Stratégies d'influence et déploiement de la 5G en France : la recherche d'un point d'équilibre entre impératifs de sécurité et développement économique

Tuteur de stage : Jean-Claude BRIER, Délégué régional Ile-de-France d'Altice France
Directeur de mémoire : Colonel Dominique MUSSEAU

Master 2 Droit public, option droit et politique de défense et de sécurité nationale
Université de Lille – Année universitaire 2018-2019

Maxence CHALLUT

REMERCIEMENTS

Je tiens à remercier le Lieutenant-Colonel MUSSEAU pour m'avoir accompagné dans la réalisation de ce travail universitaire et pour le temps passé à me prodiguer de précieux conseils.

Je tiens également à remercier Madame Myriam MADORE et Monsieur François VINCENT pour avoir accepté de mettre leurs lumières au service de ce mémoire. Leur expertise ainsi que leurs interventions m'ont permis de saisir toutes les facettes du sujet et d'apporter une source de documentation très intéressante à ce travail de recherche.

Je tiens à remercier tout particulièrement Jean-Claude BRIER, Délégué régional d'Ile-de-France d'Altice France, pour s'être attaché à me présenter toutes les subtilités du domaine des affaires publiques. Il m'a donné l'envie de continuer à évoluer dans ce secteur qui se situe à la croisée du droit, de la communication et des relations publiques.

Enfin, cette expérience m'a permis de mettre en pratique les connaissances acquises au cours de mes cinq années d'enseignements universitaires. Cela m'a définitivement convaincu du fait que l'Université nous a admirablement bien préparé aux étapes qui nous attendront demain, alors, pour cela aussi, je souhaite remercier l'ensemble du personnel des Universités de Reims Champagne-Ardenne et de Lille.

SUMMARY

While the arrival of the fifth generation of telephone switchboards is imminent, the Government has made the decision to supervise the deployment with a new legal package. Mainly targeted by this text, operators have put in place important lobbying campaigns to limit the harmful effects of this new law on their activities. The arguments of the telecom operators have found an echo among senators, who have dcided to rebalance the text promulgated on August 2nd, 2019. This new licensing regime takes into consideration the need to raise the level of security networks, given 5G, while allowing a rapid arrival of this new technology on the french territory, synonymous with economic potential and new activities for industry, but also political responses to the major problems that shakes the country in the digital sector.

Le rapport que je vous fais parvenir aujourd'hui incarne, pour moi, bien plus que cinq mois de stage au sein du groupe Altice France. Cette entrée dans le monde professionnel a en effet été l'occasion de mettre en pratique mes cinq années de droit passées au sein des Universités de Reims Champagne-Ardenne puis de Lille.

En intégrant cette société, j'ai eu la chance de me confronter à des secteurs d'activité dissemblables mais complémentaires, ce qui a conduit à apporter de la variété dans les missions qui m'incombaient. Altice France est en effet un groupe fondé sur la convergence entre télécoms et médias. A travers SFR, Altice France est, dans un premier temps, le 2ème opérateur de télécommunication sur le territoire ; partenaire historique des collectivités, il couvre également 99% de la population en 4G. Dans un second temps, Altice France est également un groupe médias de premier plan avec plus d'une dizaine de chaînes de télévision et des titres de presse parmi lesquels BFM, RMC, Libération ou encore L'Express. Avec un chiffre d'affaire de 10,24 milliards d'euros pour l'année 2018, Altice France se présente comme un poids lourd de l'écosystème économique français.

De prime abord, établir un lien entre l'objet de ce stage et les problématiques de défense et de sécurité nationale n'était pas chose aisée. Toutefois, les vifs débats relatifs au déploiement de la 5G en France et dans le monde ont permis de faire émerger deux objectifs, parfois antagonistes, poursuivis par le Gouvernement et les opérateurs télécoms : garantir la sécurité et la résilience des réseaux et permettre le développement de potentialités économiques. M'intéresser à ce sujet a alors sonné comme une évidence. J'ai bénéficié d'une place de choix pour assister au bras de fer opposant les acteurs des télécoms aux instances administratives concernées ; je tenais donc à en établir un condensé, retraçant les différentes étapes qui ont permis d'accoucher sur le texte adopté finalement le mercredi 24 juillet 2019 par le Sénat, confirmant par la même la position que l'Assemblée nationale avait exprimée 6 jours plus tôt. Cette proposition de loi, qui vise à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, dite loi « 5G » ou encore loi « anti-Huawei », est à la croisée des enseignements que j'ai suivis au sein de ce Master 2 et des missions que j'ai été amené à réaliser durant mon stage professionnel.

C'est donc avec une immense fierté que je me permets d'attirer votre attention, aujourd'hui, sur ce travail qui constitue le point d'orgues de cinq années d'études qui m'ont préparé à entrer dans la vie professionnelle de la meilleure des manières.

SOMMAIRE

INTRODUCTION

« *Il faut avoir l'honnêteté, la franchise, la sincérité de l'admettre, le lobbying fait évidemment partie intégrante de la décision publique. En effet, comment imaginer, dans un pays libre comme le nôtre, une délibération, un vote, sans aucune intervention des personnes ou des groupements concernés ? Le jeu même des institutions démocratiques, la liberté d'expression et la liberté de la presse impliquent que chacun puisse défendre et promouvoir ses intérêts et s'organiser dans ce but* ». C'est par ces propos que Richard Ferrand, Président de l'Assemblée nationale, ouvrait le colloque « Lobbying : quelle place et quels enjeux pour la démocratie ? »[1] le 15 mai 2019.

