ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Mardi
2 avril 2019
Séance de 9 heures 30

Compte rendu n° 31

SESSION ORDINAIRE DE **2018-2019**

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de M. Jean-Jacques Bridey, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures trente.

M. le président Jean-Jacques Bridey. Nous sommes réunis aujourd'hui pour examiner la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, dont la commission s'est saisie pour avis.

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

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

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

La 5G revêt des enjeux de défense et de sécurité nationale pour des raisons qui tiennent davantage à ses usages et à ses applications, dont nous avons encore du mal à imaginer l'étendue. Cette technologie permettra des progrès considérables pour ce qui est de la capacité des réseaux. D'abord, elle accroîtra considérablement les débits, qui pourraient atteindre un ou plusieurs gigaoctets par seconde, ce qui revêt une importance considérable dans le domaine de la défense, notamment pour le combat « collaboratif ». Les temps de latence dans les transmissions seront également réduits, ce qui permettra notamment aux véhicules autonomes d'être beaucoup plus réactifs et, sur le champ de bataille, de mettre plus rapidement en relation un capteur et un effecteur, et de gagner ainsi la supériorité opérationnelle. Enfin, les réseaux virtualisés de 5G pourront être orientés presque en temps réel en fonction des besoins locaux, ce qui permettra d'éviter la saturation des réseaux ; notons que la concentration des moyens est une logique bien maîtrisée par les forces dans leurs zones d'intervention.

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

les réseaux sont de plus en plus vitaux pour le fonctionnement des services de la Nation et les secours, les forces de sécurité intérieure et les armées en auront de plus en plus besoin.

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

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

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

De façon cohérente avec l'objectif de protection des intérêts de la défense et de la sécurité nationale, le nouveau régime d'autorisation ne concerne que les opérateurs d'importance vitale, les OIV. Leur liste est classifiée, mais on peut estimer qu'ils sont plusieurs centaines à l'échelle nationale, parmi lesquels les grands opérateurs de téléphonie mobile nationaux ont toutes les chances de figurer.

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

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

permettra, au cas par cas, de ne pas soumettre à autorisation toutes les mises à jour logicielles. Nous en reparlerons lors de l'examen des amendements.

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

J'émets un avis favorable à cette proposition de loi. La saisine pour avis de la commission de la Défense a permis de mettre en avant les enjeux de défense à chaque audition et de promouvoir l'esprit de défense, aussi bien auprès de nos interlocuteurs que de nos collègues siégeant dans d'autres commissions. Nous ne pouvons que nous en féliciter.

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

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

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

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

M. Yannick Favennec Becot. Le déploiement du réseau mobile de cinquième génération constitue une innovation de rupture, dans un domaine touchant à la souveraineté et à la sécurité. Sur des questions aussi sensibles que celles relatives à la protection des données, à la sûreté nationale ou à des choix technologiques structurants, il est dommage que le Gouvernement fasse le choix de passer en catimini, d'abord *via* un amendement au projet de

loi PACTE, puis par une proposition de loi, projet de loi déguisé qui permet de faire l'économie de l'étude d'impact et de l'avis du Conseil d'État utiles pour éclairer le législateur.

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

Les grands choix en matière numérique ont des implications sécuritaires indéniables, mais les risques potentiels relatifs au déploiement de la 5G, tant du fait de la nature du réseau que de ses usages, notamment dans le domaine industriel, demeurent mal connus.

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

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

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

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

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

Il faut aborder cette proposition de loi sans naïveté géopolitique. Il n'est pas question d'approuver des dispositions destinées uniquement à soutenir les États-Unis dans leur entreprise d'offensive économique et diplomatique vis-à-vis de la Chine. Il est vrai qu'il convient de se protéger contre des risques d'un cyberespionnage chinois, qui pourrait passer par l'équipement des réseaux mobiles. En 2017, une loi a été votée en Chine, qui prévoit que

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

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

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

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

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

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

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

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

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

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

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

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

L'objectif de cette proposition de loi est de faire évoluer les exigences de sécurité sur les nouveaux équipements qui supportent les réseaux 5G. Il est essentiel de garantir la sécurité et la fiabilité des réseaux, dont certains serviront, par exemple, au fonctionnement des véhicules connectés. Les investissements étant colossaux, il y va aussi de l'intérêt économique sur le long terme.

