équipements déployés par les opérateurs de réseaux radioélectriques, soit au titre de la protection du secret de la correspondance et de la vie privée, soit au titre de la protection des activités d'importance vitale. Ces dispositifs ne permettent cependant pas de répondre efficacement aux objectifs de protection de bout en bout des systèmes de nouvelles générations déployés par les opérateurs de réseaux radioélectriques mobiles.

Des réflexions sur l'opportunité d'encadrer ces systèmes sont en cours dans la plupart des États qui ont opté pour des solutions plus ou moins robustes et des méthodes différentes en phase avec leur système juridique comme avec l'organisation de leur cyberdéfense. L'Union européenne a entamé une démarche normative mais qui risque de ne pas aboutir très rapidement.

Or le déploiement des réseaux de cinquième génération est prévu à partir de 2020 au moins dans la configuration intermédiaire, ce qui incite à une intervention préalable du législateur.

A. LES LÉGISLATIONS ACTUELLES SONT INSUFFISANTES

1. Le régime actuel de contrôle des équipements de réseau ne permet pas une protection de bout en bout des systèmes de nouvelles générations

La législation actuelle portant sur la protection de la vie privée et du secret des correspondances électroniques (art. 226-3 du code pénal) met en œuvre un régime d'autorisation encadrant la mise sur le marché des équipements de réseaux radioélectriques en vue de contrôler leur fiabilité technique. Toutefois, ce régime qui ne répond pas aux mêmes finalités est devenu, malgré des adaptations successives, insuffisant pour parer les risques liés aux nouvelles technologies et garantir la résilience des réseaux tels qu'ils seront reconfigurés à l'occasion du déploiement de la 5G.

a) Le cadre légal en vigueur

(1) Un régime d'autorisation des équipements de réseau fondé sur le droit de la protection du secret de la correspondance et de la vie privée

Le 1° de l'article 226-3 du code pénal punit de cinq ans d'emprisonnement et de 300 000 euros d'amende *« la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques »*, sans autorisation administrative ou sans en respecter les conditions, y compris en cas de négligence. Ces appareils ou dispositifs, qui

figurent sur une liste dressée dans des conditions fixées par décret en Conseil d'État, répondent à l'une des conditions alternatives suivantes :

- être « de nature à permettre la réalisation d'opérations pouvant constituer une atteinte au secret de la correspondance privée (infraction prévue par le second alinéa de l'article 226-15) ;

- s'ils sont « conçus pour la détection à distance des conversations », et permettent de porter atteinte à la vie privée (infraction prévue par l'article 226-1) ;

- avoir 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) ;

Les articles R. 226-1 à R. 226-12 du code pénal ont défini la procédure applicable pour la délivrance de ces autorisations administratives.

(2) Le champ d'application de ces dispositions a été progressivement étendu,

Cette base juridique a permis à l'administration de contrôler la sécurité des équipements les plus sensibles des réseaux de télécommunications mobiles. Le régime d'autorisation s'applique ainsi à tous types de matériels permettant l'écoute de personnes à leur insu, l'enregistrement de communications téléphoniques, l'interception des données transmises sur les réseaux de télécommunications de tous types – internet comme la téléphonie – et ce, quelle que soit leur nature.

La liste des équipements dont la mise sur le marché est soumise à l'autorisation du Premier ministre est fixée par un arrêté du Premier ministre. On notera que certains de ces équipements ne sont pas exploités par des opérateurs de communications électroniques mais relèvent d'autres types de dispositifs (notamment, de captation à l'usage des services judiciaire d'enquête enquêteurs ou à l'usage des services de renseignement dans le cadre légal du code de la sécurité intérieure)[1].

Afin de mettre à jour la base juridique applicable, l'article 23 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire 2014-2019 a fait évoluer le champ des appareils ou dispositifs soumis à autorisation préalable, des produits « conçus pour réaliser » des interceptions ou des captations de données aux produits « de nature à permettre la réalisation » de telles opérations.

En conséquence, un nouvel arrêté en date du 11 août 2016 dont les dispositions n'entreront en vigueur que le 1er octobre 2021[2] a ajouté à la liste

---

[1] *les dispositifs de captation informatique prévus aux articles 706-102-1 du code de procédure pénale et L.853-2 du code de la sécurité intérieure.*

[2] *A la demande de l'ARCEP, l'entrée en vigueur de cette modification de la liste a été renvoyée au 1er octobre 2021 afin de laisser aux sujets de cette obligation le temps de se préparer aux démarches*

soumise à l'autorisation préalable « *les appareils qui permettent aux opérateurs de communications électroniques de connecter les équipements de leurs clients au cœur de leur réseau radioélectrique mobile ouvert au public, dès lors que ces appareils disposent de fonctionnalités, pouvant être configurées et activées à distance, permettant de dupliquer les correspondances des clients, à l'exclusion des appareils installés chez ceux-ci* ».

Cette extension est justifiée par le fait que les stations de base des réseaux mobiles de cinquième génération pourraient à terme être amenées à porter certaines des fonctions d'interception légale qui constituent le principal objet de ces régimes d'autorisation. Ces fonctions d'interception légale sont actuellement exclusivement concentrées dans les équipements dits de cœur de réseau. Ce positionnement ne sera pas remis en cause dans les premiers déploiements 5G en France, à compter de 2019 ou 2020. En effet, ces déploiements porteront sur la technologie dite « *Non Standalone* », qui conservera les cœurs de réseaux 4G existants. L'évolution des fonctions d'interception légale n'interviendra qu'avec le déploiement de réseaux 5G « *Standalone* », anticipée au plus tôt en France à compter de 2021 voire 2022.

(3) Les modalités de délivrance de l'autorisation

L'autorisation est délivrée par le Premier ministre après avis d'une commission consultative, présidée par le directeur général de l'ANSSI et composée de représentants des administrations de l'État concernées, d'un représentant de la Commission nationale de contrôle des techniques de renseignement (CNCTR)[1] et de deux personnalités qualifiées désignées par le Premier ministre. L'ANSSI instruit les dossiers et assure le secrétariat de la commission. Elle est ainsi devenue l'interlocuteur de référence des opérateurs pour la sécurisation de leurs réseaux radioélectriques.

Ce régime d'autorisation est applicable aux équipementiers comme aux opérateurs qui utilisent leurs produits. L'autorisation est délivrée aux équipementiers au titre de l'article R. 226-3 du code pénal pour une durée maximale de 6 ans, celle délivrée aux opérateurs au titre de l'article R. 226-7 pour une durée maximale de 3 ans.

b) Les limites du dispositif actuel face aux spécificités de la 5G

Si le droit en vigueur, a permis à l'État, par touches successives, de s'assurer de l'intégrité des réseaux jusqu'à la 4G, au regard des finalités recherchées, le dispositif de contrôle de la sécurité des nouveaux réseaux perd en efficacité au rythme actuel de l'évolution technologique :

---

administratives nécessaires. En effet, l'évolution technologique des équipements de télécommunication, qui permettent aux équipements d'interface en bordure de réseau d'accéder au contenu des flux d'information qu'ils transportent, ne serait-ce que pour hiérarchiser les flux en fonction de leur caractère prioritaire, multiplie de façon significative le volume des équipements concernés.

[1] *Autorité administrative indépendante, créée par la loi du 24 juillet 2015 en charge du contrôle de l'utilisation des techniques de renseignement par les services spécialisés de renseignement.*

• sa base légale conçue à une époque où ces réseaux servaient essentiellement à des correspondances privées est devenue trop étroite pour prendre en compte les applications industrielles qui constitueront les principaux usages de la 5G. Le régime ne porte que sur les équipements de nature à permettre une atteinte à l'intimité de la vie privée ou au secret des correspondances, et ne s'applique donc, par construction, qu'à des communications émises par et/ou à destination d'individus, et non aux communications de machine à machine ;

• le régime actuel se limite au contrôle de l'intégrité technique des équipements, tels qu'ils sont fournis par les équipementiers, sans prise en compte de l'architecture des réseaux en elle-même qui devient un élément-clef pour assurer leur sécurité et leur résilience. Il ne suffit pas à couvrir l'ensemble des enjeux de sécurité induits par la place plus importante des logiciels. Une analyse complémentaire des modalités d'exploitation adoptées par chaque opérateur devient indispensable ;

• en outre, l'entrée en vigueur tardive de l'extension de la liste aux équipements d'interface en bordure de réseau, notamment aux antennes-relais (*voir supra p.13*) pourrait conduire, par un effet d'aubaine, certains acteurs à presser leurs investissements afin de les réaliser avant la mise en œuvre des contrôles élargis prévue à partir du 1er octobre 2021 au préjudice de la sécurité et de la résilience des futurs réseaux 5G. Ce risque est probable car le déploiement de la 5G devrait être largement commencé à cette date, et pourrait accélérer la tendance à la mise en place d'une architecture distribuée permettant aux flux d'information de ne plus transiter systématiquement par les cœurs de réseau. Ce faisant la seule modification de la date prévue pour la mise en œuvre des contrôles, qui pourrait être réalisée par voie réglementaire, resterait insuffisante au regard des finalités exposées.

• enfin, les nouveaux usages soulèvent des problématiques différentes de la protection de la vie privée et du secret des correspondances, puisqu'ils nécessiteront avant tout d'assurer la disponibilité et l'intégrité des réseaux, face à des menaces potentielles de niveau stratégique.

Le dispositif prévu par la présente proposition de loi et le régime d'autorisation prévu notamment aux articles R. 226-3 et R. 226-7 du code pénal n'ont donc ni la même portée ni le même objectif *:*

• le dispositif R.226 traite de l'atteinte à la vie privée et s'applique donc indépendamment de l'opérateur de communications électroniques pour lequel les appareils et dispositifs prévus à l'article R. 226-1 seront utilisés ;

• la présente proposition de loi vise exclusivement les opérateurs d'importance vitale exploitants de réseaux de communications électroniques ouverts au public, dans un objectif de protection de la souveraineté et de sécurité des réseaux ;

- **les équipements visés par les deux dispositifs sont différents même si certains équipements pourront *in fine* être concernés par les deux dispositifs.**

2. La législation relative aux opérateurs d'importance vitale du secteur des télécommunications n'est pas adaptée

Comme il a été indiqué, la législation relative à la protection des opérateurs d'importance vitale, et notamment à certains de leurs systèmes d'information, est applicable aux opérateurs de réseaux radioélectriques mobiles *(voir supra p.20)*. L'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[1] » définit les règles de sécurité que les opérateurs d'importance vitale sont tenus de respecter pour protéger leurs systèmes d'information (annexe I), les délais dans lesquels les opérateurs sont tenus d'appliquer les règles de sécurité (annexe II), les modalités selon lesquelles les opérateurs déclarent à l'Agence nationale de la sécurité des systèmes d'information la liste de leurs systèmes d'information d'importance vitale identifiés par types de système (annexe III), ainsi que les modalités selon lesquelles les opérateurs déclarent à l'agence certains types d'incidents affectant la sécurité ou le fonctionnement de leurs systèmes d'information (annexe IV).

La Stratégie nationale de cyberdéfense justifie le renforcement du cybersécurité des opérateurs « supercritiques » par leur rôle de fournisseur de services auprès d'autres OIV[2] : « *les secteurs des communications électroniques et de l'approvisionnement en énergie électrique peuvent être qualifiés de « supercritiques ». Une attaque informatique à l'encontre d'un de ces acteurs est susceptible d'avoir des répercussions sur l'ensemble des activités d'importance vitale, et donc des effets potentiellement catastrophiques sur la résilience de l'ensemble de la Nation.* »

a) Des réseaux critiques pour la diffusion des attaques informatiques

Prenant en compte la place spécifique des réseaux de télécommunications dans la propagation d'une attaque informatique à fin de prévention et de détection, le code de la défense avait dès 2013 doté l'ANSSI de moyens accrus de prévention à l'égard des opérateurs en complétant pour partie les dispositions du code des postes et communications électroniques et pour partie celles du code de la défense. En particulier, l'article L. 2321-3 du code de la défense dispose que la sécurité des systèmes d'information des

---

[1] *Dont seuls le texte et l'annexe I ont fait l'objet d'une publication* https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033521327&categorieLien=id

[2] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/ *p.61*

OIV justifie que « *les agents de l'Autorité nationale de sécurité des systèmes d'information (…) peuvent obtenir des opérateurs de communications électroniques (…) l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système* ».

La loi n°2018-607 du 13 juillet 2018 de programmation militaire a renforcé les dispositifs de prévention et de protection :

- elle autorise les opérateurs à installer et exploiter sur leurs réseaux des dispositifs de détection des cyberattaques, dispositifs dont la mise en œuvre entraîne une obligation de déclaration, une obligation d'exploitation à la demande de l'ANSSI aux fins de prévenir une menace susceptible de porter atteinte à la sécurité des systèmes d'information et au besoin en recourant à des marqueurs techniques qu'elle leur fournira, une obligation d'information des évènements détectés et d'informer les abonnés à la demande de l'ANSSI (article L. 33-14 du code des postes et des communications électroniques). En outre, l'ANSSI pourra obtenir des opérateurs de communications électroniques, les données strictement nécessaires à l'analyse de cet évènement (article L. 2321-3 du code de la défense) ;

- elle autorise l'ANSSI à mettre en œuvre et à exploiter, dans des conditions définies par la loi, des systèmes de détection sur le réseau d'un opérateur ou sur le système d'information d'un fournisseur de service de communication au public en ligne dans les cas où l'ANSSI a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques ou des opérateurs d'importance vitale ou des opérateurs de services essentiels (article L. 2321-2-1 du code de la défense).

b) Avec l'arrivée des nouvelles technologies, l'enjeu est d'intervenir sur l'architecture des réseaux et les équipements mis en œuvre

Les dispositions existantes (articles L. 1332-6-1 et suivants du code de la défense) visant à garantir la cybersécurité des opérateurs d'importance vitale (OIV) n'offrent pas la souplesse requise pour répondre à ces enjeux. Elles reposent en effet sur la désignation de systèmes d'information d'importance vitale (SIIV), qui est du seul ressort des OIV, et sur l'application indifférenciée à l'ensemble de ces SIIV d'un ensemble de mesure de sécurité générique. Ce dispositif ne permet par conséquent pas la mise en œuvre de mesures techniques précises et propres à une technologie comme la 5G, ni l'appréciation au cas par cas des facteurs de risques qui semble justifiée au regard de la nouveauté et de la forte évolutivité des technologies.

Si ces mesures permettent d'améliorer la prévention et la détection des attaques, le renforcement, en raison de leur criticité spécifique, de la résilience des réseaux radioélectriques mobiles, exige une intervention législative afin de pouvoir disposer des leviers juridiques nécessaires pour imposer aux opérateurs des mesures contraignantes dans le choix de leurs équipements.

Ce régime ne s'appliquant qu'aux seuls réseaux radioélectriques mobiles, donc à un champ spécifique, les auteurs de la proposition ont naturellement opté pour une intervention du législateur dans le code des postes et télécommunications électroniques, plutôt qu'une intervention dans le code de la défense. Créer une législation spécifique à ces réseaux au sein des dispositions législatives relatives aux OIV qui présentent l'avantage d'une unicité de règle, la spécificité n'étant introduite qu'au niveau réglementaire par des arrêtés du Premier ministre, se serait avéré complexe.

B. LA PLUPART DES ÉTATS ONT PRIS CONSCIENCE DES ENJEUX

Le nombre d'opérateurs qui dans le monde auront lancé commercialement la 5G en 2020 est estimé à 170 environ. Les États-Unis, la Corée du Sud, le Japon et l'Australie ont déjà lancé la 5G avec une dizaine d'opérateurs. Six pays en Europe ont déjà attribué les fréquences spécifiques à la 5G et 12 autres ont déjà attribué des fréquences utilisables en 5G. Le processus d'enchères des fréquences 5G est en cours en Allemagne. Treize autres pays d'Europe ont annoncé des enchères 5G entre mi 2019 et fin 2020. La grande majorité des pays d'Europe aura donc ainsi lancé commercialement la 5G avant fin 2020. La grande majorité des opérateurs de Chine, du reste de l'Asie et du Moyen Orient lanceront également la 5G à cette période.