En candidatant pour réaliser ce stage, mon objectif était de découvrir le lobbying sous toutes ses dimensions. De la proposition initiale d'une norme jusqu'à son adoption, en passant par l'organisation d'évènements publics ou la préparation d'entretiens avec des parties prenantes du groupe Altice France, j'ai assisté à la mise en place de stratégies d'influence visant à influer sur les décisions publiques qui, de par leur nature, pèsent ou auraient pu peser sur les activités du groupe.

Le texte législatif qui a particulièrement retenu l'attention des opérateurs de télécommunications ces derniers mois est la 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. Elle répond officiellement à la nécessité de se préparer au déploiement de la cinquième génération de standards de télécommunications mobiles (5G) sur le territoire, annoncé pour 2020 par l'Autorité de régulation des communications et des Postes[2] (Arcep).

La promulgation de cette loi, le 2 août 2019, marque le point d'orgues de plusieurs mois d'échanges, de débats et de rebondissements. Tout d'abord par sa forme : initialement inséré par un amendement du projet de loi relatif à la croissance et la transformation des entreprises, ce nouveau dispositif se voit rejeter par le Sénat au motif d'avoir été préparé trop hâtivement. Sujet d'envergure méritant son propre texte, la loi 5G aura par la suite opposé tous les acteurs

[1] Discours d'ouverture de Richard FERRAND, Président de l'Assemblée nationale, « Lobbying : quelle place et quels enjeux pour la démocratie ? », colloque organisé par Sylvain WASERMAN, Vice-président de l'Assemblée nationale, au titre de la délégation chargée des représentants d'intérêts et des groupes d'études, les 15 et 16 mai 2019

[2] Publication de l'Autorité de régulation des communications électroniques et des postes : « *5G : une feuille de route ambitieuse pour la France* », le 16 juillet 2018

du secteur sur le fond, preuve de sa délicatesse. Ainsi, quand les opérateurs français dénoncent une énième usine à gaz administrative entravant leurs activités, l'Agence nationale de la sécurité des systèmes d'information (l'ANSSI, la branche cybersécurité du Secrétariat Général de la Défense et de la Sécurité nationale (SGDSN)) plaide pour un contrôle plus strict encore que celui envisagé par le Gouvernement. Pourtant, des obligations similaires pesaient déjà sur les acteurs des télécoms français, de par leur statut et la nature de leurs missions.

En effet, les secteurs des communications électroniques, de l'audiovisuel et de l'information sont considérés comme d'importance vitale par le Gouvernement. Dès lors, on peut légitimement penser que les entreprises du secteur des télécommunications sont considérées comme des opérateurs d'importance vitale (OIV), que l'article L.1332-1 du code de la défense définit comme des « *opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* »[3]. Ce statut implique que les opérateurs télécoms français soient soumis à un dispositif juridique spécifique garantissant la résilience de leurs activités. Concrètement, ce dispositif repose sur la délivrance d'autorisations pour acquérir et installer des équipements 4G, visant à garantir la protection des systèmes d'information et le secret des correspondances. Ce cadre juridique repose sur deux fondements : l'article L.1332-6-1 qui dispose que « *Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2* (les OIV) *et 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. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais* »[4]. Ainsi que l'article R. 226-3 du Code pénal qui prévoit quant à lui que « *la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques* » qui sont de nature à permettre la captation de données informatiques sont soumises à une autorisation administrative délivrée par le Premier Ministre.

Officieusement, cette proposition de loi, que certains renomment volontiers « loi anti-Huawei », semble répondre à une suite d'évènements qui a fait naître, chez le Gouvernement, la crainte de voir les réseaux de télécommunication menacés par les nouveaux équipements qui

[3] Alinéa 1er, article L. 1332 du code de la défense
[4] Alinéa 1er, paragraphe 6 de l'article L. 1332 du code de la défense

accompagneront et permettront le déploiement de la 5G sur le territoire. En effet, dans la continuité de la guerre commerciale que se livrent Etats-Unis et Chine, Donald TRUMP prend un décret interdisant aux entreprises américaines d'utiliser des matériels de télécommunication fabriqués par des entreprises présentant un risque pour la sécurité nationale, le 15 mai 2019. La décision revient à empêcher les firmes américaines de commercer avec le leader international des équipements télécoms, l'entreprise chinoise Huawei, accusée d'espionnage pour le compte du Président Xi Jinping.

Dès lors, l'Administration américaine met en place une campagne de lobbying d'envergure visant à convaincre d'autres pays de refuser au géant chinois l'accès à leur marché[5]. Si l'appel est entendu par les plus proches alliés des Etats-Unis (Canada et Australie notamment), les pays d'Europe refusent de bannir Huawei et préfèrent attendre avant de se positionner. Lorsque les américains menacent de ne plus coopérer en matière de partage de renseignements si l'Allemagne en venait à accepter de contracter avec l'équipementier chinois, Huawei répond que son exclusion du marché européen aurait un coût : 55 milliards d'euros et 18 mois de délais supplémentaires pour déployer la 5G en se passant de ses services. La loi adoptée définitivement par le Parlement français le 24 juillet 2019 tire inéluctablement sa source de ces campagnes d'influence.

Pour les opérateurs, cette loi est présentée comme un frein au déploiement de la 5G ; elle allonge les procédures administratives relatives aux autorisations d'acquisition et d'installation des équipements et perturbe leur visibilité par rapport au calendrier prévisionnel qu'ils avaient établis. Pris entre les annonces ambitieuses du Gouvernement, qui leur demande de déployer cette nouvelle technologie au plus vite (en raison notamment des potentialités économiques qu'on lui prête), et les obligations qui leur incombent en tant qu'opérateurs d'importance vitale, les acteurs des télécoms français ont eux aussi mis au point des stratégies d'influence afin de limiter les effets de cette loi sur leurs activités.