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

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

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

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

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

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

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

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

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

Nous sommes effectivement dans un calendrier adéquat – je n'avais pas mentionné cet élément dans mon propos introductif – au regard de celui de l'attribution des fréquences,

qui sera effective à la fin de l'année, mais également des grands choix d'investissement que nécessite la 5G. Il faut sécuriser dès à présent le cadre juridique applicable car, une fois que l'on a choisi un équipementier, les coûts liés à des modifications ultérieures sont extrêmement importants, de même que les délais nécessaires pour s'adapter : cela peut prendre plusieurs années.

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

Monsieur Bazin a évoqué le contrôle parlementaire des dispositifs. La saisine pour avis de notre commission a bien pour objet de réintroduire une forme de contrôle parlementaire sur le sujet. En matière de défense et de sécurité, nous avons effectivement intérêt à trouver le bon équilibre entre ce que fait l'exécutif et ce que fait le Parlement. On pourrait s'étonner, à cet égard, que le Parlement n'ait pas accès – entre autres – à la liste des OIV. Pour ma part, je trouve que le mécanisme est bien conçu. Nous pouvons, chacun à notre niveau, échanger avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), pour savoir quelles sont les modalités d'autorisation des équipements de réseau. Aller plus loin risquerait de poser des problèmes de sécurité nationale.

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

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

Monsieur Belhamiti, vous avez parlé de l'aménagement numérique du territoire. C'est quelque chose que nous devons bien entendu garder à l'esprit. L'une des craintes que l'on pouvait avoir à l'égard de cette proposition de loi tenait au fait que l'on vient de conclure un *new deal* avec les opérateurs, qui s'est traduit par des engagements importants de leur part concernant le déploiement de nouveaux relais 4G. Le Premier ministre a d'ailleurs fait des annonces il y a une dizaine de jours à ce sujet. Dans ma circonscription, par exemple, un

nouveau relais 4G va être installé du fait de cet accord. La liste des 400 premiers – soit, en moyenne, un peu moins d'un par circonscription – a été révélée, me semble-t-il. Il faut effectivement rester attentif à l'exigence d'un aménagement numérique du territoire. Certes, ce n'est pas le rôle principal de la commission de la Défense que de s'intéresser à la question mais, au-delà du service rendu à nos concitoyens, l'aménagement numérique de tout le territoire est aussi important pour le fonctionnement de nos services critiques – il a ainsi été question de la gendarmerie.

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

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

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

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

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

Article 1er

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

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

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

M. Mounir Belhamiti. Je retire l'amendement.

L'amendement est ***retiré****.*

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

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

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

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

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

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

M. le président. Pas seulement.

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

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

M. Alexis Corbière. Nos collègues ont raison d'ouvrir ce débat : les événements des dernières années nous montrent, notamment à travers le cas des métadonnées révélées par Edward Snowden, que les enjeux d'ordre économique et politique sont extrêmement importants. On l'a vu par exemple à propos d'Alstom, me glisse mon collègue Bastien Lachaud. Cela dépasse largement la seule question de la sécurité nationale : cela concerne les intérêts économiques et les stratégies économiques et industrielles. Il y a donc sans doute un

intérêt à élargir la formulation pour que l'ensemble de ces éléments soient bien pris en compte.

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

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

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

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

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

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

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

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

M. le président. Ou à la SNCF.

M. Thomas Gassilloud, rapporteur pour avis. Effectivement. Il peut s'agir de services dont l'importance est critique ou de réseaux délivrant par la suite un service au grand public. La SNCF, par exemple, pourrait déployer un réseau 5G pour ses propres usages puis, quelques années plus tard, sur la base de ce réseau, ouvrir le service à ses usagers pour divers services. Je rappelle que le droit des OIV dépend du code de la défense : d'où le fait que nous visions, dans ce texte, les intérêts de défense.