La plupart des États ont pris conscience des enjeux de sécurité représentés par le déploiement des nouvelles technologies. Ces enjeux sont évidemment variables selon le développement économique des États et notamment le degré de numérisation de la société. Certains de ces enjeux sont de nature géostratégique car le saut technologique et les potentialités économiques qu'offrent la 5G sont susceptibles d'avoir un effet disruptif sur l'équilibre des puissances.

Les enjeux stratégiques du déploiement de la 5G interfèrent dès lors avec la simple question de la sécurité des réseaux et sont devenus une partie importante de la « guerre commerciale » que se livrent la Chine et les États-Unis, autour de la question de savoir si l'on peut avoir une égale ou suffisante confiance en tous les équipementiers. Cette question qui doit être envisagée selon des critères multiples s'est focalisée, notamment aux États-Unis sur les craintes que les équipements chinois puissent constituer des « chevaux de Troie » dans les systèmes d'information supercritiques que sont devenus les réseaux radioélectriques mobiles de 5ème génération.

Cette question s'appuie sur le fait que la législation chinoise de 2017 fasse obligation aux entreprises ayant leur siège en Chine de collaborer avec les services de renseignement de ce pays et pour l'une d'entre elles, Huawei, sur le manque de transparence de son actionnariat et le soutien financier important dont elle a bénéficié de la part du gouvernement chinois, soit sous forme d'aides directes, soit sous forme de réduction d'impôt, soit sous forme

de crédits à l'export très favorables. Ces doutes légitimes ont été résumés dans une récente étude de l'Institut Montaigne[1].

La position de la France, et de nombreux autres États européens, à laquelle correspond d'ailleurs celle de l'Union européenne, n'est pas la même que celle des États-Unis dans la valorisation de ce critère pour l'équipement des futurs réseaux.

1. États-Unis

L'approche américaine de la sécurité des réseaux de 5G est fondée sur la sélection et l'agrément des fournisseurs d'équipements.

Les administrations américaines successives expriment publiquement, depuis une dizaine d'années au moins, leurs fortes réticences à voir des équipements de réseaux américains fournis par l'industrie chinoise, dont les deux premiers acteurs du secteur sont Huawei et ZTE et font obstacle à certains investissements de ces entreprises[2] , pression sur les opérateurs pour les dissuader d'utiliser des équipements[3] , exclusion de certains projets[4] ou marchés[5]. Il ressort également des débats au Congrès et de la lecture de la presse américaine que les États-Unis envisagent d'interdire aux entreprises américaines d'utiliser des équipements d'origine chinoise dans les réseaux critiques de télécommunications[6].

De telles mesures ont déjà été prises en Australie, où Huawei et ZTE sont écartés de la construction des réseaux de 5G[7]. Un refus d'installation formulé en Nouvelle-Zélande et les opérateurs japonais ont annoncé ne pas

---

[1] *Mathieu Duchâtel et François Godement, « L'Europe et la 5G : le cas Huawei» Institut Montaigne mai 2019*

[2] *Invocation de raisons de sécurité nationale pour s'opposer à la vente de la société américaine 3Com, spécialisée dans les équipements de réseaux, à Huawei en 2008*

[3] *Vis-à-vis de l'opérateur Sprint pour la construction de son réseau de 4G en 2011*

[4] *Huawei a été exclu du projet de câble sous-marin transatlantique* Hibernia Express

[5] *En 2018, les autorités américaines ont interdit l'utilisation des équipements de Huawei et de ZTE dans les principaux réseaux des administrations publiques américaines.*

[6] *Le président Donald Trump a adopté un executive order, daté du 15 mai 2019, visant à permettre au secrétaire américain du commerce d'interdire toute transaction portant sur l'acquisition ou la mise en œuvre par une entité publique ou privée américaine de produits ou services dans le domaine numérique, dès lors que ces produits ou services reposeront sur une technologie contrôlée par un « adversaire étranger », et poseront un risque pour la sécurité nationale américaine (notamment, mais pas exclusivement, pour la résilience et la sécurité d'infrastructures critiques). Cette décision appelle des travaux subséquents de déclinaison concrète de ses orientations (notamment pour la définition précise de ce qui constitue un adversaire étranger), mais semble bien viser une interdiction à large portée (non limitée aux seuls opérateurs de télécommunications) de certains fournisseurs.*

[7] *En août 2018, l'Australie a signifié aux entreprises Huawei et ZTE qu'elles seraient exclues des futurs réseaux 5G. Cette interdiction fait écho aux mesures de sécurité déclinées dans la loi* « Telecommunications sector security reforms » *de 2017, qui confère au gouvernement des pouvoirs de contrôle et de prescription vis-à-vis des opérateurs sur tout sujet pouvant affecter la sécurité nationale. Elle est formellement motivée par la loi chinoise sur le renseignement de 2017.*

souhaiter s'appuyer sur des fournisseurs chinois pour leurs réseaux 5G. Les équipementiers chinois sont aussi absents des réseaux mobiles en Israël.

Enfin, les États-Unis déconseillent ouvertement à leurs alliés d'ouvrir l'équipement de leurs réseaux à des fournisseurs « non dignes de confiance » soulignant les « *questions d'intégrité et de confidentialité des communications sensibles* » et la menace que cela pourrait représenter pour la coopération et les échanges d'informations.

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

2. Allemagne

L'Allemagne travaille à l'élaboration de normes qui seront rendues obligatoires pour les équipements des réseaux 5G.

L'autorité allemande de régulation des télécommunications (*Bundesnetzagentur*) a en effet rendu publique, le 7 mars 2019, une liste de nouvelles exigences ou recommandations de sécurité, élaborées avec le concours de l'homologue allemand de l'ANSSI (BSI – *Bundesamt für Sicherheit in der Informationstechnik*) qu'elle souhaite rendre applicable aux réseaux 5G. Cette liste met notamment l'accent sur des procédures de certification des équipements de télécommunication, et recommande aux opérateurs d'éviter la dépendance exclusive envers un fournisseur unique, et de s'appuyer sur des fournisseurs de confiance.

Ce travail est ambitieux, s'il veut tendre à l'exhaustivité ce qui serait nécessaire en termes de sécurité, et complexe dans la mesure où le développement de la technologie n'est encore totalement stabilisé et que celle-ci connaît des évolutions permanentes. Les travaux de standardisation de la 5G ne seront pas terminés avant fin 2019. Les équipementiers réalisent un travail de normalisation mais qui est loin d'être achevé et risque, au rythme du progrès technique, de ne pas être figé dans le temps. L'actualisation des normes sera donc nécessaire pour répondre à l'objectif de sécurité et de résilience.

Ce dispositif n'est par ailleurs pas utilisé à ce jour, dans la mesure où la liste publiée le 7 mars ne l'a été qu'afin d'engager des concertations avec l'industrie, et qu'elle ne prendra de portée contraignante qu'à l'issue de ces consultations, au plus tôt à l'automne. Les exigences et recommandations contenues dans cette liste nécessiteront vraisemblablement des précisions (définition de la notion de fournisseur de confiance) voire de conséquents travaux complémentaires (établissement d'un cadre de certification adapté) pour acquérir un réel caractère prescriptif.

3. Royaume-Uni

La question au Royaume-Uni est controversée au sein du gouvernement. La position britannique n'est pas totalement arrêtée oscillant entre des partisans d'un alignement sur les positions américaines et l'attitude pragmatique qui a conduit jusqu'à maintenant à l'ouverture du marché britannique aux produits chinois et l'autorité britannique en charge de la cybersécurité à travailler étroitement, mais sans complaisance avec les équipementiers. Cette pratique libérale de partenariats publics-privés a conduit à la mise en place de structures d'évaluation des équipements qui publient des rapports d'évaluation et éclairent les décisions des autorités britanniques. Ainsi le Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board est un organisme, financé par le groupe Huawei à la demande du gouvernement britannique, présidé par le patron du Centre national de cybersécurité britannique (NCSC). Depuis 2010, il étudie les risques posés par son implication de ces fournisseurs dans l'équipement des réseaux de télécommunications du Royaume-Uni et procède à des expertises techniques des matériels et logiciels employés[1].

British Telecom a fait connaître publiquement son intention d'expurger les parties sensibles de ses réseaux de 3G et 4G des équipements chinois, et de ne pas y avoir recours pour une large part de son futur réseau de 5G, mais cette entreprise n'est pas le seul opérateur en Grande-Bretagne.

C. L'ÉLABORATION DE NORMES EUROPÉENNES INTERVIENDRA AVEC RETARD

Les États prennent conscience des enjeux autour de ces nouveaux réseaux, mais réagissent à ce stade en ordre dispersé. La carte interactive publiée sur le site de l'Institut Montaigne fournit des informations à jour sur l'attitude des différents États de l'Union européenne sur cette question[2].

La souveraineté et la sécurité des États, entreprises et sociétés civiles dans le contexte du déploiement des réseaux 5G dépendra nécessairement d'une réponse réglementaire, économique et politique.

Ce faisant les conditions du déploiement de la 5G relèvent, en effet, d'une compétence nationale exclusive.

---

[1] *Son dernier rapport se montre particulièrement critique ;il souligne des problèmes de sécurité récurrents dans les équipements analysés, créant des risques à long terme pour les réseaux Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board – Annual Report 2019.- A report to the National Security Adviser of the United Kingdom March 2019.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf https://www.lesechos.fr/tech-medias/hightech/huawei-un-rapport-au-vitriol-publie-par-des-experts-britanniques-1004599

[2] https://www.institutmontaigne.org/publications/leurope-et-la-5g-le-cas-huawei-partie-2

Les actions menées au niveau communautaire ont pour objectif de faciliter la mise en place de ces réponses nationales, sans leur substituer des dispositions de niveau européen. Les travaux menés actuellement visent, d'une part le partage entre États Membres des analyses de risque nationales, et d'autre part, la création d'une « boîte à outils de dispositifs européens susceptibles de faciliter la mise en œuvre de mesures nationales (en particulier, un cadre harmonisé d'évaluation des caractéristiques techniques des équipements 5G, qui permettrait de mutualiser les travaux d'analyse technique conduits par les différents États Membres).

Votre Rapporteur souligne néanmoins l'importance et l'urgence de ce travail. Avec l'interconnexion des réseaux, la cybersécurité à l'échelle de l'Europe se mesure à l'aune des réseaux les moins protégés. Un effort important reste à conduire pour mettre à niveau certains États et assurer un niveau de sécurité et de résilience acceptable de l'ensemble européen.

Ces travaux communautaires ne devraient par conséquent pas avoir d'impact sur le cadre législatif national, mais éventuellement faciliter à terme l'instruction des demandes d'autorisation qui pourrait s'appuyer pour partie sur des dispositifs issus de la « boite à outils ».

La politique suivie par l'Union européenne

L'Union européenne propose que les États échangent des informations, avec le soutien de la Commission et de l'Agence de l'Union européenne pour la cybersécurité. Elle souhaite que chaque État soit conscient des risques et prenne les mesures nécessaires pour y faire face.

Un travail a été engagé pour parvenir à l'élaboration de recommandations pour une approche commune. Ainsi, le Conseil européen, à l'issue de sa réunion du 22 mars 2019, considérant qu'« *il convient d'accorder une attention particulière à l'accès aux données, à leur partage et à leur utilisation, à la sécurité des données et à l'intelligence artificielle, dans un environnement de confiance* » a appelé la Commission à publier une recommandation relative à une approche concertée en matière de sécurité des réseaux de 5G.

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

Au niveau national, la Commission recommande que chaque État membre évalue les risques liés aux infrastructures des réseaux 5G avant juin 2019, tenant compte « *de différents facteurs, tels que les risques techniques et les risques liés au comportement des fournisseurs ou des opérateurs, y compris ceux de pays tiers* ». Sur la base de cette évaluation, les États sont invités à mettre à jour les exigences de sécurité existantes pour les fournisseurs de réseaux ainsi que les conditions d'octroi des droits d'utilisation des fréquences dans les bandes qui seront ouvertes pour la 5G. Ils peuvent prendre, le cas échéant, les mesures nécessaires pour garantir « *l'obligation renforcée, pour les fournisseurs et les opérateurs, de garantir la sécurité des réseaux* » de 5G.

La Commission européenne souligne que les mesures prises par les États membres pour assurer la sécurité des points sensibles des réseaux « *devront inclure des obligations renforcées pour les fournisseurs et les opérateurs* » :

- les autorités compétentes à l'échelle nationale pourront demander la communication de toute information leur paraissant nécessaire avant toute modification des réseaux de communications électroniques par un acteur du secteur ;
- elles pourront également contraindre, pour des raisons de sécurité et d'intégrité des réseaux, les fournisseurs et les opérateurs à utiliser des équipements et des systèmes de traitement de l'information préalablement testés.

Au-delà des facteurs techniques le comportement des fournisseurs, et notamment l'influence qu'un « pays tiers » pourrait exercer sur eux, devrait être pris en compte dans l'évaluation des risques pesant sur les réseaux 5G. En conséquence, la Commission a affirmé clairement le droit, pour les États membres de l'Union européenne, « *d'exclure des prestataires ou des fournisseurs de leurs marchés pour des raisons de sécurité nationale* ».

La France se situe plutôt en avance dans cette mobilisation et le cadre européen envisagé paraît compatible avec la législation envisagée. La lecture de cette recommandation montre que la présente proposition de loi s'inscrit pleinement dans la continuité de la position de la Commission européenne.

Pour autant, selon certains observateurs, l'Union européenne afin de peser face à des acteurs soutenus par des marchés domestiques puissants, de minimiser les coûts et donc d'éviter les retards, devrait apporter une réponse européenne coordonnée qui assure un niveau d'exigence élevé dans l'ensemble des pays membres. En effet, les acteurs européens ne peuvent pas être les plus efficaces et rapides possible s'ils doivent respecter des régulations différenciées dans chacune des zones dans lesquelles ils opèrent.

En outre, la législation sera insuffisante. La capacité de la France et de l'Europe à soutenir l'émergence d'acteurs alternatifs de cet écosystème est certainement l'une des conditions *sine qua non* pour garantir sa souveraineté. L'Institut Montaigne formule quelques orientations, pour y parvenir dans une récente étude[1]. Le Sénat a créé une commission d'enquête sur la souveraineté numérique qui rendra ses conclusions en octobre 2020[2].

D. L'INTERVENTION DU LÉGISLATEUR DOIT ÊTRE EN PHASE AVEC LE DÉPLOIEMENT DE LA 5G

Le déploiement des réseaux de 5G étant prévu dans des délais très rapides, la modernisation du cadre juridique du contrôle de leur sécurité revêt donc un caractère d'urgence.

Au niveau international, les premiers déploiements et commercialisations des services 5G ont été rendus possibles par *Samsung*, *Ericsson*, *Nokia*, et *Huawei*. Aux États-Unis, *Verizon* et *AT&T*, ont commercialisé en octobre et en décembre 2018 respectivement des box 5G qui fournissent l'accès à l'internet très haut débit au domicile via une

[1] *Institut Montaigne mai 2019 « L'Europe et la 5g: passons la cinquième » (note sous la supervision de Gilles Babinet) p.15 et suivantes et « L'Europe et la 5G : le cas Huawei» (Rapporteurs : Mathieu Duchâtel et François Godement) p.15 et suivantes.*

[2] http://www.senat.fr/commission/enquete/souverainete_numerique.html

antenne 5G. Ces commercialisations américaines ont été suivies par la Corée du Sud, dont les opérateurs nationaux ont lancé une offre à destination des entreprises en décembre 2018 et des offres grand public en avril 2019.

Des expérimentations de technologies de 5G ont été lancées en France en 2018, l'attribution de bandes de fréquences spécifiques est prévue pour la fin de l'année 2019[1] et le déploiement d'équipements de 5G doit commencer dès 2020. Le passage à la 5G sera probablement graduel.