Pour SFR, la situation est plus complexe que pour ses concurrents, un tableau intégré au rapport réalisé par la Sénatrice Catherine PROCCACIA et représentant les parts de marché

[5] S. DUMOULIN : « *Huawei : les Etats-Unis mettent la pression sur l'Europe* », Les Echos, le 12 février 2019, (https://www.lesechos.fr/tech-medias/hightech/huawei-les-etats-unis-mettent-la-pression-sur-leurope-963897), consulté le 20 mai 2019

des équipementiers dans les « sites » mobiles détenus en propre par chaque opérateur en France[6] permet de prendre conscience de sa dépendance à la firme chinoise (annexe 1).

La décision d'exclure Huawei du marché porterait un sérieux coup à la concurrence entre équipementiers. En raison des risques de coupures et des effets catastrophiques qu'ils engendreraient sur les services publics, la population et l'économie, les opérateurs s'attachent généralement à ne pas faire reposer la résilience de leurs réseaux de télécommunication sur un seul équipementier. Cette décision leur permet d'augmenter la probabilité d'être capable de fournir une connexion en cas de défaillance d'un équipementier. En excluant Huawei du marché, seulement 2 groupes contrôleraient donc l'ensemble des parts de marché des différents opérateurs téléphoniques. Cette décision leur aurait permis d'augmenter leurs prix en se passant d'un concurrent des plus encombrants : Huawei est en effet l'équipementier le plus avancé sur les problématiques touchant à la 5G, mais aussi le moins cher. De plus, Nokia et Ericsson auraient-ils été capables de fournir assez d'antennes dans des délais raisonnables pour compenser la mise à l'écart du marché de Huawei ? Rien n'est moins sûr.

Le Gouvernement n'avait donc pas le choix compte tenu des nombreuses attentes qu'il fonde quant à l'arrivée de cette technologie sur le territoire ; contraint de laisser au géant chinois l'accès à ses réseaux, il a toutefois retenu la possibilité de durcir le cadre juridique encadrant ce secteur si sensible. La France est consciente des promesses d'avenir que porte la 5G – nouveaux usages, innovations permises et retombées économiques – elle ne peut donc risquer d'être dépassée dans la course à cette révolution numérique. Alors que les enchères pour attribuer les fréquences disponibles pour la 5G ont abouti en Finlande, en Italie ou encore en Allemagne, certains pays ont d'ores et déjà proposé des offres commerciales 5G, à l'image de la Corée du Sud, des Etats-Unis ou même du Lesotho. Au-delà des considérations économiques, la question de l'accès à la 5G pose des enjeux de souveraineté nationale, ce qui accroît inévitablement l'importance que le Gouvernement français attache au déploiement rapide de cette technologie.

[6] Rapport n°579 de Mme Catherine PROCACCIA, fait au nom de la commission des affaires économiques, déposé le 19 juin 2019, (*voir annexe 1*)

Dès lors, il conviendra d'observer dans quelles mesures la prise en compte des arguments relatifs aux caractéristiques inhérentes au déploiement de la 5G avancés par les différentes parties prenantes de cette technologie ont conduit à modifier le cadre juridique relatif à l'exploitation des réseaux radioélectriques mobiles français.

Afin de tenter d'embrasser tous les aspects que renferme ce sujet, il semble primordial de constater, dans un premier temps, que la 5G est annoncée comme le principal levier de transformation numérique pour la France en raison des potentialités économiques qu'elle permettrait, faisant de cette technologie une impérieuse priorité pour le Gouvernement et les industriels. Il sera néanmoins nécessaire de contrebalancer le poids de ces promesses d'innovations technologiques par la portée des recommandations adressées à l'Etat, qui ont conduit à une prise en compte plus rigoureuse des potentiels risques et vulnérabilités résultant du déploiement de la 5G sur le territoire (I). Dans un second temps, il sera alors plus aisé d'analyser les différents dispositifs juridiques encadrant le déploiement des équipements de télécommunication, en tentant d'identifier les motifs à l'origine du nouveau régime d'autorisations destiné à permettre à la France d'ouvrir plus sereinement son territoire à la 5G (II).

I) La 5G, un levier de transformation numérique également vecteur de potentiels risques et vulnérabilités pour la France

Toute nouvelle technologie s'accompagne de son lot de promesses. Chaque jour des articles de presse relatifs aux nouveaux usages qui seront permis par la 5G sont mis en ligne. Si certains semblent tout droit sortis d'une œuvre de science-fiction, les scientifiques et les industriels s'accordent pour avancer que cette technologie permettra de réaliser des prouesses encore inatteignables à l'heure de la 4G. Alors que personne n'avait prédit l'avènement des applications mobiles il y a encore une quinzaine d'années, elles sont aujourd'hui un réel moteur d'innovation et font partie intégrante de notre quotidien. Plus encore, l'ère des applications mobiles a contribué à créer un volume de richesses incalculable et a permis l'émergence de services qui rapportent aujourd'hui des milliards à certaines sociétés (Snapchat, Airbnb, WhatsApp, Uber…). Conscient du potentiel économique que revêt la 5G pour de nombreux secteurs d'activités, ainsi que des solutions qu'elle propose pour demain, le Gouvernement français se doit de favoriser son déploiement sur le territoire (A). Toutefois, ces innovations technologiques impliqueront de prendre en compte leur corolaire : les risques inédits qui menacent la résilience des réseaux. Tendre vers une société de plus en plus interconnectée conduit à s'exposer davantage aux actes d'espionnage ou aux tentatives de déstabilisation provenant de puissances étrangères. Au-delà de ces menaces, la dépendance de la Nation aux systèmes d'information et de communication implique de garantir la permanence des réseaux afin d'éviter la survenance d'une rupture généralisée qui engendrerait inévitablement des effets catastrophiques pour l'Etat (B).