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

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

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

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

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

M. Laurent Furst. Je ferai une réflexion de profane sur le sujet. Tout à l'heure, j'ai abordé la question des satellites et de la sécurité des câbles sous-marins ; maintenant, il s'agit des logiciels. On voit bien que tous ces problèmes forment un ensemble. Or la proposition de loi ne traite que d'une partie de la question, qui va se poser pour ainsi dire immédiatement, car le déploiement de la 5G sur le territoire national va se faire de manière extrêmement rapide. Je nous invite donc tous à reprendre, dans le cadre de nos travaux, l'ensemble de la question dans les semaines et les mois à venir.

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

M. Thomas Gassilloud, rapporteur pour avis. Monsieur Lachaud, votre amendement concernerait l'ensemble des appels d'offres publics, y compris par exemple celui d'une mairie souhaitant commander un logiciel de bureautique. Le périmètre paraît donc très large. Je rappelle, une fois encore, que des règles dérogatoires existent déjà en matière de défense et de sécurité. Nous pouvons porter la même appréciation que vous sur le choix fait par certaines entités ; de là à proscrire l'acquisition de logiciels étrangers par l'ensemble des

acheteurs publics, il y a un pas qui me semble potentiellement excessif car, parfois, le choix de ces logiciels est pertinent dans un contexte donné. Leur laisser la liberté d'appréciation, sous le contrôle du Parlement, peut être une option tout à fait souhaitable.

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

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

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

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

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

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

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

*L'amendement est **retiré**.*

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

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

*L'amendement est **retiré**.*

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

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

M. Thomas Gassilloud, rapporteur pour avis. C'est une lourde responsabilité qui m'est confiée puisque, dans le cadre de ce texte, vous l'avez bien compris, on cherche à trouver un équilibre : il s'agit de préserver la sécurité de la Nation, s'agissant d'un certain

nombre d'enjeux, sans pour autant entraver le développement des télécoms, et donc notre économie. En ne fondant pas son action sur un risque « sérieux », on pourrait donner l'impression que l'intervention du Premier ministre est susceptible d'être aléatoire ou arbitraire. En effet, en matière de télécommunications et d'informatique, au sens large, le risque existe en permanence.

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

L'amendement est ***retiré****.*

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

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

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

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

Article 2

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

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

L'amendement est ***retiré****.*

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

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

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

Article 3

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

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

La séance est levée dix heures quarante.

*

* *

Membres présents ou excusés

Présents. - M. Xavier Batut, M. Thibault Bazin, M. Mounir Belhamiti, M. Christophe Blanchet, Mme Aude Bono-Vandorme, M. Jean-Jacques Bridey, M. Philippe Chalumeau, M. Alexis Corbière, Mme Marianne Dubois, Mme Françoise Dumas, M. Yannick Favennec Becot, M. Laurent Furst, M. Claude de Ganay, M. Thomas Gassilloud, Mme Séverine Gipson, M. Fabien Gouttefarde, M. Stanislas Guerini, M. Loïc Kervran, M. Bastien Lachaud, Mme Sereine Mauborgne, M. Philippe Michel-Kleisbauer, Mme Bénédicte Pételle, Mme Josy Poueyto, Mme Natalia Pouzyreff, M. Joaquim Pueyo, M. Charles de la Verpillière

Excusés. - M. Jean-Philippe Ardouin, M. Florian Bachelier, M. Didier Baichère, M. Sylvain Brial, Mme Carole Bureau-Bonnard, M. Luc Carvounas, M. André Chassaigne, M. Olivier Faure, M. Richard Ferrand, M. Jean-Jacques Ferrara, M. Christian Jacob, M. Jean-Michel Jacques, Mme Manuéla Kéclard-Mondésir, M. Jean-Christophe Lagarde, M. Fabien Lainé, M. Jean-Charles Larsonneur, M. Didier Le Gac, M. Christophe Lejeune, M. Jacques Marilossian, M. Franck Marlin, M. Joachim Son-Forget, Mme Sabine Thillaye, Mme Laurence Trastour-Isnart, M. Patrice Verchère