Compte tenu de la nouveauté des technologies de 5G et à l'aube de son déploiement qui va nécessiter des investissements très importants (fréquences, équipements de réseaux) afin de tendre vers le niveau de qualité de service et de couverture attendu par les consommateurs, les entreprises et les pouvoirs publics, **les opérateurs ont besoin d'un cadre juridique et technique clair pour garantir la fiabilité de leurs équipements et les conditions dans lesquelles ils pourront les exploiter**. À cet égard, il est important que les dispositions envisagées et leurs mises en œuvre opérationnelles minimisent l'insécurité juridique pour les opérateurs concernés. L'expérience de la 4G a montré qu'il est plus simple pour l'industrie que les pouvoirs publics fixent d'emblée une doctrine claire sur diverses questions techniques, étant entendu qu'une concertation est nécessaire lors de l'instruction des demandes d'autorisation.

Ce besoin a été rappelé par l'ARCEP dans son avis n° 2019-0161 en date du 4 février 2019 sur le projet d'amendement déposé par le gouvernement lors de la lecture au Sénat du projet de loi PACTE[2], dans lequel elle a indiqué qu'il convenait « *d'une part, que le cadre et les modalités associées à ce nouveau dispositif soient les plus claires possibles pour que les opérateurs puissent en tenir compte dans leur stratégie de déploiement de la 5G en particulier et de l'ensemble des technologies utilisées sur les réseaux mobiles en général, et, d'autre part, que les éventuels effets rétroactifs (mêmes indirects) des décisions prises dans le cadre de ce dispositif sur les déploiements passés soient évalués* » .

Cette approche concertée a été celle de l'ANSSI pour la mise en œuvre des articles R. 226-3 et R 226-7 du code pénal (voir supra), comme pour l'édiction des règles spécifiques applicables aux systèmes d'importance vitale (*voir supra p.21*). Un cadre d'application strict et une application souple de la loi reste la meilleure garantie d'une approche équilibrée entre l'impératif de sécurité et les objectifs de développement économique attendus de cette nouvelle technologie.

---

[1] *Le code européen des communications électroniques exige d'attribuer les « bandes cœur » fin 2020.*

[2] *Avis n° 2019-0161 de l'Autorité de régulation des communications électroniques et des postes en date du 4 février 2019 sur un projet de texte visant à instaurer un régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques*
https://www.arcep.fr/uploads/tx_gsavis/19-0161.pdf

III. LE DISPOSITIF PROPOSÉ

L'approche française de la sécurisation des réseaux de 5G ne fait pas reposer autant qu'aux États-Unis la résilience de ces réseaux sur le seul agrément des équipementiers. Au contraire, l'objectif poursuivi consiste à établir un cadre clair pour que les industriels planifient leurs investissements permettant à l'État de maîtriser, grâce à un nouveau régime d'autorisation administrative, le déploiement de certains des équipements, tant matériels que logiciels, afin de conserver la maîtrise de l'architecture et de s'assurer de la résilience des réseaux de 5G. Il procède d'un souci d'équilibre entre les impératifs de sécurité et de soutien au développement du numérique sur l'ensemble du territoire.

A. UN RÉGIME D'AUTORISATION DESTINÉ À PRÉSERVER LES INTÉRÊTS DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Le nouvel article L. 34-11 (**alinéa 4**) soumet à **une autorisation du Premier ministre** l'exploitation, sur le territoire national, « *d'appareils, à savoir tous dispositifs matériels ou logiciels* » qui permettent la **connexion au réseau radioélectrique mobile**.

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

La rédaction proposée pour le I. de l'article L. 34-11 du code précité par les **alinéas 4 et 5** vise à soumettre à une autorisation préalable du Premier ministre l'exploitation, sur le territoire national, certains appareils, « *à savoir tous dispositifs matériels ou logiciels* », permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, dès lors que « *leurs fonctions présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation* » dudit réseau.

L'autorisation est explicitement « *destinée à préserver les intérêts de la défense et de la sécurité nationale* » ce qui constitue une base juridique nouvelle par rapport au droit existant fondé sur la protection des correspondances et de la vie privée (*voir supra p.25*). Le régime proposé ne se substitue pas au régime existant dit du « 226-3 du code pénal », mais le complète.

2. Un régime applicable aux opérateurs d'importance vitale dans le secteur des télécommunications.

a) Le régime nécessaire en raison de la « criticité » élevée de leur activité

L'obligation porte ainsi sur les seuls opérateurs d'importance vitale exploitants de réseaux de communication téléphonique ouverts au public alors que le régime prévu pour l'application de l'article 226-3 du code pénal porte sur les équipementiers (article R.226-3) et sur les opérateurs (article R. 226-7).

Les opérateurs visés par cette autorisation sont les opérateurs reconnus d'importance vitale (OIV) en application des articles L. 1332-1 du code de la défense, appartenant au secteur des télécommunications qui exploitent ces appareils directement ou par l'intermédiaire de leurs fournisseurs en vertu de leur activité d'exploitant, direct ou par l'intermédiaire de tiers fournisseurs, d'un réseau de communications électroniques ouvert au public. La liste de ces opérateurs est confidentielle, mais on peut avancer sans trop de risque qu'elle comprend les quatre principaux opérateurs nationaux.

b) Un régime qui ne s'applique pas aux opérateurs dits verticaux

L'Assemblée nationale avait adopté dans un premier temps un amendement de sa commission de la défense et des forces armées tendant à étendre ces règles à l'ensemble des opérateurs d'importance vitale et non aux seuls assurant une activité d'exploitants d'un réseau de communications électroniques ouvert au public. Cette extension du champ d'application de la proposition de loi visait au sein des OIV, les opérateurs dits « verticaux », c'est-à-dire ceux qui pour les besoins de leurs activités utilisent des réseaux de radiocommunication privée (« *Private Mobile Radiocommunication »/ PMR)*.

Les réseaux « PMR »

Les réseaux mobiles professionnels (dits PMR) sont des réseaux mobiles indépendants, d'ampleur généralement locale ou régionale, exploités par des entreprises de tailles très diverses (depuis le professionnel indépendant jusqu'aux grands groupes) et de différents secteurs d'activités pour leurs propres usages professionnels, tels que les transports (entreprises de transports routiers, sociétés de bus, de taxis, services aéroportuaires, sociétés d'autoroutes, ambulanciers…), la sécurité et le gardiennage, le bâtiment et les travaux publics, l'énergie (sociétés de distribution d'électricité), l'industrie, des associations dans le cadre d'activités sportives ou de loisirs.

Des réseaux « PMR » sont également utilisés par certains services de l'État, des hôpitaux, des collectivités locales, ainsi que certains établissements publics.

Comme les autres utilisations du spectre par des services de communications électroniques, l'utilisation de fréquences par de tels réseaux est soumise à autorisation d'utilisation de fréquences délivrée par l'ARCEP. Ce n'est toutefois pas le cas de ceux exploités par le ministère de l'intérieur et le ministère de la défense qui sont eux-mêmes affectataires de bandes de fréquences au même titre que l'ARCEP.

Les utilisations de réseaux professionnels concernent un nombre très élevé d'installations. En avril 2018, 24 916 réseaux PMR avaient fait l'objet d'une autorisation attribuée à titre individuel par l'ARCEP. À cela s'ajoutent les nombreuses utilisations dans des bandes libres, c'est-à-dire non soumises à autorisation individuelle.

Les conditions générales d'établissement et d'exploitation de ces réseaux sont définies aux articles L. 33-2 et D. 99 et suivants du code des postes et des communications électroniques (CPCE). Les exploitants de réseaux indépendants peuvent bénéficier d'attribution de fréquences dans les limites prévues aux articles L. 42 et suivants du CPCE.

Dans les bandes de fréquences 50 MHz, 60 MHz, 80 MHz, 160 MHz et 400 MHz, dont l'ARCEP est affectataire, l'utilisation de ces fréquences est soumise à une autorisation préalable délivrée par l'ARCEP à l'utilisateur à titre individuel.

Ces réseaux reposent aujourd'hui sur des technologies robustes mais bas débit (2G). Aussi depuis le 9 mai 2019 l'ARCEP attribue, sous réserve de leur disponibilité, les fréquences 2575 - 2615 MHz de la bande 2,6 GHz TDD dans des zones circonscrites de France métropolitaine, correspondant aux zones où une couverture mobile spécifique est nécessaire afin de répondre aux besoins de couverture en très haut débit des professionnels.

L'Assemblée nationale a finalement renoncé à cette disposition à la demande du gouvernement après que celui-ci a sollicité une deuxième délibération.

Le gouvernement considère que le risque est suffisamment couvert par les dispositions applicables aux OIV, qu'il s'agisse de celles relatives aux plans de continuité (*voir supra p.19*) de service ou de celles relative à la sécurité des systèmes d'information, et que ces dispositions sont, en l'état, suffisantes. En effet, ces opérateurs verticaux ne sont pas désignés OIV en vertu des réseaux qu'ils opèrent, mais au titre d'autres activités. L'impact d'un dysfonctionnement de leur réseau de communications mobiles sur ces activités critiques dépendra tant de l'usage que ces opérateurs verticaux feront de leurs réseaux 5G, que de l'adhérence éventuelle de leurs activités critiques à ces réseaux. La contribution de ces réseaux aux activités d'importance vitale des opérateurs verticaux pourrait être appréciée dans le cadre des dispositions régissant ces activités (découlant des articles L. 1332-6-1 et suivants du code de la défense), mais n'est pas avérée a priori et ne semble par conséquent pas justifier à ce stade une logique d'autorisation préalable[1].

[1] *D'ores et déjà, pour leurs systèmes d'information les plus sensibles, les OIV procèdent à une séparation stricte entre les réseaux critiques sensibles et les autres et travaillent étroitement avec l'ANSSI qui conduit des audits périodiques. Ils sont également audités très régulièrement au titre de*

Il considère également que les possibilités de « privatisation » de parties des réseaux des opérateurs de réseaux de télécommunication ouverts au public (slicing) au profit d'OIV inciteront au développement de certains services via ces réseaux couverts par les dispositions de la présente proposition de loi.

La 5G offre une opportunité aux opérateurs « verticaux » de sortir du concept de réseaux privatifs pour certaines utilisations

Dans le cadre de la consultation publique de l'Arcep « Attribution de nouvelles fréquences pour la 5G », certains opérateurs verticaux ont indiqué leur intérêt pour la technologie 5G mise en œuvre dans un modèle de réseau grand public, si toutefois son introduction dans les réseaux des opérateurs nationaux ouvre la voie à l'émergence d'offres innovantes, performantes aussi bien sur le plan technique qu'économique, et capables de supporter des usages métiers que les réseaux grand public 4G n'adressent pas. En d'autres termes, ils se tiennent à l'écoute des opérateurs mobiles qui ambitionnent de fournir à des acteurs verticaux, via la technologie 5G, des solutions permettant à ceux-ci de sortir du concept de réseaux privatifs.

Le modèle de réseau privatif, mis en œuvre de longue date par les opérateurs verticaux, restera pertinent, pour tous les environnements métiers non adressables par des réseaux grand public. C'est typiquement le cas aujourd'hui, eu égard :

- aux environnements contraints ou zones spécifiques (par exemple espaces souterrains, tunnels, emprises nucléaires, zones techniques profondes) au sein desquels les acteurs professionnels exercent leurs missions ;

- au respect des dispositions légales (par exemple celles de la loi de programmation militaire) auxquelles sont soumis certains acteurs professionnels.

- à la nécessité en termes de sécurité de l'activité de disposer de réseaux redondés pour maintenir la continuité et l'intégrité du service.

Enfin, s'agissant d'applications nouvelles ou innovantes, développées par des OIV ou par d'autres opérateurs :

- soit elles se développeront via les réseaux des opérateurs de réseaux de télécommunications ouverts au public et auxquels cas, elles relèveront des dispositions proposées,

- soit il s'agira de services assimilables à ceux proposés par ces opérateurs auxquels cas ces opérateurs « verticaux » seront assimilés à des opérateurs de réseaux de télécommunications ouverts au public. Ils pourraient, par ailleurs, voir leurs activités d'importance vitale amendées pour inclure les réseaux de télécommunications, si le périmètre de ces derniers leur conférait une criticité au regard des enjeux de défense et de sécurité nationale,

la sécurité interne de chaque opérateur, notamment lorsque ces activités peuvent induire des risques pour les usagers, les salariés ou la population.

• soit enfin, ces réseaux seront privatifs et dans cette hypothèse il faudra analyser les risques au regard de la sécurité nationale et, le cas échéant, les intégrer dans la liste des opérateurs d'importance vitale.

La maturité actuelle de la 5G ne permet pas, à ce stade, d'envisager ou d'imaginer tous les développements d'activités et de services possibles, ni leurs modalités. Il est sans doute prématuré d'intervenir dès aujourd'hui pour mettre en place un cadre juridique qui risque de s'avérer inadapté, ou trop large ou trop contraignant et décourageant le développement des opportunités offertes par ces technologies.

Votre rapporteur en convient. Ce faisant, il souhaite que le SGDSN et l'ANSSI, ainsi que les ministères concernés par les activités d'importance vitale soient extrêmement attentifs aux évolutions en cours et vigilants dans l'appréciation des activités d'importance vitale pour en revoir régulièrement le périmètre, dans le contrôle des déclarations des systèmes d'information des OIV asservies aux nouvelles activités des OIV, et dans l'adaptation des prescriptions des plans de continuité et des contrôles de l'ANSSI sur les systèmes d'information d'importance vitale.

Au-delà de l'adaptation du cadre réglementaire, il souhaite qu'une évaluation du dispositif prévu par la présente proposition puisse intervenir régulièrement au regard du développement des nouveaux services et activités mis en œuvre ou projetés et qu'au besoin, la loi puisse être adaptée ou étendue afin d'assurer de préserver les intérêts de défense et de sécurité nationale qui constituent la finalité de cette évolution législative. En effet, si comme certains le prévoient, la frontière entre réseaux publics et réseaux privés s'efface, le risque systémique s'étendra probablement au-delà des réseaux des quatre grands opérateu**rs** de téléphonie mobile actuels et il y aura peut-être lieu à intervenir si les dispositifs mis en place s'avèrent insuffisants.

À ce stade, à la différence de l'Allemagne[1], les premières enchères pour l'exploitation de fréquences destinées à l'installation de réseau de 5G, dont les résultats sont attendus à la fin de l'année, ne seraient ouvertes qu'aux opérateurs de télécommunications. Dans la lettre d'orientation adressée au Président de l'ARCEP le 10 mai 2019[2], les ministres indiquent que « *s'il ne considère pas a priori nécessaire de réserver une partie du spectre pour de tels acteurs le gouvernement souhaite que l'ARCEP s'assure que les opérateurs qui bénéficieront d'autorisations dans cette bande de fréquences permettront aux acteurs des « verticales » de l'économie de solliciter dans des conditions financières et opérationnelles adaptées à leurs besoins y compris dans les zones peu denses du territoire, et notamment dans des territoires d'industrie* » .

---

[1] *En Allemagne, 100 MHz de bandes hertzienne ont été réservés aux opérateurs « verticaux » dans l'allocation des fréquences dédiées à la 5G allemande.*

[2] *https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=ACDD5F68-767C-42B6-9A54-86E0EA96420B&filename=1214%20-%20CP%20et%20lettre%20de%20cadrage%20orientations%205G.pdf*

3. Un régime qui couvre un nombre important mais limité d' « appareils »

Le régime proposé, constitue un nouveau régime d'autorisation qui dans un objectif de stricte suffisance est limité aux appareils qui « *présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau* » et exclut les appareils installés chez les utilisateurs finaux (**alinéa 4**).

Les opérateurs de communications électroniques principalement concernés par les dispositions de cet article sont contraints de s'équiper en appareils de réseau sur un marché oligopolistique : *Nokia, Ericsson* et *Huawei* sont leurs principaux équipementiers, tandis que *Samsung* fait office d'entrant potentiel, concentré toutefois sur les équipements 5G et que *CISCO* fournit principalement des systèmes spécifiques des routeurs et des interrupteurs.