A) L'éclosion de nouveaux écosystèmes économiques et numériques favorisée par la 5G

Les opérateurs télécoms n'ont pas eu à réaliser de vastes campagnes d'influence afin de mettre en avant les avancées que permettront les caractéristiques propres à la 5G, tant elles sont attendues par les industriels et les décideurs publics, qui en assurent eux-mêmes la promotion. C'est ainsi que l'entreprise américaine ISH Markit, spécialisée dans la réalisation d'analyses relatives à l'intelligence économique, annonçait par exemple que « *l'adoption de la technologie mobile 5G pourrait générer 12,4 mille milliards de dollars de production économique mondiale d'ici 2035* », un montant équivalant à la somme des PIB du Japon, de l'Allemagne et de l'Inde en 2018. Sans prétendre que ce montant soit exagéré, le fait que cette étude ait été commandée par Qualcomm[7], une entreprise américaine spécialisée dans la conception et la mise en place de solutions de télécommunications, impose de nuancer quelque peu ce résultat.

Dans une toute autre mesure, il est possible d'évoquer le plan pour l'égal accès aux soins dans les territoires, présenté par Edouard Philippe, Premier ministre, et Agnès Buzyn, ministre des Solidarités et de la Santé, le 13 octobre 2017[8]. Parmi les 4 axes développés par le Gouvernement afin que « *chaque territoire dispose d'un projet de santé adapté et sur-mesure* », il en est un qui dépend inexorablement du déploiement de la 5G : « *la mise en œuvre de la révolution numérique en santé pour abolir les distances* ». La prise en charge de patients à distance permettrait effectivement, pour certains cas, de réduire les contraintes liées à l'offre de soins lacunaire des zones sous-denses en France. Ce projet laisse imaginer toute l'attente que le Gouvernement a placée dans l'arrivée de la 5G sur le territoire.

Il est aisé de comprendre pourquoi la cinquième génération de standards de télécommunications mobiles est attendue depuis de si nombreuses années. Une multitude d'usages diversifiés seraient en effet permis par cette technologie de rupture, qui souffrirait d'un problème d'appellation d'après Thierry BOISNON, président de Nokia France. A l'occasion de l'édition 2018 du « Telco & Digital Forum », une conférence organisée par Les Echos, ce-dernier déclarait en effet : « la 5G a un problème de nom et n'est pas une simple

---

[7] P. HART : « *5G : The twelve trillion dollar technology »,* ISH Markit, le 3 mai 2017, (https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf), consulté le 18 mai 2019

[8] Ministère des Solidarités et de la Santé : « *Présentation du plan pour l'égal accès aux soins dans les territoires* », le 13 octobre 2017

évolution de la 4G. C'est avant tout un enjeu de révolution industrielle ».[9] Bien que ce type de déclaration contribue à favoriser ses activités, Thierry BOISNON n'est pas le seul à avoir placé autant d'attente autour des révolutions que permettra la 5G. Il en est ainsi d'Agnès PANNIER-RUNACHER, Secrétaire d'Etat auprès du Ministre de l'Economie et des finances, qui estimait par exemple que « déployer rapidement la 5G est une priorité, pour lutter contre la fracture territoriale et pour développer les usages de demain »[10] lors d'une audition devant la Commission des Affaires économiques du Sénat en juin 2019. Concrètement, la 5G accroit sensiblement 3 paramètres sur lesquels repose la connexion mobile : le débit, la latence et la densité.

Le débit est la caractéristique la plus connue, car le lien entre « débit plus puissant » et « usage plus rapide » est souvent avancé par les professionnels. Il se mesure par le nombre de données numériques transmises en une seconde, ainsi, plus le débit est élevé, plus l'utilisateur pourra profiter de services rapidement et aisément. En promettant des débits entre 10 et 100 fois supérieurs à ceux de la 4G[11], la 5G pourrait permettre des téléchargements beaucoup plus rapides, tels qu'il est encore difficile de les imaginer. En 2014, déjà, le Premier Ministre britannique de l'époque, David Cameron, se rendait au salon CeBIT (Centrum für Büroautomation, Informationstechnologie und Telekommunikation, en français : « Salon des Technologies de l'Information et de la Bureautique »), le plus grand salon pour les technologies de l'information du monde, pour échanger autour des potentialités qu'offrirait la 5G. Il annonçait entre autre « *qu'avec la 4G, un film de 800 méga-octets prend environ 40 secondes à télécharger : avec la 5G ce serait réduit à une seule seconde. C'est un trésor que tous les chercheurs du monde vont rechercher* »[12].

Aujourd'hui les attentes se concrétisent ; le journaliste Andy BOXALL, spécialisé dans l'actualité des technologies digitales et innovantes, a par exemple réalisé des tests de connexion 5G à Monaco en juillet 2019, relate le site d'information Digital Trends. Monaco est en effet

---

[9] S. DUMOULIN : « *Le monde fabuleux de la 5G* », *Les Echos*, le 05 mai 2019 (https://weekend.lesechos.fr/business-story/innovation/0600742311487-le-monde-fabuleux-de-la-5g-2247013.php), consulté le 20 mai 2019

[10] Audition d'Agnès Pannier-Runacher, Secrétaire d'Etat au numérique auprès du ministre de l'économie et des finances, par la commission des affaires économiques du Sénat sur la proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques, le 4 juin 2019

[11] Plaquette de présentation de l'Agence nationale des fréquences : « Préparer l'arrivée de la 5G », le 18 décembre 2018

[12] Extrait du discours prononcé par David Cameron, ancien Premier Ministre du Royaume-Uni, à la tribune du Centrum für Büroautomation, Informationstechnologie und Telekommunikation (CeBIT), le 9 mars 2014, à Hanovre

l'un des premiers pays du globe à avoir été complètement couvert en 5G, ce qui rend les expérimentations sur son territoire très intéressantes puisque réalisées en conditions réelles. Les résultats de ce test sont sans équivoque, avec un débit de plus d'1 Gigabit par seconde, il est possible de télécharger une série entière en moins de 40 secondes, de regarder des vidéos retransmises en direct en haute définition, et d'envoyer des fichiers de plusieurs méga-octets en quelques dixièmes de secondes[13].

Les deux autres paramètres vont jouer un rôle prépondérant dans l'avènement de l'Internet des objets, aussi appelé IoT (Internet of Things). Il s'agit de la latence et de la densité de connexion. La latence constitue le délai qu'un ensemble de données met pour transiter de sa source à la destination, à travers le réseau. Cette caractéristique est cruciale pour permettre de meilleures interactions entre les outils numériques. La 5G promet ici de diviser ce temps de latence par 10 par rapport aux précédents standards de communication. Ainsi, un ensemble conséquent de données pourrait être transmis en quelques millisecondes, soit quasiment instantanément. Cette évolution rendra possible le développement de technologies sensibles qui semblaient encore hors de portée il y a peu, à l'image de la téléchirurgie ou des véhicules connectés et autonomes, des projets qui nécessitent un temps de réaction extrêmement rapide. Ces secteurs d'innovation impliquent, pour la plupart, une connexion entre les objets afin qu'ils s'échangent des données et communiquent entre eux pratiquement en temps réel : la voiture connectée du futur (proche) sera, par exemple, en liaison avec les autres véhicules, les feux de signalisation, les stations météorologiques, les smartphones des piétons…

Tendre vers l'ère de l'Internet des objets suppose donc assez logiquement que les réseaux parviennent à prendre en charge un nombre plus important, voire exorbitant, de connexions. C'est sur ce point que les progrès de la 5G vont réellement conduire à une rupture dans le quotidien de chacun. En effet, d'après l'Agence Nationale des Fréquences, les nouvelles performances en termes de densité de connexion permettront ainsi de multiplier par 10 le nombre d'objets connectés simultanément au réseau. Dans une étude réalisée en 2015[14], le Swiss Federal Institute of Technology de Zurich (Ecole Polytechnique Fédérale de Zurich) déclarait ceci : « *Les réfrigérateurs, les machines à café, les brosses à dents, les téléphones et les appareils intelligents seront équipés de capteurs communicants. Dans dix ans, 150 milliards*

[13] A. BOXALL : « *How the Monaco Grand Prix inspired the country to win the 5G race* », Digital Trends, le 27 juillet 2019, (https://www.digitaltrends.com/mobile/5g-in-monaco-with-huawei-interview/) (consulté le 1er août 2019)

[14] E. POURNARAS & D. HELBING « *Society : Build a digital democracy* », 2 novembre 2015, Nature n°527, pages 33-34

de « choses » se connecteront entre elles et avec des milliards de personnes. L'Internet des objets générera des volumes de données qui doubleront toutes les 12 heures au lieu de tous les 12 mois, comme c'est le cas actuellement ».

Un tout autre avantage présenté par les spécialistes de la 5G est celui de pouvoir destiner des tranches de réseau à des usages spécifiques. Actuellement, regarder un film en streaming, participer à une visioconférence et télécharger des morceaux de musique se fait sur le même réseau. Or, la 5G permettra d'attribuer des parts de réseau à certaines activités, ce qui permettra d'avoir la main sur les consommations pour les gérer et les réguler en fonction des besoins et des priorités. Ainsi, Börje Ekholm, Président Directeur Général de l'équipementier Ericsson, expliquait, dans un discours de janvier 2018 au World Economic Forum, que « *si je subis une opération chirurgicale à distance, je n'aimerais pas ne pas avoir la priorité sur un gamin en train de télécharger un film* »[15]. Cette possibilité permettra de s'assurer que certains services jugés prioritaires ne connaîtront pas d'interruption en raison d'un nombre trop important de connexions sur le réseau.

Après s'être brièvement intéressé aux améliorations propres aux caractéristiques fondamentales des réseaux de télécommunications, il convient d'apprécier ce qu'elles permettront d'imaginer et de mettre en place dans un futur proche.

Dans un premier temps, il est nécessaire de rappeler que la 5G n'étant même pas encore déployée dans certains pays, il est difficile de détailler, de manière exhaustive, l'ensemble des usages qu'elle rendra possible. Toutefois, de profondes innovations sont particulièrement attendues dans certains secteurs : les « smart cities », ou villes intelligentes, les automobiles autonomes, l'e-santé, les divertissements, l'agriculture...

Pour le Gouvernement, l'e-santé et ses potentialités représentent aujourd'hui une solution aux problématiques des offres de soins lacunaires dans certaines zones géographiques du territoire, encore appelées désert médicaux. Ainsi, lorsque Monica MICHEL, députée des Bouches-du-Rhône, attire l'attention de Jacqueline GOURAULT, ministre de l'Aménagement du territoire, sur le fait que « *la lutte contre la désertification médicale est une préoccupation majeure des français* » et qu' « *il y a urgence à assurer une égalité d'accès aux soins quel que soit le lieu de résidence* », la ministre est contrainte de lui répondre qu'*« il n'y a plus de démographie médicale suffisante pour imaginer que l'on puisse déplacer ou encourager des*

[15] Extrait du discours de Börje Ekholm au World Economic Forum : « *How 5G could speed up global growth ?* », le 12 janvier 2018, à Davos

médecins à aller dans une zone à une autre, il n'y a plus de zone sur-dense en France »[16]. Quelques dizaines de minutes auparavant, Jacqueline GOURAULT, interrogée sur le même sujet, expliquait néanmoins que le maillage des territoires ruraux en Haut et Très Haut Débit devrait permettre une prise en charge à distance des patients, grâce aux technologies de l'information et de la communication. Même s'il est évident que les territoires ruraux ne seront pas couverts immédiatement en 5G, et qu'il faudra encore plusieurs années pour y assister, les caractéristiques de ce nouveau standard de télécommunications auront pour effet de rendre plus pratique le suivi des patients qui ne peuvent pas se déplacer.