Présence des équipementiers

	Huawei	Ericsson	Nokia	Samsung
Part de marché (Monde) *	21%	27%	22%	5%
Part des équipements (France)**	28,72%	28,55%	42,73%	0%

(*)IHS Markit, 2018, https://techblog.comsoc.org/2019/04/03/huawei-led-global-4g-lte-infrastructure-market-which-totalled-22-9b-in-2018/
(**) Part des sites équipés tous opérateurs confondus (source : FFT)

a) Les appareils concernés

Ces appareils figureront sur une liste établie par arrêté du Premier ministre (**alinéa 6**) après avis de l'ARCEP. Cet arrêté est actuellement en préparation de façon à ce que les opérateurs puissent prendre connaissance de cette liste avant de planifier leurs investissements.

La liste de ces appareils ne coïncidera pas nécessairement avec celle prévue à l'article R 226-1 du code pénal pour la délivrance des autorisations de fabrication, d'importation, d'exposition, d'offre de location ou de vente » délivrées aux fournisseurs au titre de l'article R 226-3 et d'acquisition ou de détention aux opérateurs en application de l'article R 226-7 du même code. La coïncidence sera sans doute plus grande à partir du 1er octobre 2021 lorsque la liste des appareils visés par l'article R 226-1 sera étendue en application de l'arrêté du 11 août 2016 pris pour l'application de l'article 23 de la loi n° 2013-1168 du 18 décembre 2013 de programmation militaire (2014-2019) (*voir supra p.26*) mais ne sera pas totale. Certains appareils relèveront des deux régimes, d'autre d'un seul des deux, car ils n'obéissent pas aux mêmes finalités et les modalités de contrôle seront différentes même si ce contrôle est réalisé par le même centre d'expertise de l'ANSSI. Il n'est pas envisagé de conditionner systématiquement les autorisations au titre de l'article L. 34-11 à l'obtention préalable d'une autorisation au titre de

l'article R.226-3, dans la mesure où les deux dispositifs n'ont pas strictement les mêmes champs d'application.

b) L'exclusion des appareils installés chez les utilisateurs finaux

L'exclusion des équipements déployés chez les utilisateurs finaux vise à sortir du champ du contrôle tant les équipements terminaux, que les équipements de desserte locale à très courte portée déployés au profit d'un utilisateur particulier, 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 auquel la proposition de loi apporte une réponse..

Cette exclusion ne vise en revanche pas à exclure du champ du contrôle les réseaux professionnels d'entreprises (de type PMR). Ces réseaux seront de fait exclus du contrôle, centré sur les réseaux ouverts au public, 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) conduisent néanmoins d'envisager, à terme, des réseaux professionnels adossés aux réseaux publics, et qui en partageraient les éléments d'infrastructure. Il entre bien dans l'objet de la proposition de loi de soumettre, dans ce cas, les éléments d'infrastructure mutualisés au contrôle.

4. Une procédure d'autorisation *a priori*

La rédaction proposée pour le II. de l'article L. 34-11 du code des postes et des communications électroniques décrit la procédure de présentation de demandes et en fixe la durée des autorisations délivrées.

a) La demande est présentée par l'opérateur

L'**alinéa 7** confirme que l'autorisation est octroyée après examen d'un dossier de demande remis par l'opérateur. Celui-ci est donc bien l'interlocuteur unique du Premier ministre et du service instructeur l'ANSSI. Il est responsable de la cohérence de l'architecture de son réseau et de la fiabilité de son exploitation, des équipements mis en œuvre, et des modes d'organisation retenus, notamment par le recours à la sous-traitance de certaines fonctions.

La virtualisation et le passage à des implémentations logicielles des principaux équipements confèrent une liberté accrue aux opérateurs dans les choix de déploiement et de mise en œuvre de ces équipements et, par conséquent, un rôle accru dans leur sécurisation. Ceci justifie que le régime de contrôle proposé porte sur les modalités d'exploitation, et donc les opérateurs qui en ont la responsabilité, plutôt que sur les seules caractéristiques propres des équipements.

b) Un régime aussi souple que possible pour les mises à jour

Le premier alinéa du texte proposé (**alinéa 7**) précise que l'autorisation est donnée pour « *un ou plusieurs modèles* » et « *une ou plusieurs versions* » des appareils susmentionnés.

Il s'agit d'**éviter que toute mise à jour logicielle ou que toute modification technique d'un équipement déjà contrôlé soit systématiquement soumise à une nouvelle procédure** d'autorisation préalable, dans les mêmes formes que l'autorisation initiale.

Ainsi, l'ANSSI pourra choisir de traiter les mises à jour au cas par cas, suivant trois modalités :

- pour les cas les plus simples, l'autorisation du matériel ou du logiciel initial pourra porter également sur certains types de mises à jour ;
- le cas échéant, l'ANSSI pourra assortir l'autorisation du matériel ou du logiciel initial d'une obligation de déclaration de certains types de mises à jour ;
- pour les cas comportant des risques éventuels, les mises à jour pourront être soumises à autorisation au même titre que le matériel ou le logiciel initial.

Votre rapporteur comprend le souci d'éviter de possibles lourdeurs administratives et de garantir, en conséquence, la liberté et la rapidité de déploiement des réseaux de communications électroniques. Il estime que la rédaction proposée est suffisamment large pour garantir une liberté d'appréciation à l'ANSSI. Une intervention législative pour définir les notions de mise à jour mineure ou majeure ou les distinguer de la notion de version serait périlleuse et risquée car ces notions relèvent pour l'essentiel du fournisseur et de sa politique commerciale autant que du contenu technique des matériels et des logiciels[1] et que certains fournisseurs s'orientent vers des mises à jour en continu par télétransmission. Il appartiendra donc à l'ANSSI dans ces conditions d'utiliser la durée de l'autorisation pour s'assurer régulièrement de la fiabilité des logiciels au regard de la sécurité nationale. En effet, en termes de sécurité, les risques d'introduction de failles logicielles, voire de « portes dérobées » sont aussi grands à l'occasion d'une simple mise à jour qu'à l'occasion d'un changement de version.

---

[1] *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) d'une part, et majeures (évolutions du périmètre fonctionnel, par exemple support de nouveaux protocoles ou de nouvelles révisions des normes) d'autre part. 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.*

c) La prise en compte du périmètre géographique d'exploitation

Selon sa stratégie d'équipement, un opérateur, a soit acquis auprès d'un fournisseur l'intégralité des éléments du réseau 2G-3G-4G pour une zone géographique définie, soit distingué les fournisseurs selon les différentes composantes du réseau – les équipements « cœur de réseau » pouvant, par exemple, être distingués de ceux présents sur ses extrémités.

L'**alinéa 7** précise que l'autorisation est délivrée « *pour un périmètre géographique* » déterminé par l'opérateur dans sa demande. Cette procédure qui va au-delà de l'appréciation de la seule intégrité technique des matériels, permettra à l'État de contrôler l'architecture des réseaux du point de vue de leur agencement géographique. Elle permet à l'État :

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

- d'**éviter un monopole d'équipement** dans certaines zones et, avec le développement de la concurrence, pousser les opérateurs et les équipementiers à rechercher les voies et moyens d'une plus grande interopérabilité de leurs réseaux. C'est à ce titre que le zonage sera apprécié non seulement au regard de la sensibilité des installations de la zone concernée, mais aussi de façon à **garantir la résilience des réseaux en cas de défaillance – involontaire ou non – d'un équipement**. L'objectif est de permettre, en cas de défaillance, la bascule du trafic, probablement en mode dégradé, sur un brin du réseau redondé avec un équipement d'une autre marque ou d'un autre modèle, qu'il s'agisse d'équipement du même opérateur sur sa plaque géographique ou du réseau d'un autre opérateur sur une plaque géographique couvrant peu ou prou la même zone géographique, afin d'assurer la continuité du service.

En règle générale, les opérateurs opèrent des zonages en six ou sept plaques importantes sur le territoire métropolitain et quelques plaques spécifiques communes à des équipements particuliers (stades, centres commerciaux, zones blanches…). Il est peu probable qu'ils créent une zone spécifique autour d'une installation isolée intéressant la défense. En effet, le zonage n'est donc pas imposé par l'État.

L'objectif consiste à **éviter une homogénéité trop poussée des équipements**. En effet, le fait que tout équipement soit faillible, a pour conséquence que l'impératif de résilience suppose une certaine hétérogénéité des équipements, quitte à ce que, dans une même zone, un même équipement puisse être autorisé pour un opérateur mais pas pour un autre.

On observera qu'actuellement sur l'ensemble du territoire métropolitain les opérateurs ont su préserver une certaine diversité des équipements. Chacun recourt actuellement à deux équipementiers pour la couverture globale du territoire, mais généralement à un équipementier unique par plaque géographique. Au total, aucune zone du territoire

métropolitain, tous opérateurs confondus, ne semblent desservie par des équipements provenant du même équipementier. Ce faisant, cette situation ne garantit pas qu'en cas de défaillance d'un équipement à l'échelle d'une plaque géographique, les flux puissent être facilement reroutés par les opérateurs utilisant un autre type d'équipements.

Les échanges réguliers que les pouvoirs publics ont avec les opérateurs portent notamment sur la maîtrise des différents risques pesant sur les réseaux de télécommunications, et sur les bonnes pratiques et recommandations utiles à la maîtrise de ces risques, au-delà des exigences légales et réglementaires. Le fait de maintenir une diversité suffisante de fournisseurs fait naturellement partie de ces recommandations, qui ne sont néanmoins assorties ni d'une portée contraignante, ni de critères précis en termes de types d'équipement, de zone géographique ou de taux de dépendance envers un fournisseur donné.

La 5G apporte une rupture significative par rapport à la situation préexistante, à la fois du fait de facteurs de risques accrus, d'une plus grande complexité à maîtriser ces risques, et d'impacts potentiels bien plus graves en cas de concrétisation de ces risques. Ces différents facteurs, ainsi que la forte évolutivité attendue dans les années à venir de la technologie, justifient ces mesures d'encadrement spécifiques.

d) Un risque limité d'application « en cascade » à des équipements déjà installés

Les opérateurs ont fait part de leur inquiétude s'agissant de l'articulation des dispositions de la proposition de loi qui ne se limite pas aux équipements 5G avec les déploiements d'équipements de générations antérieures.

Il a été précisé à votre 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 sera précisé dans le projet d'arrêté listant les types d'appareils dont l'exploitation devra faire l'objet d'une autorisation[1].

Pour autant, si, à terme, il est probable que les opérateurs soient tenus de mettre en place la 5G « *stand alone* » pour tirer pleinement parti de ses fonctionnalités, ce sera en mode « *non stand alone* » qu'ils effectueront les premiers déploiements 5G afin de pouvoir lancer rapidement cette nouvelle technologie. Ainsi, les équipements 5G devront interagir avec les équipements 4G. De manière générale, les opérateurs peuvent avoir tendance à retenir pour une nouvelle génération d'équipement, le même équipementier que pour les versions antérieures afin de s'assurer de la bonne interaction entre équipements de différentes générations.

[1] *Réponse au questionnaire parlementaire*

Ainsi ces nouvelles dispositions pourraient avoir un effet notable sur l'activité des opérateurs. Le choix d'équipement de 5G d'un nouveau fournisseur, après refus de déploiement d'un équipement du fournisseur historique, pourrait, dans un cas extrême, rendre nécessaire le remplacement de toute une gamme des équipements fournis par ce dernier, avec un coût financier et humain qui serait potentiellement élevé pour l'opérateur. En effet, les équipementiers n'ont pas développé de solutions standardisées ou de solutions techniques permettant une interopérabilité de leurs produits. C'est la raison pour laquelle l'ARCEP a appelé de ses vœux dans son avis que *les éventuels effets rétroactifs (mêmes indirects) des décisions prises dans le cadre de ce dispositif sur les déploiements passés soient évalués »*[1].

Ce faisant, l'importance du marché de 5G conduit d'ores et déjà certains opérateurs à organiser des consultations ouvertes à l'ensemble des fournisseurs, n'excluant pas des changements de fournisseurs pour aborder cette nouvelle phase de leur développement technologique.

Il conviendra donc, dans l'application de la loi, de trouver un juste équilibre entre l'impact économique du refus d'autorisation et les préoccupations de sécurité, mais sans pouvoir déroger à l'impérative obligation de préserver le réseau des risques sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale.

e) Une durée d'autorisation modulable

L'**alinéa 8** fixe à **huit ans** la durée maximale pour laquelle sera donnée l'autorisation. Cette durée est sans doute excessive au regard des évolutions technologiques mais elle offre la capacité à l'ANSSI en fonction des différents critères d'appréciation de sécurité et de résilience des équipements, de l'architecture et d'exploitation des réseaux de moduler la durée d'autorisation voire, s'agissant de technologies nouvelles, à l'augmenter progressivement, dans la limite prévue par le texte, en fonction de la mise en exploitation et de la maturité de l'équipement sous examen. Il s'agit aussi d'éviter qu'un refus abrupt d'exploitation d'un équipement qui obligerait un opérateur à remettre en cause le choix d'une gamme d'équipements alors que des améliorations en terme de fiabilité et de sécurité de l'équipement concernés sont préconisées et envisageables.

Le renouvellement de l'autorisation fait l'objet d'un dossier de demande qui est remis au moins deux mois avant l'expiration de l'autorisation d'exploitation (**alinéa 8**).

---

[1] *Avis n° 2019-0161de l'Autorité de régulation des communications électroniques et des postes en date du 4 février 2019 sur un projet de texte visant à instaurer un régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques*
https://www.arcep.fr/uploads/tx_gsavis/19-0161.pdf

Un équilibre est à rechercher pour fixer la durée d'autorisation offrant la meilleure visibilité possible aux plans d'affaires des opérateurs sans obérer la sécurité des réseaux.

f) Les modalités de l'autorisation et la composition des dossiers de demande seront fixées par décret.

L'Assemblée nationale a précisé que ce décret sera pris **après avis de l'ARCEP et de la Commission supérieure du numérique et des postes (CSNP)** dans un délai d'un mois afin de ne pas allonger les délais administratifs nécessaires au bon déploiement des réseaux (**alinéa 9**).

Si le droit commun veut que le silence gardé par l'administration vaille accord, il a été précisé au rapporteur pour avis de l'Assemblée nationale que le gouvernement envisageait de prendre un décret portant dérogation à ce principe pour l'autorisation en question. Ainsi, le silence gardé par le Premier ministre ne vaudrait pas autorisation implicite. Dans la pratique, le dialogue avec l'ANSSI conduit en règle générale à notifier dans les délais des décisions de refus assorties de conditions à respecter ouvrant un dialogue avec les opérateurs qui peuvent représenter le dossier moyennant les aménagements demandés. Sans préjudice de l'opinion du rapporteur de la commission saisie au fond, votre Rapporteur estime que cette dérogation au principe selon lequel le silence gardé par l'administration vaut accord pourrait rendre nécessaire la saisine du Conseil d'État sur le projet de décret. En effet, les articles L. 231-4 et L. 231-5 du code des relations entre le public et l'administration semblent poser cette exigence[1]. On rappellera également que la décision implicite de rejet ne dispense pas l'administration de motiver ses actes à la demande de l'intéressé, formulée dans les délais du recours contentieux (article L. 232-4 du code des relations entre le public et l'administration).

Ces différents moyens (liste des équipements, durée d'autorisation, périmètre géographique) devraient permettre au Premier ministre et au service instructeur d'arbitrer et de moduler avec une certaine subtilité les critères d'équilibre du marché, de déploiement des réseaux en temps voulu pour permettre à l'économie française de profiter pleinement de cet atout dans la compétition mondiale, de fiabilité des réseaux de conditions d'exploitation et de réductions des risques pour la sécurité nationale.

En outre, rien n'interdit le Premier ministre d'assortir l'autorisation de conditions à l'instar de ce qui est pratiqué actuellement dans le cadre du contrôle 226-3. À titre d'exemple, de telles conditions peuvent imposer la désactivation d'une fonctionnalité optionnelle de l'appareil considéré qui serait jugée insuffisamment sécurisée, ou au contraire imposer l'activation

---

[1] *Code des relations entre le public et l'administration articles L.231-4 et L.231-5* https://www.legifrance.gouv.fr/affichCode.do;jsessionid=9A0D0F892992AD8AB733F876300EA07C.tplgfr34s_1?idSectionTA=LEGISCTA000031367617&cidTexte=LEGITEXT000031366350&dateTexte=20190607

d'une fonctionnalité optionnelle (chiffrement et authentification des communications par exemple) qui améliorerait la sécurité générale de l'appareil. Elles peuvent également requérir la mise en œuvre de mécanismes ou équipements complémentaires permettant de sécuriser certaines opérations sensibles, par exemple en imposant des modalités de contrôle d'accès et de traçabilité des opérations de configuration réalisées à distance sur l'appareil pendant son fonctionnement. Ces conditions d'autorisation ne sont à ce stade mentionnées que dans la déclinaison réglementaire de la proposition de loi, et leur non-respect serait dans cette optique traité au même titre qu'une exploitation en l'absence d'autorisation.

5. Les moyens susceptibles d'être mis en œuvre par le Premier ministre pour refuser l'octroi d'une autorisation

Aux termes de la rédaction proposée pour l'article L. 34-12 du code des postes et des communications électroniques, le Premier ministre refuse par décision motivée l'octroi de l'autorisation d'exploitation ou son renouvellement s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale (**alinéa 10).**

a) Un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale

Pour la définition de ce risque, la rédaction proposée pour l'article L. 34-12 du code précité renvoie aux règles mentionnées au a, b et e du I de l'article l de l'article L. 33-1 du même code.

Ces règles sont des conditions requises pour l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques :

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

b) des conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications ;

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

Le texte proposé ne fait pas référence au f et f bis de l'article L.33-1 qui visent d'une part, l'acheminement gratuit des appels d'urgence, y compris la fourniture gratuite aux services d'urgence de l'information relative à la localisation de l'appelant (f) et, d'autre part, l'acheminement des communications des pouvoirs publics destinées au public pour l'avertir de dangers imminents ou atténuer les effets de catastrophes majeures (f bis). Ces deux dispositions concerne la sécurité intérieure, il est donc opportun de les faire figurer dans l'article L. 34-12.

Tel est l'objet de l'amendement COM-8 proposé par votre Rapporteur.

b) Une décision motivée

Si le principe de transparence dans les relations entre le public et l'administration est une règle générale inscrite à l'article L. 211-2 du code des relations entre le public et l'administration qui prévoit que « *les personnes physiques ou morales ont le droit d'être informées sans délai des motifs des décisions administratives individuelles défavorables qui les concernent. À cet effet, doivent être motivées les décisions qui : (…) refusent une autorisation, (…)*. Toutefois, dans ce même article, cette règle générale est assortie d'exceptions : (…) « *sauf lorsque la communication des motifs pourrait être de nature à porter atteinte à l'un des secrets ou intérêts protégés par les dispositions du a au f du 2° de l'article L. 311-5*».

En effet, il est des circonstances dans lesquelles l'État peut être dans l'incapacité de motiver une décision sans divulguer ou publier des faits couverts par le secret au titre d'autres dispositions législatives, il en va ainsi notamment des dispositions couvertes par le secret de la défense nationale. En conséquence, l'article L. 311-5 du code des relations entre le public et l'administration dispose que « *ne sont pas communicables : (…) 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte :*
a) Au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ;
b) Au secret de la défense nationale ;
c) A la conduite de la politique extérieure de la France ;
d) A la sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations ;
e) A la monnaie et au crédit public ;
f) Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;

Dans le cas spécifique de l'article L. 34-12 du code des postes et des communications électroniques, en réaffirmant le principe de la motivation de la décision du Premier ministre sans mentionner explicitement les restrictions figurant à l'article L. 311-5 du code des relations du public et de l'administration précité, il pourrait être considéré, par un raisonnement *a*

contrario, que le législateur a renoncé, à l'application des dispositions permettant de déroger à l'obligation générale de motivation, dans un texte législatif postérieur prévalant sur la règle antérieure posée du code des relations entre le public et l'administration.

Or, ces exceptions protectrices du secret doivent impérativement être préservées dans un domaine où l'enjeu est d'éviter un risque d'atteinte aux intérêts de la défense et de la sécurité nationale. **Aussi votre Rapporteur vous propose d'ajouter au premier alinéa du texte proposé pour l'article L. 34-12 du code des postes et des télécommunications (alinéa 10) la phrase suivante : « *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 du a au f du 2° de l'article L. 311-5 du code des relations entre le public et l'administration* » et par coordination de supprimer dans la première phrase, les mots : « *par décision motivée* ». (Amendement COM-9)**

c) L'appréciation de ces critères par le Premier ministre

Dans la rédaction proposé pour le deuxième alinéa de l'article L. 34-12 du code précité (**alinéa 11**), il est indiqué que le Premier ministre « *peut prendre* » en considération, pour l'appréciation de ces critères, les modalités de déploiement et d'exploitation mises en places 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.

Pour votre Rapporteur, l'apport du dispositif envisagé et sa portée eu égard aux fonctionnalités des nouvelles technologies est de permettre de prendre en considération, dans l'appréciation du risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale, les modalités de déploiement et d'exploitation mises en place par l'opérateur. En effet, il a été rappelé que selon ses conditions d'exploitation, un équipement peut présenter un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale. Dès lors, de son point de vue, l'autorité administrative ne peut se dispenser d'apprécier ce risque lors de l'examen de la demande sauf à affaiblir la portée de cette disposition.

Il en va de même de l'appréciation du contrôle ou des actes d'ingérence auxquels un opérateur ou un de ses prestataires pourrait être soumis de la part d'un État non membre de l'Union européenne. Les intérêts fondamentaux de la Nation exigent que cet examen soit réalisé et que, s'il existe des doutes sérieux, le Premier ministre puisse refuser d'octroyer une autorisation en s'appuyant sur ce critère. Pour cela, dans l'instruction, il dispose des analyses auxquelles le SGDSN est associé au titre du dispositif national de sécurité économique. Sans entrer dans le débat ouvert sur la fiabilité de tel ou tel équipementier, il doit être réaffirmé qu'une telle clause

de sécurité nationale est parfaitement légitime dès lors qu'elle n'introduit pas de distorsion entre les opérateurs qui sont tous soumis à la même règle.

Comme l'a rappelé la ministre au cours des débats en commission à l'Assemblée nationale[1] « *il faut savoir si certains équipementiers pourraient être légalement contraints de communiquer des données à leur gouvernement – c'est un élément important à prendre en considération dans une décision, mais cela ne concerne pas que les acteurs chinois ; et deuxièmement et surtout, il faut anticiper les possibles failles techniques : cela concerne tous les équipementiers, mais la faille ne se situera pas nécessairement au niveau de l'équipementier ; elle peut être le fait d'un de ses sous-traitants, au niveau des lignes de codage, par exemple. L'enjeu de la souveraineté technologique concerne donc tous les équipementiers, tous les logiciels, toute la sous-traitance. Il s'agit de nous doter d'un dispositif robuste de contrôle pour préserver notre souveraineté technologique – (…) car elle est au cœur de notre indépendance industrielle.* »

Votre Rapporteur propose en conséquence de remplacer, dans l'alinéa 11 les mots « peut prendre » par le mot « prend » (amendement COM-10).

6. Un pouvoir d'injonction en cas d'exploitation sans autorisation d'un appareil

La proposition de loi prévoit dans un texte proposé pour l'article L. 34-13 du code des postes et des télécommunication (**alinéa 12**) de donner au Premier ministre la capacité d'enjoindre à l'opérateur de déposer une demande d'autorisation ou de renouvellement ou de faire rétablir à ses frais la situation antérieure, dans le délai qu'il fixe, si l'exploitation d'un appareil est réalisée sans autorisation préalable.

L'**alinéa 13** précise les conditions d'une **procédure contradictoire** préalable à la prise d'effet de l'injonction. Celle-ci doit être précédée d'une mise en demeure de l'opérateur de présenter des observations dans un délai de quinze jours, sauf urgence, circonstances exceptionnelles ou atteinte imminente à la sécurité nationale.

L'absence de mise en conformité avec l'injonction est punie par la même peine que l'exploitation sans autorisation (*voir infra*).

---

[1] *Assemblée nationale – XVème législature – Rapport n°1832fait au nom de la commission des affaires économiques par m. Éric Bothorel député, p.24*

7. Une clause de nullité des engagements, conventions et clauses contractuelles prévoyant l'exploitation des équipements en cas de refus d'exploitation

Les auteurs de la proposition de loi ont introduit (**alinéa 14**) une clause de nullité des engagements, conventions ou clauses contractuelles prévoyant l'exploitation des appareils concernés - ceux mentionnés au I de l'article L. 34-11 du code des postes et des communications électroniques - lorsque l'activité n'a pas fait l'objet de l'autorisation préalable sur le fondement du même article ou d'une régularisation dans les délais impartis.

8. Un dispositif qui repose sur les capacités de l'ANSSI à traiter les demandes en temps utile

La mise en œuvre de ce dispositif requiert une instruction par l'ANSSI et donc l'affectation de moyens. À défaut de réalisation d'une étude d'impact, vos rapporteurs au fond et pour avis ont recueilli auprès des administrations concernées des éléments d'appréciations.

a) Estimation du volume des demandes d'autorisation et de renouvellement

La typologie d'équipements concernée par le nouveau dispositif n'est pas équivalente, mais globalement comparable à celle relevant du R.226[1]. Une volumétrie de demandes du même ordre de grandeur est par conséquent anticipée, à hauteur d'au plus un millier de demandes annuelles. 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 : les seuls équipements spécifiques à la 5G qui seront déployés à ce titre seront ceux assurant la desserte radioélectrique (stations de base), le reste des réseaux demeurant par ailleurs dans une technologie 4G. Les premiers déploiements de réseau 5G « *standalone* », qui élargiront la typologie des équipements 5G, et par conséquent, le volume de demandes, n'interviendront probablement qu'à compter de 2022.

---

[1] *Le contrôle R.226 donne lieu, dans sa globalité, à environ 1200 autorisations annuelles, auxquelles s'ajoutent une centaine de refus d'autorisation. Les autorisations sont équitablement réparties entre celles prononcées au titre de l'article R.226-3 (autorisations de fabrication, importation, exposition, location ou vente – 664 autorisations accordées en 2018) et celles qui le sont au titre de l'article R.226-7 (autorisations d'acquisition ou de détention – 602 en 2018). Parmi ces dernières, environ 500 portent sur des équipements de télécommunication et sont accordées aux opérateurs de communications électroniques, les autres relevant d'autre types de dispositifs (notamment, dispositifs de captation judiciaire à l'usage des services enquêteurs) relevant également du champ du R.226. Il est également à noter qu'une part significative de ces autorisations porte sur des tests réalisés par les opérateurs en amont de potentiels déploiements, opérations qui n'entreront pas dans le champ du contrôle prévu par la proposition de loi.*

b) Estimation des capacités de l'ANSSI pour traiter les demandes

L'instruction technique des demandes repose sur les compétences des équipes d'audit ou d'assistance technique et des laboratoires de l'ANSSI. Le directeur général de l'ANSSI a indiqué que l'Agence ne réclamait pas de moyens supplémentaires à ce titre, compte-tenu du renforcement déjà prévu des compétences techniques dans le domaine de la 5G intégré dans le cadre du triennal budgétaire. Le schéma d'emplois de l'ANSSI prévoit 50 créations de postes par an.

L'instruction administrative des demandes d'autorisation et de renouvellement sera assurée par le Bureau des Contrôles Réglementaires de l'ANSSI, qui assure déjà une mission similaire dans le cadre dit du « R.226 », ainsi que la contribution de l'ANSSI à différents autres dispositifs de contrôle réglementaire (exportations de biens à double usage et investissements étrangers par exemple). Ce traitement est actuellement assuré par deux agents dédiés à cette mission. Le traitement des nouvelles demandes nécessitera un renfort de deux personnels dédiés au traitement administratif.

Pour le directeur général de l'ANSSI, la clé de la fluidité de la procédure réside dans l'anticipation des demandes par les opérateurs qui pourront engager des discussions avec l'ANSSI sur leurs projets à une phase très amont, comme c'est déjà le cas pour l'examen des autorisations du régime prévu par les articles R 226-7 et suivant du code pénal. En outre, une partie des équipements aura déjà fait l'objet d'un agrément de mise sur le marché au regard des dispositions de l'article R 226-3 du code pénal sur la protection des correspondances et de la vie privée.[1]

Enfin, le dialogue avec les opérateurs permet à l'ANNSI de nuancer les décisions qui ne se limitent pas à une autorisation ou à une interdiction mais peuvent être assortie de restrictions d'application géographique, des restrictions d'application d'usage ou formuler des recommandations en vue d'améliorer les dispositifs et modulées dans leur durée. Le texte permet une application souple et pragmatique afin d'assurer un équilibre entre, d'une part, la qualité attendue des réseaux technologiques en terme d'usage et de calendrier de déploiement et, d'autre part, la capacité à maîtriser les risques en matière de souveraineté et de fragilité technique.

---

[1] *Dès lors qu'un appareil faisant l'objet d'une demande d'autorisation au titre de l'article L 34-11 aura auparavant obtenu une autorisation R.226-3, les conclusions de l'analyse technique approfondie menée au titre du R.226-3 pourront être versées dans l'analyse menée au titre du L 34-11, et faciliter celle-ci en évitant des redondances d'instruction.*

B. UN RÉGIME CONTRÔLÉ ET ASSORTI DE SANCTIONS

1. L'absence de dispositif de contrôle spécifique

La proposition de loi et sa déclinaison réglementaire ne prévoient pas de modalités spécifiques de contrôle. Ces contrôles pourraient cependant être réalisés par le biais d'audits de sécurité, confiés à l'ANSSI ou par 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. S'agissant d'OIV, on rappellera également qu'ils restent soumis aux dispositions qui permettent au Premier ministre de soumettre les opérateurs à un processus de contrôle et d'audit de leurs systèmes d'information d'importance vitale destiné à vérifier leur niveau de sécurité et le respect des règles de sécurité[1]. Le déploiement d'appareils sans autorisation préalable ou en contravention avec les conditions posées par l'autorisation seraient naturellement considérés comme une infraction aux règles de sécurité.

À travers ces mécanismes de contrôle généralement réalisés par l'ANSSI, l'État dispose d'ores et déjà de moyens de vérifier l'application rigoureuse des dispositions prévues par la proposition de loi et de constater le cas échéant les contraventions afférentes, lesquelles sont passibles de sanctions définies à l'article 2.

Pour autant, il n'est pas prévu de régime spécifique d'abrogation ou de retrait des autorisations afin de sécuriser les opérateurs et à leurs plans d'investissements. Ceci dit, d'un strict point de vue juridique, les possibilités de retrait existent dans des conditions de droit commun (articles L. 242-1 et L. 242-2 du code des relations entre le public et l'administration) s'il existe un motif d'intérêt général suffisant.

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

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

Sont ainsi créées deux infractions :

- l'exploitation sans autorisation préalable des appareils entrant dans le champ de l'autorisation (**alinéa 4**) ;
- le défaut d'exécution, même partiel, des injonctions que peut prononcer le Premier ministre en cas de défaut d'autorisation (**alinéa 5**).

---

[1] *Article L .1332-6-3 et R. 1332-41-11 à R. 1332-41-16 du code de la défense*

Ces infractions sont punies de cinq ans d'emprisonnement et de 300 000 euros d'amende pour toute personne physique[1] (alinéa 3).

Des sanctions pénales complémentaires sont prévues par renvoi aux articles L. 39-6 et L. 39-10 du même code : le tribunal peut prononcer la confiscation des matériels et installations constituant le réseau ou permettant la fourniture du service. Il peut ordonner la destruction de ces matériels et installations aux frais du condamné, et l'interdiction d'établir un réseau radioélectrique mobile pour une durée d'au plus trois ans, ainsi que l'affichage de la décision de sanction ou sa diffusion par voie électronique (**alinéa 6**).

Les personnes morales déclarées responsables pénalement encourent, quant à elles, une amende dont le taux maximal est égal au quintuple de celui prévu pour les personnes physiques. Des sanctions complémentaires leurs seront applicables : le juge pourra prononcer l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités d'exploitation de réseaux radioélectriques mobiles publics (peine mentionnée au 2° de l'article 131-39 du code pénal) et l'affichage ou la diffusion de la décision prononcée par la presse écrite ou par voie électronique, peines mentionnées au 9° de l'article 131-39 du code pénal (**alinéa 7**).