Au-delà de la téléconsultation, les praticiens tentent, depuis plusieurs années, de faire de la chirurgie à distance une réalité. Bien que des premières expériences se soient révélées fructueuses grâce aux capacités de connexion offertes par la fibre optique, le fait de parvenir à s'affranchir d'un réseau câblé constituait l'objectif ultime en raison des coûts et des limites que cela entraine (pour des opérations chirurgicales réalisées en zone de guerre, par exemple, il est préférable que les manipulations dépendent d'ondes radio plutôt que d'un câble, d'autant plus lorsque le terrain est accidenté, ce qui est généralement le cas). Cette prouesse a été accomplie le 10 janvier 2019, à l'hôpital de Fuzhou, en Chine. D'après le site d'information chinois Technology-Info, un chirurgien est parvenu à opérer un porc qui se trouvait à 50 km de l'hôpital, au moyen d'une simple connexion 5G[17]. Deux mois plus tard, le China Daily se faisait l'écho d'une intervention chirurgicale réalisée sur un patient atteint de la maladie de Parkinson qui se trouvait à 3000 kilomètres de distance[18], tout en précisant que celle-ci avait été couronnée de succès. Ces deux annonces ont été reprises par la presse internationale, qui en a avéré les faits. Toutefois, ces deux articles, provenant de la presse chinoise, ont en commun la mise en avant d'un élément présenté comme essentiel à la réalisation de ces deux opérations : le recours à des équipements Huawei. Bien que la véracité de ces informations ait été établie, leur relai massif par des médias pro-Chine s'inscrit néanmoins dans un contexte particulier pour l'équipementier ; la justice américaine venait d'ouvrir une enquête criminelle à son encontre pour vol de secrets industriels[19].

---

[16] Questions relatives à la politique du Gouvernement sur le maintien des services publics sur le territoire, le 29 avril 2019, à l'Assemblée nationale

[17] O. SHAOXIA : « *5G network remote animal surgery succesfully implemented in Fuzhou* », Technology-Info, le 10 janvier 2019, (https://technology-info.net/index.php/2019/01/10/5g-network-remote-animal-surgery-successfully-implemented-in-fuzhou/) (consulté le 6 mai 2019)

[18] S.N. « *China performs first 5G-based remote surgery on human brain* », Chinay Daily, le 18 mars 2019, (http://www.chinadaily.com.cn/a/201903/18/WS5c8f0528a3106c65c34ef2b6.html) (consulté le 6 mai 2019)

[19] D. STRUMPF & AL. « *Huawei Targeted in U.S. Criminal Probe for Alleged Theft of Trade Secrets* », The Wall Street Journal, le 16 janvier 2019

Mais les promesses qui entourent l'e-santé ne sont pas les seules à attirer l'attention des gouvernements. Le 18 juillet 2019, les sénateurs de la commission d'enquête sur la souveraineté numérique de la France découvraient le projet « 5GRuralFirst » lors de l'audition des dirigeants de Cisco France, la branche nationale de l'entreprise américaine spécialisée dans les réseaux informatiques. En 2019, la France reste un pays comprenant d'importantes zones rurales, tandis que le nombre d'agriculteurs ne cesse de baisser depuis des années[20], et que la balance commerciale de la France n'est plus aussi excédentaire qu'avant dans ce domaine. Le secteur agricole traverse en effet des crises à répétition, qui conduisent les petits chefs d'exploitations à revendre aux plus importants, qui voient eux-aussi leur marge fondre du fait de la concurrence qu'a apportée la mondialisation. Un rapport d'information[21] réalisé par les députés Alexandre FRESCHI et André CHASSAIGNE, en date du 31 mai 2018 indique ainsi que « *ce sont les subventions d'exploitation qui permettent d'éviter à un quart d'exploitants d'avoir des résultats négatifs* », des subventions qui représenteraient en effet près de 12% de leurs ressources. Il évoque également que l'Union européenne compte 14 millions d'exploitations agricoles et que le secteur représente un total de 44 millions de salariés. Alors que le si décrié Comprehensive Economic and Trade Agreement (CETA) a été adopté par l'Assemblée nationale le 23 juillet 2019[22], présageant d'un contexte encore plus concurrentiel pour le domaine agroalimentaire en France et en Europe, les pouvoirs publics ne peuvent se permettre de passer à côté des potentialités que renferme la 5G pour le secteur.