Le montant de la sanction paraît proportionné compte tenu du risque pour la défense et la sécurité nationale.

C. UN RÉGIME APPLICABLE DE FAÇON RÉTROACTIVE

L'article 3 prévoit que ce régime d'autorisation préalable sera applicable à l'exploitation des appareils installés depuis le 1er février 2019. Les opérateurs concernés auront deux mois à compter de l'entrée en vigueur de ce texte pour déposer leurs dossiers de demande d'autorisation pour des équipements déjà mis en place.

L'application rétroactive est justifiée par le besoins de régulariser la situation des appareils déployés au titre des expérimentations en cours, lesquels pourraient soit être laissés en place à l'issue des expérimentations et, à terme intégrés aux réseaux ouverts au public et d'éviter que des opérateurs, cherchent à contourner les contraintes du dispositif d'autorisation annoncé.

---

[1] *La proposition de loi initiale avait fixées ces peines à 1an d'emprisonnement et 150 000 euros d'amende. L'Assemblée nationale a aligné celles-ci sur les sanctions prévues à l'article 226-3 du code pénal*

CONCLUSION GÉNÉRALE

Globalement le texte paraît strictement suffisant pour assurer la protection des intérêts de la défense et de la sécurité nationale. Il parait équilibré et pourra faire l'objet d'une application souple en conciliant divers critères d'appréciation du risque, en assortissant l'autorisation de conditions d'exploitation et en modulant sa durée. Il devra néanmoins faire l'objet d'une évaluation notamment au regard de l'évolution des usages et du développement des technologies afin de garantir la pérennité dans le temps de cette protection.

Sous réserve de ces observations et des trois amendements « techniques » présentés, votre Rapporteur vous propose de donner un avis favorable à l'adoption de la proposition de loi.

EXAMEN EN COMMISSION

Réunie le mercredi 12 juin 2019, sous la présidence de M. Christian Cambon, président, la commission des affaires étrangères, de la défense et des forces armées a procédé à l'examen du rapport pour avis de M. Pascal Allizard 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.

M. Pascal Allizard, rapporteur pour avis. – Les réseaux de télécommunications sont devenus des réseaux « supercritiques ». Comme les réseaux d'électricité, ils sont indispensables au fonctionnement de l'ensemble des réseaux et des services qui irriguent les activités économiques, mais aussi la vie quotidienne. Leur résilience présente un intérêt vital pour la défense et la sécurité nationale.

Les réseaux mobiles vont connaître, avec l'arrivée des technologies de cinquième génération (5G), une profonde évolution de leurs configurations techniques qui permettra de développer de nouveaux usages mais entraînera de nouvelles vulnérabilités.

La proposition de loi votée par l'Assemblée nationale soumet à autorisation du Premier ministre le déploiement et les conditions d'exploitation de certains équipements – matériels et logiciels – par les opérateurs sur leurs réseaux, afin de préserver les intérêts de la défense et de la sécurité nationale.

La 5G est une technologie de rupture – et non de la 4G améliorée – qui devrait permettre la transformation de nombreux secteurs d'activités et en priorité les acteurs économiques. Elle constitue un véritable changement d'échelle dans les capacités des réseaux de télécommunications avec : un accroissement considérable des débits de données, environ dix fois supérieurs à la 4G ; une réduction des temps de latence à quelques millisecondes ; et un accroissement de la densité des flux, qui permettra la création de tranches de réseaux à la demande avec des capacités personnalisés. En outre, son architecture décentralisée permet d'opérer, dans les stations de base des antennes, une partie du traitement des données sans que celles-ci transitent par le cœur du réseau. Cet accroissement de la vitesse et cette décentralisation posent des problèmes de sécurité.

La diffusion de cette technologie ouvre la voie à des applications et des usages variés et nouveaux. Elle permettra le déploiement massif de l'internet des objets qui jouera un rôle essentiel dans le domaine de la mobilité – par exemple les véhicules autonomes – de la domotique, de la

réalité augmentée, de la production industrielle ou encore des réseaux énergétiques et des « villes intelligentes ». Son déploiement sera progressif.

Nous entrons dans un nouveau cycle économique qui, dans un environnement de concurrence mondialisée, bénéficiera aux États et aux entreprises qui maitriseront ces développements. Les économies chinoises et américaines bénéficient d'un marché domestique suffisamment large pour que leurs champions nationaux puissent développer ces activités et prennent dès aujourd'hui une avance considérable. Tout retard pris dans le déploiement de la connectivité des territoires retardera d'autant le développement de l'écosystème 5G par les acteurs européens. Il s'agit d'un enjeu majeur de compétitivité donc de politique publique.

Cela interroge sur la souveraineté des États quant à la maîtrise de la donnée générée sur leur territoire, mais également sur la capacité des opérateurs à assurer la sécurité de leurs réseaux. C'est un enjeu de sécurité nationale à deux titres au moins : la résilience de ces réseaux revêt une importance vitale. Une interruption majeure de service constituerait une catastrophe économique et sociale et une atteinte à la sécurité nationale ; les armées et les forces de sécurité intérieure utiliseront de plus en plus les réseaux civils de télécommunications. En outre, ces réseaux constituent des actifs économiques substantiels dont la dégradation serait préjudiciable. Garantir leur sécurité procède de l'intérêt économique à long terme de la Nation.

Or la vulnérabilité de ces réseaux de nouvelle génération s'accroîtra inexorablement. En effet, ils reposent sur des équipements de plus en plus virtuels et des architectures de réseaux de plus en plus déconcentrées : les efforts de sécurisation qui portaient jusqu'à présent essentiellement sur les cœurs de réseau devront être étendus à ces nouveaux équipements en périphérie ; certains équipements physiques seront remplacés par des solutions logicielles. Ce transfert accroîtra la vélocité et la résilience des réseaux mais il ne sera pas exempt de failles d'un nouveau genre, en raison de la complexité et de la rapidité de leur développement, d'erreurs de configuration, et de risques d'interception. Les modalités de déploiement retenues par chaque opérateur prendront une importance considérable dans l'analyse de sécurité ; la diversité des usages induit également de nouvelles vulnérabilités. Des menaces proviendront de la croissance exponentielle des appareils ou systèmes connectés, qui eux-mêmes ne pourront pas garantir un niveau de sécurité infaillible.

Ces évolutions préfigurent une redistribution des rôles. Les opérateurs traditionnels s'appuieront toujours davantage sur des sous-traitants – leurs fournisseurs ou des intégrateurs – pour maîtriser de bout en bout leurs capacités techniques : certains équipementiers proposent à leurs clients d'acquérir un service de mise à jour en permanence effaçant la notion de version des logiciels. Rien n'empêcherait de réaliser ces mises à jour à distance sans intervention physique des opérateurs. En outre, une

technologie nouvelle appelle dans sa phase de déploiement des modifications nombreuses, cela accroît les risques liés à l'utilisation de technologies encore immatures et au temps d'adaptation du niveau de protection. Ce recours à la sous-traitance est naturellement porteur de risques, tant du fait de la possible méconnaissance des obligations de sécurité par les prestataires concernés, qu'au regard de leur soumission potentielle à des formes d'ingérence. La proposition de loi soutient donc aussi l'implication des opérateurs dans la sécurité de leurs réseaux.

Plusieurs dispositifs législatifs, obéissant à des finalités différentes, sont actuellement applicables aux équipements déployés par les opérateurs de réseaux radioélectriques au titre la protection du secret de la correspondance et de la vie privée – par les dispositifs dits de l'article 226-3 du code pénal – ou au titre de la protection des activités d'importance vitale. Cependant, ces dispositifs ne répondent pas efficacement aux objectifs de protection de bout en bout des systèmes de nouvelle génération déployés par les opérateurs de réseaux radioélectriques mobiles ; l'intervention du législateur est donc nécessaire.

Le déploiement des réseaux de cinquième génération est prévu à partir de 2020, au moins dans une configuration intermédiaire, et nécessitera des investissements très importants. Les opérateurs ont besoin d'un cadre juridique et technique clair pour garantir la fiabilité et les conditions d'exploitation de leurs équipements.

La plupart des États ont pris conscience des enjeux, dont certains stratégiques : le saut technologique et les potentialités économiques offertes par la 5G sont susceptibles d'avoir un effet disruptif sur l'équilibre des puissances. Ces enjeux stratégiques interfèrent dès lors avec la simple question de la sécurité des réseaux et sont devenus une partie importante de la guerre commerciale que se livrent la Chine et les États-Unis – ces dernières semaines, la presse regorgeait d'articles sur ce sujet. La question de savoir si l'on peut avoir une égale ou suffisante confiance en tous les équipementiers, qui doit être envisagée selon des critères multiples, s'est focalisée sur les craintes que les équipements chinois puissent constituer des « chevaux de Troie » dans les systèmes d'information supercritiques des réseaux de 5G. En effet, la législation chinoise oblige les entreprises ayant leur siège en Chine de collaborer avec les services de renseignement de ce pays Et pour l'une d'entre elles, Huawei, sur le manque de transparence dans son actionnariat et ses liens financiers avec l'État.

La position de la France, de nombreux autres États européens, et de l'Union européenne, n'est pas la même que celle des États-Unis dans la valorisation de ce critère, lequel n'est cependant pas exclu de l'analyse du risque. Le Parlement n'est pas invité à voter une proposition « anti-Huawei », mais à mettre en place un régime d'autorisation applicable à tous les opérateurs pour préserver les intérêts de la défense et de la sécurité nationale. Ce n'est pas qu'une nuance.

La proposition de loi institue un nouveau régime d'autorisation administrative, permettant à l'État de maîtriser le déploiement des réseaux de 5G et de s'assurer de leur résilience sans pour autant entraver leur développement.

L'article 1er introduit trois nouveaux articles dans le code des postes et des communications électroniques. Le nouvel article L. 34-11 soumet à une autorisation du Premier ministre l'exploitation, sur le territoire national, « d'appareils, à savoir tous dispositifs matériels ou logiciels » qui permettent la connexion au réseau radioélectrique mobile dès lors que leurs fonctions présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation dudit réseau. Le régime d'autorisation est appliqué aux seuls opérateurs d'importance vitale exploitants de réseaux de communication téléphonique ouverts au public. La liste de ces opérateurs est confidentielle, mais on peut avancer sans trop de risque qu'elle comprend les quatre principaux opérateurs nationaux.

Ce régime d'autorisation ne s'applique pas aux opérateurs dits verticaux. L'Assemblée nationale avait adopté, dans un premier temps, un amendement tendant à étendre ces règles à l'ensemble des opérateurs d'importance vitale (OIV), avant d'y renoncer. Cette extension visait les OIV qui, pour les besoins de leurs activités, utilisent des réseaux de radiocommunication privée. Selon le Gouvernement, le risque est suffisamment couvert par les dispositions applicables aux OIV, et les possibilités de privatisation de parties des réseaux des opérateurs de télécommunications ouverts au public inciteront les OIV à développer des certains services via ces réseaux.

Enfin, les applications nouvelles ou innovantes soit relèveront des dispositions proposées, soit elles utiliseront des réseaux privatifs – dans cette hypothèse, il faudra analyser les risques au regard de la sécurité nationale et au besoin, les intégrer dans la liste des OIV.

La maturité actuelle de la 5G ne permet pas, à ce stade, d'envisager ou d'imaginer tous les développements d'activité et de services possibles, ni leurs modalités. Il serait prématuré d'intervenir pour instaurer un cadre juridique qui risque de s'avérer inadapté. Les services de l'État devront être extrêmement attentifs aux évolutions en cours et vigilants dans l'appréciation des activités d'importance vitale. Une évaluation régulière du dispositif prévu est nécessaire, au regard du développement des nouveaux services et activités mis en œuvre ou projetés.

Le régime proposé, dans un objectif de stricte suffisance, est limité aux appareils qui « présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau » et exclut les appareils installés chez les utilisateurs finaux. Ces appareils figureront sur une liste établie par arrêté du Premier ministre après avis de l'Autorité de régulation des communications électroniques et des Postes (Arcep).

L'alinéa 6 précise que l'autorisation est délivrée « pour un périmètre géographique » défini par l'opérateur dans sa demande. Ainsi, l'État pourra exiger des conditions de sécurité plus élevées pour les zones où sont situées des installations ou des services plus sensibles, en cohérence avec les préoccupations de défense nationale. Cela évitera un monopole d'équipement dans certaines zones et poussera les opérateurs et les équipementiers à rechercher une plus grande interopérabilité de leurs réseaux, de façon à garantir leur résilience en cas de défaillance d'un équipement.

Les opérateurs ont su globalement préserver une certaine diversité des équipements. Aucune zone du territoire métropolitain, tous opérateurs confondus, ne semble desservie par des équipements provenant du même fournisseur. Mais cette situation ne garantit pas qu'en cas de défaillance d'un équipement à l'échelle d'une plaque géographique, les flux puissent être facilement transmis par les opérateurs utilisant un autre type d'équipement. La présence de fournisseurs plus nombreux est donc souhaitable pour ouvrir la concurrence. Trois équipementiers sont actuellement présents : Nokia, Ericsson et Huawei. L'arrivée d'un quatrième opérateur, Samsung, serait la bienvenue pour une meilleure concurrence.

L'alinéa 7 confirme que l'autorisation est octroyée après examen d'un dossier de demande remis par l'opérateur. Celui-ci est donc bien l'interlocuteur unique, responsable de la cohérence de l'architecture de son réseau et de la fiabilité de son exploitation, des équipements mis en œuvre, et des modes d'organisation retenus, notamment par le recours à la sous-traitance. Cela aura des conséquences industrielles.

Le premier alinéa du texte proposé pour le II. de l'article L. 34-11 précise que l'autorisation est donnée pour « un ou plusieurs modèles » et « une ou plusieurs versions » des appareils susmentionnés. Il s'agit d'éviter que toute mise à jour logicielle ou modification technique d'un équipement déjà contrôlé soit systématiquement soumise à une nouvelle procédure. Je comprends ce souci. La rédaction proposée est suffisamment large pour garantir une liberté d'appréciation à l'Agence nationale de la sécurité des systèmes d'information (Anssi). Mais les risques d'introduction de failles logicielles, voire de « portes dérobées » sont aussi grands à l'occasion d'une simple mise à jour qu'à l'occasion d'un changement de version, et que dans l'avenir les mises à jour se feront de manière continue.

L'alinéa 8 fixe à huit ans la durée maximale pour laquelle sera donnée l'autorisation. Les modalités de l'autorisation et la composition des dossiers seront fixées par décret, après avis de l'Arcep et de la Commission supérieure du numérique et des postes (CSNP). Les moyens susceptibles d'être mis en œuvre par le Premier ministre pour refuser l'octroi d'une autorisation sont définis à l'article 34-12 : « le Premier ministre refuse par décision motivée l'octroi de l'autorisation s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale. »

Pour la définition de ce risque, la rédaction renvoie aux conditions mentionnées au a), b) et e) du I de l'article L.33-1 du code des postes et des communications électroniques, requises pour l'établissement et l'exploitation des réseaux ouverts au public : des conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service ; des conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications ; et les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique.

Les règles mentionnées au f) et f bis) du même article concernant l'acheminement gratuit des appels d'urgence, et l'acheminement des communications des pouvoirs publics destinées au public pour l'avertir de dangers imminents ou atténuer les effets de catastrophes majeures ne sont pas incluses. Elles relèvent de préoccupations de sécurité nationale, et je propose de les ajouter par mon premier amendement.

Le texte proposé pour l'article L.34-12 précise que « le refus du Premier ministre doit être motivé. » Ce principe, figurant déjà dans le code des relations entre le public et l'administration, est donc d'application générale. Mais il est assorti d'exceptions lorsque la communication des motifs pourrait être de nature à porter atteinte à l'un des secrets protégés par la loi. En réaffirmant le principe sans mentionner explicitement les exceptions, il pourrait être considéré, par un raisonnement *a contrario*, que le législateur a renoncé, dans le cas spécifique de l'article L. 34-12 du code des postes et des communications électroniques, à l'application des exceptions à l'obligation générale de motivation. Or ces exceptions devront impérativement être préservées pour éviter un risque d'atteinte aux intérêts de la défense et de la sécurité nationale. C'est pourquoi mon deuxième amendement ajoute à l'alinéa 10 les phrase suivantes : « 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 du a) au f) du 2° de l'article L. 311-5 du code des relations entre le public et l'administration ». par coordination, on supprimerait « par décision motivée » dans la première phrase.

Enfin, selon la rédaction proposé pour le deuxième alinéa de l'article L 34-12, le Premier ministre « peut prendre » en considération, pour l'appréciation de ces critères, les modalités de déploiement et d'exploitation mises en places 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.

Les intérêts fondamentaux de la Nation exigent que l'examen des éléments d'appréciation soit réalisé et que, s'il existe des doutes sérieux, le Premier ministre puisse refuser d'octroyer une autorisation en s'appuyant sur ces critères. Sans entrer dans le débat ouvert sur la fiabilité de tel ou tel équipementier, une telle clause de sécurité nationale est parfaitement légitime dès lors qu'elle n'introduit pas de distorsion entre les opérateurs et

les fournisseurs qui sont tous soumis à la même règle. Je propose d'affirmer cette règle en introduisant l'indicatif et en conséquence de remplacer, dans l'alinéa 11, les mots « peut prendre » par le mot « prend », par mon dernier amendement.

La proposition de loi autorise le Premier ministre – par ses alinéas 12 et 13 – à adresser aux opérateurs des injonctions après mise en demeure si l'exploitation d'un appareil est réalisée sans autorisation préalable.

Le texte ne prévoit pas de dispositif de contrôle spécifique. L'Anssi dispose d'ores et déjà de la capacité à réaliser des audits de sécurité. L'État aura les moyens de vérifier l'application de la proposition de loi et de constater, le cas échéant, les contraventions afférentes, lesquelles sont passibles de sanctions définies à l'article 2 dont le montant paraît proportionné.

L'article 3 prévoit enfin que le régime sera applicable à compter du 1er février 2019. Cette application rétroactive est justifiée par le besoin de régulariser la situation des appareils déployés au titre d'expérimentations et d'éviter que des opérateurs cherchent à contourner les contraintes du dispositif d'autorisation.

Concrètement, le dispositif reposera sur les capacités de l'Anssi à traiter les demandes d'autorisation et de renouvellement en temps utile afin de ne pas freiner le déploiement de la 5G. À défaut de réalisation d'une étude d'impact, les éléments d'appréciation que nous avons recueillis montrent que le volume des demandes d'autorisation augmentera progressivement et qu'il est globalement compatible avec la montée en puissance de l'Anssi et de ses effectifs – 50 personnes supplémentaires chaque année – prévue dans le cadre du triennal budgétaire.

Ces différents moyens devraient permettre au Premier ministre et au service instructeur d'arbitrer et de moduler avec une certaine subtilité les critères d'équilibre du marché, de déploiement des réseaux en temps voulu pour que l'économie française puisse profiter pleinement de cet atout dans la compétition mondiale, de fiabilité des réseaux et de réduction des risques pour la sécurité nationale, d'autant que rien n'interdit au Premier ministre d'assortir l'autorisation de conditions.

Globalement, le texte ainsi amendé me paraît suffisant pour assurer la protection des intérêts de la défense et de la sécurité nationale. Équilibré, il pourra faire l'objet d'une application souple en conciliant divers critères d'appréciation du risque, en assortissant l'autorisation de conditions d'exploitation et en modulant sa durée. Il devra néanmoins faire l'objet d'une évaluation, notamment au regard de l'évolution des usages – inconnus aujourd'hui – et du développement des technologies afin de garantir la pérennité de cette protection.

Sous réserve de ces observations et de l'adoption de mes trois amendements techniques, je vous propose de donner un avis favorable à l'adoption de la proposition de loi.

M. Christian Cambon, président. – Merci de nous avoir aidés à saisir toute la portée de ce texte, qui n'est pas dirigé contre un opérateur en particulier.

Mme Isabelle Raimond-Pavero. – Le 6 juin dernier, une partie du trafic mobile européen a été reroutée vers China Telecom. Sommes-nous capables d'évaluer les risques de la remontée de telles informations vers Pékin pour notre défense nationale et la sécurité intérieure ? Les espaces d'entrainement et de détection des radars militaires sont saturés. Comment faire face à l'arrivée de la 5G ?

Mme Sylvie Goy-Chavent. – Merci pour cet exposé très complet. La 5G est une technologie d'avenir, qui a fait ses preuves. Comment s'articule-t-elle avec la fibre très haut débit ? Mon département de l'Ain, peu équipé en 5G, compte deux bases militaires : Ambérieu-en-Bugey et la Valbonne, pas très éloignées du site très sensible du Mont-Verdun. Qu'en est-il de leur vulnérabilité ? Ces deux bases pourront-elles s'équiper de systèmes 5G ?

Mme Joëlle Garriaud-Maylam. – Félicitations pour ce travail…

M. Christian Cambon, président. – … d'autant plus que M. Allizard n'a pas eu beaucoup de temps pour le préparer.

Mme Joëlle Garriaud-Maylam. – Nous devons être vigilants. Le risque évolue en permanence. Qu'ont fait les autres pays européens ? Les technologies évoluent rapidement, nous avons besoin de réactivité, et pourrions proposer une initiative européenne. Nous débattons de ce sujet depuis le traité de Maastricht, malheureusement l'Europe n'avance pas assez.

M. Ladislas Poniatowski. – Restons lucides. Si les uns et les autres, nous avons gardé notre smartphone allumé toute la semaine dernière, nos positions – voire nos conversations– ont été connues. Les appareils et les technologies connaissent une croissance exponentielle… Cela ne signifie pas qu'il ne faut rien faire. Selon vous, il faut limiter le périmètre d'intervention des opérateurs, contrôler les appareils et créer plus de concurrence, cela me fait bien rire : c'est très bien mais cela n'empêchera pas le déploiement de la 5G, qui est déjà là, et qui se développera sans la France.

La France veut assurer sa sécurité en matière de défense, dites-vous… J'en ris, car nous n'assurons rien du tout ! Mais je suis favorable à la proposition de loi, afin d'avoir un cadre juridique. Cela me fait penser au nuage de Tchernobyl, qui se serait arrêté à la frontière. Nous sommes dépassés, mais votons quand même ce texte !

M. François Patriat. – Je partage la lucidité de M. Ladislas Poniatowski sur l'inexorabilité du déploiement de la 5G. Je remercie le

rapporteur pour son travail. Nos inquiétudes sur la sécurité et la défense sont grandissantes. Pensez aux affrontements entre les États-Unis et la Chine.

La 5G promet d'innombrables innovations technologiques mais apporte aussi des vulnérabilités nouvelles. Il est urgent de garantir la résilience de nos réseaux de communication et de contrôler la 5G tout en garantissant un développement soutenable. Je forme le vœu de débats constructifs en séance publique. Nous poursuivons le même objectif, et j'espère que la commission mixte paritaire sera conclusive afin de nous doter d'un arsenal législatif à la hauteur des enjeux de sécurité et de défense. Dans une démarche constructive, nous soutiendrons les amendements du rapporteur même si nous nous interrogeons sur les implications pratiques du troisième…

M. Rachel Mazuir. – Cette proposition de loi fait suite au refus d'un amendement proposé lors du débat sur la loi relative à la croissance et à la transformation des entreprises (Pacte). Je me félicite d'un débat, même rapide, sur ce sujet. Si nous voulons encadrer le développement de la 5G, et non arriver après en étant coercitifs, il faut faire vite. La 5G aurait mérité un débat plus long. Les réseaux physiques seront dilués, nous aurons des réseaux virtuels, des *clouds*, difficiles à apprécier. L'Anssi a certifié que les logiciels mis à jour régulièrement posent des difficultés supplémentaires, difficilement appréciables.

Il est difficile pour la France d'être présente. Notre collègue M. Gérard Longuet préside une commission d'enquête sur la souveraineté numérique. Alcatel a été démantelé et racheté par Nokia. Nokia et Ericsson sont faibles par rapport à Huawei. Mais une porte s'ouvre avec l'interdiction de Huawei aux États-Unis. Nous sommes inquiets de la place grandissante de Huawei, et aimerions à sa place un champion européen. Votre deuxième amendement autorisant le Premier ministre à ne pas motiver sa décision m'interroge. Même s'il ne le dit pas publiquement, il doit bien motiver sa décision ! Sinon ; c'est la porte ouverte à des dérives autoritaires.

Cette loi, essentielle, arrive avant le déploiement de la 5G, avec un effet rétroactif ; ainsi, les essais de 5G depuis 2018 ne pourront mettre à profit cette faille pour avoir du matériel non certifié par l'Anssi. Le groupe socialiste et républicain votera ce texte.

M. Pierre Laurent. – Je remercie le rapporteur pour son exposé clair sur un sujet complexe. Le groupe communiste, républicain et citoyen votera le texte proposé.

Cette situation témoigne, de la part de la France et de l'Europe, d'une faille industrielle majeure. Nous avons raté, dans les grandes largeurs, une technologie de rupture majeure. Cela pose des problèmes de souveraineté et de sécurité nationale, mais aussi des problèmes industriels et dans les usages. Nous avons des atouts industriels et technologiques, mais

ne sommes pas à la hauteur de la situation. Cela met l'accent sur l'obsolescence de la seule obsession concurrentielle, qui nous a fait passer à côté d'une véritable politique industrielle. Ayons une politique industrielle à la hauteur des enjeux contemporains. Il ne s'agit pas de conquérir des marchés, mais de maîtriser une technologie donnant la main sur le monde. Des politiques de concurrence industrielle ou protectionnistes impliquant une guerre commerciale accrue suffiront-elles à traiter ces enjeux ? Il faudrait réfléchir à un partage mondial, et les traiter comme un bien commun, au même titre que l'eau, d'intérêt vital. Est-ce utopique ? Je n'en suis pas certain.

Nous avons traité la politique industrielle publique avec désinvolture, avec une logique concurrentielle européenne. Bruno Le Maire a un discours un peu différent désormais. C'est très bien de faire des batteries électriques, mais allons plus loin. Actuellement, il serait impossible de faire le CERN (Organisation européenne pour la recherche nucléaire) avec la logique concurrentielle actuelle. Impulsons un débat d'une autre ampleur. Je me félicite que la proposition de loi ne soit pas uniquement tournée contre Huawei mais qu'elle prévoie des autorisations pour tous les opérateurs ; les Chinois ne sont pas les seuls à espionner…

M. Christian Cambon, président. – Cette proposition de loi sera examinée en séance publique mercredi 26 juin après-midi. L'Europe a raté une porte.

M. Bruno Sido. – Je remercie le rapporteur et le président. La cybersécurité est un sujet qui ne date pas de l'invention de la 5G. J'ai décrit ses enjeux dans un rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques (opecst), sans angélisme. J'ai fait l'expérience à l'Anssi en passant par un portique : toutes mes données ont été interceptées – numéros de téléphone, courriels, effacés ou non… La 5G n'apportera rien.

Le cryptage est une technologie cachant ce qu'on veut transmettre. Si l'on a mis quelques années à décrypter la machine Enigma, désormais, grâce à leur puissance, les ordinateurs décryptent en quelques heures voire minutes. Pour des affaires vraiment secrètes, des informations d'État, il faudra revenir aux fondamentaux, au bouche-à-oreille ou au messager portant un message. Il n'y a pas d'autre solution avec ces technologies.

M. Christian Cambon, président. – On peut rêver !

M. Olivier Cadic. – Cette proposition de loi est utile et bienvenue. J'ai soutenu l'amendement du gouvernement lors de la loi Pacte. Il y a urgence. Le Sénat avait demandé au Gouvernement d'inclure ces dispositions dans un texte législatif. La Chine garantit son indépendance en mettant les autres pays sous sa dépendance, avec un risque de vulnérabilité. La Chine n'autorise pas de réciprocité et a créé son propre cyber-mur, créant un monde qui nous est imperméable, grâce aux technologies vidéo et de

reconnaissance faciale pour contrôler sa population. Elle conditionne son financement d'infrastructures dans le cadre des routes de la soie par la signature de contrats avec Huawei, pour l'installation de la 5G. Après Djibouti, Huawei équipe l'Ile Maurice de 10 000 caméras, dont trois devant la résidence de l'ambassadeur britannique…

Je l'avais dit il y a un an : nous devons avoir une approche offensive sur le cyber et non exclusivement défensive. Je suis heureux de voir l'évolution de notre politique. Compte tenu de la stratégie chinoise, nous devrons envisager, à terme, de rendre notre cyberespace imperméable aux équipements chinois. Ce texte est un premier pas, pour nous protéger. L'urgence est ensuite de faire émerger les leaders européens du monde numérique de demain et assurer ainsi notre indépendance.

M. Gilbert Roger. – Ce rapport est important. Je partage les réflexions de Pierre Laurent sur l'erreur d'avoir abandonné des pans entiers de souveraineté industrielle. La bataille est un peu perdue. M. Ladislas Poniatowski est clairvoyant. Ne faut-il pas constituer un réseau indépendant sécurisé pour la sécurité nationale – armée, eau, santé ? Nous avons des satellites indépendants et autonomes pour transmettre des données militaires. Mais je ne sais pas quel sera le sort électoral du premier sénateur qui dira aux Français que nous refusons la 5G en raison de Huawei…

L'Anssi s'inquiète de la sécurité des parlementaires et des systèmes qui sont mis à notre disposition. J'aime bien les technologies. En Jordanie, en visite sur une base militaire, on nous a recommandé la messagerie chiffrée Citadel, développée par Thalès. Mais c'est impossible, je n'y arrive pas. Le Sénat n'a pas encore décidé que faire, mais nous pourrions tous basculer chez Qwant.

J'ai presque envie de m'abstenir sur les amendements : cela me gêne que le Premier ministre seul prenne une décision sans la motiver et sans contrôle.

M. Rachel Mazuir. – Le contrôle est réalisé par l'Anssi et l'Arcep.

M. Gilbert Roger. – Nous sommes en démocratie ; souhaitons que cela dure longtemps. Les Italiens ont basculé dans une forme de démocratie particulière. Imaginez un Premier ministre d'une potentielle présidente de la République... Nous n'écrivons pas pour l'immédiat mais pour de longs mois. Monsieur Allizard, prémunissez la démocratie d'un Premier ministre éloigné de nos valeurs communes.

M. Christian Cambon, président. – Le deuxième alinéa est conditionné à la mise en cause de la sécurité nationale….

M. Michel Boutant. – La 5G sera une vraie déferlante à succès, compte tenu de toutes les applications possibles. Nous, parlementaires – et cette proposition de loi va dans le bon sens – devons-nous assurer que les

mesures seront prises pour protéger les données sensibles. Il en va de notre sécurité et de notre souveraineté.

Jusqu'à présent, nos forces armées, services de renseignement et forces de sécurité avaient des réseaux de transmission totalement autonomes et protégés : Acropol pour la police, Rubis pour la gendarmerie, Quartz dans les outre-mer… Grâce aux progrès technologiques, la tentation est grande, pour la police et la gendarmerie, de s'en remettre aux opérateurs traditionnels pour la transmission de leurs informations, même s'il serait simple de leur réserver certains créneaux. La tablette Neogend utilise ainsi certains créneaux réservés.

Avec la 5G, les appareils peuvent converser les uns avec les autres sans passer par des relais par lesquels ils bornent, compliquant d'autant plus les enquêtes terroristes !Dans le cadre du développement de la 5G, nous serons obligés d'adopter de nouvelles dispositions, au-delà de celles adoptées *a minima* aujourd'hui. La gendarmerie et la police veulent un système de communication simple, rapide, mais cela peut être dangereux, avec un risque de captage voire de modification des données. Soyons-en conscients.

Le deuxième amendement me pose problème. M. Pascal Allizard prévoit un régime dérogatoire. Je ne fais pas de procès d'intention au Premier ministre actuel, ni au suivant. Mais le Premier ministre ne peut-il pas déjà invoquer le secret-défense pour refuser de motiver sa décision ? Je suis sceptique.