5GRuralFirst fait notamment parti de ces programmes plein de promesses pour les territoires et les secteurs oubliés par le numérique. Il s'agit d'un projet d'innovation dirigé principalement par Cisco, l'Université de Strathclyde, puis rejoint par de nombreux partenaires tels que des élus, des universitaires et des industriels. Le premier but de cette mission est de découvrir et établir des procédés permettant de connecter des zones rurales à la 5G, afin d'améliorer certaines activités et de développer de nouveaux modèles commerciaux. Au-delà de cet objectif, les membres du projet, qui est financé en partie par le ministère britannique du numérique, de la culture, des médias et du sport, entendent attirer l'attention des pouvoirs publics sur les potentiels de la 5G pour ces zones reculées, tout en incitant les communautés rurales à mettre au point des techniques et des méthodes afin que la connexion sans fil facilite

[20] Institut national de la statistique et des études économiques, présentation du tableau de l'économie française, janvier 2019

[21] Rapport d'information n°1017 (2018-2019) de MM Alexandre FRESCHI et André CHASSAIGNE, fait au nom de la commission des affaires européennes, déposé le 31 mai 2018

[22] M. RASCAN : « *Le CETA, controversé accord de libre-échange avec le Canada, approuvé à l'Assemblée* », Le Monde, le 23 juillet 2019

leur quotidien et l'émergence de nouvelles activités. Parmi les nombreux programmes sur lesquels se concentre le projet, les solutions tournées vers l'« Agritech » suscitent aujourd'hui un certain intérêt de la part du Gouvernement français, preuve en est des différentes questions posées par les sénateurs sur le sujet lors de l'audition du 18 juillet 2019. Au sein de fermes d'essais situés à l'ouest du Royaume-Uni, les équipes de 5GRuralFirst sont ainsi parvenues à mettre au point un applicatif permettant à un drone autonome d'être connecté à un tracteur et des capteurs situés dans le champ. Cette innovation permet au drone de recevoir les signaux envoyés par les capteurs et de cibler certaines zones de l'exploitation en fonction des données sur lesquelles l'agriculteur lui demande de se concentrer. Si le drone perçoit des informations qui ne correspondent pas aux standards, il pourra alors diriger l'agriculteur vers les capteurs concernés et lui offrir des plans d'images en haute définition. Les chercheurs ne se sont pas arrêtés à cette innovation puisqu'ils sont actuellement en train d'œuvrer pour permettre au drone de contrôler le tracteur, afin que celui-ci puisse obtenir les données des sols grâce aux capteurs et qu'il pilote le tracteur de manière autonome jusqu'à la zone déterminée pour y pulvériser, seul, les engrais. Enfin, dans un futur proche, les agriculteurs pourraient se passer de ces étapes ; une start-up britannique qui a rejoint le projet tente de savoir si la 5G pourrait « *permettre l'identification et la classification en temps réel des conditions du sol à partir d'un avion volant à 900 mètres, afin d'apporter une réponse plus rapide et en temps réel aux variations des sols, aux pâturages du bétail et à la propagation de maladie* ». Néanmoins, la mise au point de ces pratiques implique forcément d'avoir recours à la 5G, en raison de ses capacités en termes de connexions simultanées, de faible latence, d'images haute définition et de vitesse de connexion.

L'Agritech est donc la réunion du numérique (digital, intelligence artificielle, objets connectés) et de l'agriculture. Il s'agit d'un marché à très fort potentiel sur lequel les jeunes agriculteurs se ruent depuis quelques années, tant du fait des défis qu'il propose que des prouesses qu'il rendrait possible. Le 23 mai 2019, l'Agritech était même le sujet central du sommet de l'innovation et des start-up, qui se déroulait à Caen[23]. Universitaires, décideurs publics et industriels ont ainsi échangé autour des progrès déjà réalisés et des potentialités qu'il renferme encore. C'est ainsi que Rémi LAURENT, Directeur de l'innovation auprès de la Chambre d'Agriculture Régionale de Normandie, était fier de présenter l'application Pilot'élevage proposée par sa structure, qui permet « *aux 31 000 agriculteurs, pour 2 millions d'hectares de surface agricole utile* » de « *gérer l'identification, la reproduction, la santé, les*

[23] O. LASCAR : « *AgriTech : le numérique pour révolutionner l'agriculture* », Sciences et Avenir, le 23 mai 2019, (https://www.sciencesetavenir.fr/high-tech/sommet-start-up/agritech-le-numerique-pour-revolutionner-l-agriculture_133905), (consulté le 10 juin 2019)

performances lait et viande » des troupeaux. En effet, les potentialités de la 5G peuvent également améliorer le quotidien des éleveurs. Activité complexe en raison des surfaces sur lesquelles s'étend le bétail, des difficultés à détecter l'apparition d'un symptôme avant sa propagation, ou encore à appréhender certains paramètres comme les conditions météorologiques, qui imposent de réagir en temps réel, les éleveurs fondent eux aussi beaucoup d'attentes sur le déploiement de la 5G dans leurs exploitations, et de nouveaux usages pourraient voir le jour bien assez tôt.

Qu'il s'agisse de la santé ou de l'agroalimentaire, entre bien d'autres secteurs, l'optimisation que promet la 5G en matière de procédés, voire la création même de nouveaux usages, pourrait répondre à de nombreuses problématiques auxquelles les pouvoirs publics sont confrontés depuis plusieurs années en France. Apporter une réponse aux défis des déserts médicaux ou à la baisse considérable du niveau de vie des agriculteurs et des éleveurs représenterait une victoire politique majeure, d'autant plus pour le Gouvernement actuel, accusé de se déconnecter des problématiques locales et d'accroître la fracture entre Paris et la province. Le déploiement rapide de la 5G revêt donc un enjeu primordial pour les décideurs publics, qui se doivent aujourd'hui de renouer avec un électorat qui n'hésite plus à manifester son désarroi à travers des crises inédites à la fois par leur ampleur mais aussi pour les revendications qu'elles portent. Par conséquent, le Gouvernement n'a pas intérêt à voir le déploiement de la 5G prendre du retard, il l'a d'ailleurs bien compris puisque les opérateurs de télécommunications n'ont pas eu à évoquer ce point lors des discussions autour de la loi 5G du 2 août 2019.