M. Rachel Mazuir. – Lors des attentats de 2015, les forces de sécurité ont utilisé Whatsapp – sans commentaire… Rubis, Acropol et Quartz fonctionnent très bien, et sont une nécessité. Lorsqu'on réfléchit à cela, après coup, cela fait froid dans le dos…

M. Yannick Vaugrenard. – Cela rappelle *1984* de George Orwell, écrit en 1949, roman prémonitoire… Avons-nous les moyens technologiques de répondre à nos ambitions ? Il n'est pas responsable de nous focaliser sur la Chine et Huawei. Les États-Unis nous ont déjà espionné et nous espionnent… Ayons une réflexion plus globale sur la nécessité de l'Europe. La France seule ne fera pas grand-chose, il faut une articulation européenne. Ne faudrait-il pas formaliser un point d'étape et une évaluation annuelle des mesures que nous prenons ? Les évolutions technologiques sont extrêmement rapides…

M. Joël Guerriau. – Nos préoccupations vont toutes dans le même sens : doute, inquiétude, frustration quant à la position européenne sur un sujet aussi important. Nous avons tous une identité numérique, que nous créons grâce à nos smartphones, par les diverses applications par lesquelles nous montrons notre activité parlementaire : Twitter, Facebook… Est-ce sans danger ? L'empreinte numérique qualifie précisément qui nous sommes, notre profil consumériste. Elle devient importante quand nous prenons

davantage de responsabilités et peut alors être utilisée. C'est dangereux pour la sécurité des personnes et des pays.

Je rejoins l'avis de M. Olivier Cadic sur la Chine : Huawei est un danger, ne soyons pas aveugles, et prévoyons des pare-feux. Les GAFA (Google, Amazon, Facebook, Apple) échappent à l'impôt. Quelle est l'efficacité d'une loi sur un sujet dépassant les frontières ? Un proverbe chinois dit : « lorsque le tonnerre éclate, il est trop tard pour se boucher les oreilles. » Je crains que le tonnerre n'ait déjà éclaté.

M. Christian Cambon, président. – Le Maroc a confié à Huawei l'utilisation de la 5G… Certaines applications sont extraordinaires : on pourra déceler immédiatement, pour des *pacemakers* connectés à la 5G, une défaillance cardiaque – mais aussi accélérer votre rythme cardiaque pour vous faire revenir à la raison… C'est orwellien !

M. Pascal Allizard, rapporteur pour avis. – Madame Raimond-Pavero, je n'ai pas de réponse immédiate à vous donner sur le risque de remontée des données des radars militaires..

Madame Goy-Chavent, la fibre et la 5G sont deux technologies différentes, avec des vulnérabilités différences. La réponse passe par la résilience de l'ensemble du système et la notion de zones géographiques. Assurons-nous l'interopérabilité sur l'ensemble des plaques, et de la protection des sites les plus sensibles. Cela fait partie des critères d'appréciation à disposition du Premier ministre.

Madame Garriaud-Maylam, nous avons étudié ce qu'ont fait les autres pays : les États-Unis et l'Australie ont interdit Huawei ; l'Allemagne s'engage dans une politique de normes, mais nous ne savons pas où cela va la mener – elle est un peu derrière la France ; les Britanniques ont trouvé une solution pragmatique, ils créent un laboratoire commun avec Huawei, qu'ils espèrent contrôler en étant dedans. Il n'y a pas encore de réponse européenne.

Mme Joëlle Garriaud-Maylam. – C'est dommage.

M. Pascal Allizard, rapporteur pour avis. – Je partage le constat de M. Poniatowski. La 5G est une réalité, comme les routes de la soie ; on est dedans ou non. L'Europe et la France ont un retard technologique et industriel sur ce sujet. La proposition de loi donne du temps à nos opérateurs, afin de ne pas empêcher le déploiement de la 5G. Par le système d'autorisation, elle donne une chance supplémentaire aux équipementiers européens de rattraper leur retard.

Monsieur Patriat, il faut se doter de moyens de contrôle. Nous souhaitons une commission mixte paritaire conclusive, même si cela suppose de retravailler les amendements.

Monsieur Mazuir, la 5G constitue un vrai saut technologique ; elle n'est pas de la 4G améliorée mais répond à un autre paradigme. Les

« appareils » concernés sont davantage des logiciels que du matériel, avec une particularité. Actuellement, opérateurs et équipementiers ont une grosse boîte à chaque bout, même s'ils utilisent le même tuyau pour communiquer entre les boîtes. Désormais, il y a une petite boîte coupée en segments, et ces boîtes communiquent toutes entre elles. Le réseau et la porosité de chaque boîte sont extrêmement compliqués à contrôler.

L'Anssi aura une mission particulière, car les risques sont multipliés et déconcentrés. La 5G se fait déjà, avec ou sans Huawei. Nous devons nous adapter même sans maîtriser toutes ses potentialités.

Sur mon amendement relatif à la décision motivée du Premier ministre, nous avons une lecture *a contrario* de la rédaction actuelle du texte : tout motiver sans exception peut aussi créer une vulnérabilité. Faut-il instaurer un contrôle complémentaire ? Peut-être, mais des exceptions me semblent nécessaires pour protéger le secret de la défense nationale en certaines circonstances

L'article L.311-5 du code des relations entre le public et l'administration dispose que de nombreux documents ne sont pas communicables. Ces exceptions existent en droit. Conservons cet amendement, même s'il faut peut-être prévoir un contrôle parlementaire. Je peux le modifier mais pas le retirer.

Monsieur Laurent, les pays européens ont pris du retard technologique. Nous ne sommes pas absents en retard par rapport à d'autres opérateurs, d'où le régime d'autorisation pour gagner du temps et se remettre à niveau.

Monsieur Sido, les problèmes de cybersécurité ne sont pas nouveaux, mais la dématérialisation et la complexité croissantes du système de 5G rend le sujet plus difficile. Le pigeon voyageur est extrêmement dématérialisé actuellement !

Oui, Monsieur Cadic, la Chine refuse toute réciprocité, et applique la loi du plus fort. Avant elle, d'autres États nations ont appliqué ces principes. Notre responsabilité, française et européenne, est de retrouver des marges d'indépendance . Nous partageons le constat, et il faut faire avec.

Monsieur Roger, la sécurisation des réseaux nécessiterait de les doubler ou de les tripler. Des opérateurs comme la SNCF ont des réseaux parallèles. On voit dans les salons spécialisés la mise en place de boitiers spécialisés en tête ou fin de réseau. Chaque institution connaît et met en place ses solutions.

Monsieur Boutant, les réseaux protégés des forces armées doivent le rester, mais on ne pourra pas empêcher un passage partiel sur les autres réseaux. Il faut surprotéger les extrémités, mais on ne va pas démultiplier à l'infini les réseaux 5G.

Oui, Monsieur Vaugrenard, c'est 1984. Ce texte n'est pas définitif mais il permet de fonctionner aujourd'hui. Le rapporteur d'un texte peut réaliser un suivi annuel ; faisons-le au sein de notre commission, afin d'évaluer la situation et l'efficacité du texte. Ainsi, nous pourrions le revoir au fur et à mesure des évolutions technologiques.

Monsieur Guerriau, les GAFA jouent déjà un rôle dans le système actuel, qui ne va pas décroître. Je citerai un autre proverbe chinois : « Assieds-toi au bord de l'eau et tu verras passer le cadavre de ton ennemi. » Mais je ne suis pas sûr que cela arrive !

EXAMEN DES ARTICLES

M. Christian Cambon, président. – Je rappelle que nous sommes saisis pour avis.

Article 1er

M. Pascal Allizard, rapporteur pour avis. – L'amendement ETRD.1 ajoute dans le texte l'acheminement gratuit des appels d'urgence, dont la fourniture gratuite par les opérateurs aux services d'urgence des informations relatives à la localisation de l'appelant (f) et l'acheminement des communications des pouvoirs publics destinées au public pour l'avertir de dangers imminents ou atténuer les effets de catastrophes majeures, aux règles qui doivent être respectées par les opérateurs.

L'amendement ETRD.1 est adopté.

M. Pascal Allizard, rapporteur pour avis. – L'amendement ETRD.2 introduit une exception à l'obligation de motivation de la décision du Premier ministre pour des raisons de sécurité nationale. Nous ne dérogeons pas au droit commun puisque cette disposition existe déjà dans le code des relations entre le public et l'administration.

M. Jean-Marc Todeschini. – Comme l'ont rappelé MM. Boutant, Mazuir et Roger, pourquoi un tel amendement si la possibilité existe déjà ? Sauf à trouver un motif différent, pourquoi introduire un amendement qui peut poser problème à l'avenir ?

M. Pascal Allizard, rapporteur pour avis. – Dans un raisonnement *a contrario*, on créerait une vulnérabilité par la diffusion d'informations.

L'amendement ETRD.2 est adopté.

M. Pascal Allizard, rapporteur pour avis. – L'amendement ETRD.3 conforte l'examen par le Premier ministre, dans la préparation de sa décision des modalités de déploiement et d'exploitation mises en place par l'opérateur, et de la situation de l'opérateur et de ses prestataires, y compris par sous-traitance, au regard des risques de contrôle ou d'ingérence d'un État non-membre de l'Union européenne.

L'amendement ETRD.3 est adopté.

M. Pascal Allizard, rapporteur pour avis. – Je remercie le président de m'avoir confié ce rapport et je remercie mes collègues pour leur vote.

M. Christian Cambon, président. – Merci pour ce travail de fond dans des conditions compliquées. Nous aurons un beau débat en séance publique.

TABLEAU DES SORTS

Article 1er			
Auteur	**N°**	**Objet**	**Sort de l'amendement**
M. ALLIZARD	ETRD.1	Extension des règles devant être respectées par les opérateurs.	**à déposer**
M. ALLIZARD	ETRD.2	Maintenir la possibilité de dérogation au principe de motivation de la décision pour préserver le secret de la défense nationale	**à déposer**
M. ALLIZARD	ETRD.3	Affirmer la prise en considération des critères d'appréciation du risque par le Premier ministre.	**à déposer**

ANNEXE 1

AMENDEMENTS PRÉSENTÉS PAR LA COMMISSION DES AFFAIRES ÉTRANGÈRES ET DES FORCES ARMÉES

COMMISSION DES AFFAIRES ÉCONOMIQUES	PROPOSITION DE LOI EXPLOITATION DES RÉSEAUX RADIOÉLECTRIQUES MOBILES (n° 454)	N° COM-8 **12 JUIN 2019**

A M E N D E M E N T

présenté par

M. ALLIZARD
au nom de la commission des affaires étrangères

_____

ARTICLE 1ER

Alinéa 10

Après les mots

règles mentionnées aux a, b

remplacer

et e

par les mots

e, f et f bis

OBJET

Ajouter l'acheminement gratuit des appels d'urgence dont la fourniture gratuite par les opérateurs aux services d'urgence des informations relatives à la localisation de l'appelant (f) et l'acheminement des communications des pouvoirs publics destinées au public pour l'avertir de dangers imminents ou atténuer les effets de catastrophes majeures, aux règles qui doivent être respectées par les opérateurs et dont le manque de garantie pourrait motiver un 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. Ces conditions qui figurent au I de l'article L.33-1 du code des postes et des communications électroniques concernent des services importants pour la sécurité nationale.

PROPOSITION DE LOI

:XPLOITATION DES RÉSEAUX RADIOÉLECTRIQUES MOBILES

N°	COM-9

COMMISSION DES AFFAIRES ÉCONOMIQUES

(n° 454)

12 JUIN 2019

A M E N D E M E N T

présenté par

M. ALLIZARD
au nom de la commission des affaires étrangères

_____

ARTICLE 1ER

Alinéa 10

Après le mot

refuse

supprimer les mots

par décision motivée

Ajouter la phrase suivante :

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 du a au f du 2° de l'article L. 311-5 du code des relations entre le public et l'administration.

OBJET

Il est des circonstances dans lesquelles l'Etat peut être amené à ne pas motiver ses décisions, il en va ainsi lorsque des textes législatifs interdisent la divulgation ou la publication de faits ou de dispositions couverts par le secret, et notamment par le secret de la défense nationale.

Le principe de la motivation de la décision de refus d'autorisation par le Premier ministre, figure déjà dans le code des relations entre le public et l'administration à l'article L.211-2 qui est donc d'application générale. Cependant cet article introduit une restriction pour préserver le secret dans certaines circonstances définies par la loi : « doivent être motivées les décisions qui : (…) refusent une autorisation, sauf lorsque la communication des motifs pourrait être de nature à porter atteinte à l'un des secrets ou intérêts protégés par les dispositions du a au f du 2° de l'article L.311-5.

En réaffirmant ce principe sans mentionner explicitement les restrictions figurant à l'article L.311-5 précité, il pourrait être considéré, par un raisonnement a contrario, que le législateur a renoncé, dans le cas spécifique de l'article L. 34-12 du code des postes et des communications électroniques, à l'application des dispositions permettant de déroger à l'obligation générale de motivation.

Or, cette dérogation doit impérativement être préservée dans un domaine où l'enjeu est d'éviter un risque d'atteinte aux intérêts de la défense et de la sécurité nationale.

PROPOSITION DE LOI

EXPLOITATION DES RÉSEAUX RADIOÉLECTRIQUES MOBILES

N°	COM-10

COMMISSION DES AFFAIRES ÉCONOMIQUES

(n° 454)

12 JUIN 2019

A M E N D E M E N T

présenté par

M. ALLIZARD
au nom de la commission des affaires étrangères

_____

ARTICLE 1ER

Alinéa 11

Après les mots

Le Premier ministre

remplacer les mots

peut prendre

par le mot

prend

OBJET

Il s'agit d'affirmer que pour fonder sa décision, le Premier ministre prend en considération pour l'appréciation du risque sérieux d'atteintes aux intérêts de la défense et de la sécurité nationale :

- les modalités de déploiement et d'exploitation mises en place par l'opérateur,

- 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 Etat non-membre de l'Union européenne

ANNEXE 2

LISTE DES PERSONNES AUDITIONNÉES

Auditions communes avec la Rapporteure de la commission des affaires économiques

Mardi 21 mai 2019

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

Mardi 28 mai 2019

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

Mercredi 29 mai 2019

Table ronde des « opérateurs verticaux » :

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

– *SNCF* : **MM. Benoît TIERS**, directeur général et **Sébastien KAISER**, directeur Connectivité & Réseaux de la SNCF ;

Table ronde des « Opérateurs de télécommunications »

– *Fédération française des télécoms (FFT):* **M. Michel COMBOT**, directeur général ;

• *Bouygues Télécom* : **M. Hervé DE TOURNADRE**, directeur des affaires réglementaires ;

• *Altice SFR* : **M. Arthur DREYFUSS**, Secrétaire général et **Mme Marie-Georges BOULAY**, directrice des affaires réglementaires ;

• *Orange* **: MM. Laurentino LAVEZZI**, directeur des affaires publiques et **Pascal NOURRY**, responsable sécurité des réseaux ;

– *Iliad-Free :* **M. Pascal MAYEUX**, directeur des obligations légales et **Mme Ombeline BARTIN,** responsable des relations institutionnelles.

Table ronde des « Équipementiers des réseaux » :

– Nokia : **M. Marc CHARRIÈRE**, secrétaire général ;

– *Huawei Technologies France* : **MM. Minggang ZHANG**, directeur général adjoint, **Antoine BOUR**, Expert Réseau-Sécurité et **Jean-Christophe AUBRY**, Responsable des affaires publiques ;

– *Ericsson* : **M. Viktor ARVIDSSON**, directeur des relations institutionnelles et de l'innovation et **Mme Corinne MULLER**, directrice de la communication ;

– *Cisco France* : **MM. Laurent DEGRÉ**, directeur général et **Jean-Charles GRIVIAUD**, chief Security Officer France ;

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

Audition du Rapporteur pour avis

Mardi 23 mai 2019

– **M**. **Patrick PAILLOUX**, directeur technique de la direction générale de la sécurité extérieure (DGSE).