Une autre partie prenante a également largement pesé lors des débats autour de l'encadrement du déploiement de la 5G et des conséquences qui pourraient en découler : les industriels. Avec les billions de dollars de potentiel économique que pourrait développer cette technologie, les grandes entreprises comptent sur sa mise à disposition dans les meilleurs délais pour accroître leurs activités, créer de nouvelles expériences voire même participer à l'éclosion de nouveaux écosystèmes. Comme il a été rappelé précédemment, personne n'avait imaginé que la 4G révolutionnerait des pans entiers de l'économie en permettant l'émergence des applications, ce qui explique également pourquoi la 5G est attendue de pied ferme par le secteur industriel, où chacun souhaite être le premier à proposer le service du futur. Parmi toutes les expérimentations déjà lancées, il a été choisi d'en étudier principalement deux pour leur probable impact sur la société de demain : les véhicules autonomes et l'essor de l'industrie intelligente.

Le 17 juin 2019 un centre d'expérimentation unique en Europe était inauguré au cœur du site de l'autodrome de Linas-Montlhéry, dans l'Essonne, par le groupe français UTAC CERAM : le projet TEQMO. D'un coût de 20 millions d'euros, ce programme est destiné aux industriels intéressés par « *les technologies d'automatisation et de connectivité de la conduite* »[24] comme l'a rappelé le président du groupe, Laurent BENOIT. D'un point de vue technique, cette infrastructure propose de placer les véhicules en situation réelle afin de réaliser des essais et d'optimiser leurs compétences. D'après le site internet dédié au projet, l'autonomisation des automobiles pourra ainsi être testée sur des segments d'autoroute, des circuits intégrant les problématiques des aires urbaines, des voies à double sens ou encore des zones de parking. Pour assurer la connectivité de ces moyens de transport du futur, le centre d'expérimentation est équipé par les dernières technologies (5G et Wifi 6), qui devraient conduire à une meilleure appréhension des défis du secteur.

Outre l'offre d'essais techniques, Teqmo met à disposition des constructeurs des équipes d'ingénieurs chargées de perfectionner les communications entre le véhicule et les capteurs qui l'entourent. Plus encore, les objectifs de ces spécialistes des véhicules autonomes s'inscrivent dans la continuité des missions de l'UTAC-CERAM, entité notamment chargée d'homologuer les nouveaux véhicules, puisqu'ils œuvreront afin de mettre aux normes les automobiles connectées afin qu'elles puissent être certifiées et commercialisées. Ce projet français devrait attirer les constructeurs européens ainsi que les plus importants à l'échelle internationale, tous soucieux de pouvoir développer des véhicules qui appréhenderaient les règlementations qui accompagneront leur mise sur le marché. BFM TV rapporte que Bruno le Maire aurait félicité cette initiative en invitant les partenaires de ce projet à poursuivre son développement pour « *rester au premier rang de l'industrie automobile mondiale* », des propos qui s'inscrivent dans la ligne fixée par Emmanuel Macron lors du lancement de la mission sur les nouvelles mobilités et les véhicules électriques et autonomes, le 3 octobre 2018.

C'est à Anne-Marie IDRAC, nommée Haute responsable pour la stratégie nationale du développement des véhicules autonomes, qu'était revenu, dès mars 2018, le soin de préciser la feuille de route à suivre pour parvenir à répondre aux défis de la mobilité du futur. L'un des objectifs qu'elle a défini dans son rapport, « *le soutien public à l'innovation et à*

[24] P. DESAVIE : « *Unique en Europe, le centre Teqmo relève le défi du véhicule autonome et connecté* », L'usine nouvelle, le 17 juin 2019, (https://www.usinenouvelle.com/editorial/unique-en-europe-le-centre-teqmo-releve-le-defi-du-vehicule-autonome-et-connecte.N855895), (consulté le 20 juillet 2019)

l'expérimentation »[25], implique nécessairement de favoriser le déploiement de la 5G, puisque sans cette technologie et la latence qu'elle permet il sera impossible de s'assurer que les véhicules autonomes ne représentent pas de menace pour les utilisateurs et les piétons.

Dès lors, il semblerait légèrement contre-productif d'inviter les industriels à poursuivre leurs efforts pour faire de la France le premier pays dans le domaine des automobiles connectées et finalement entraver le déploiement de la 5G sur le territoire, paramètre pourtant essentiel au processus d'autonomisation de ces véhicules. Comme le rappelle Anne-Marie IDRAC dans son rapport « *Développement des véhicules autonomes : Orientations stratégiques pour l'action publique* » : « *Le développement de l'infrastructure numérique et la connectivité des réseaux routiers peut constituer un facteur d'accélération du développement du véhicule autonome. L'évolution des technologies, notamment l'arrivée de la 5G, conduit à privilégier une approche incrémentale, fondée sur les technologies les plus matures et les réseaux les plus pertinents pour justifier des investissements en connectivité dans les territoires* »[26].

Compte tenu des enjeux économiques que représente ce secteur, nul doute que les décideurs publics ont pris en compte la nécessité de soutenir et d'encourager l'émergence de la 5G pour permettre à la France de peser dans le domaine des véhicules connectés. C'est d'ailleurs ce qui ressort de la feuille de route sur la 5G présentée par l'Arcep deux mois après la publication du rapport d'Anne-Marie IDRAC, faisant de 2025 la date butoir en termes de couverture 5G des axes de transport sur le territoire[27].

Une autre innovation permise par la 5G pourrait intervenir en amont de la commercialisation de ces nouveaux véhicules : celle de la construction. En effet, si le secteur manufacturier connaît de profondes mutations du fait de sa numérisation, la 5G pourrait marquer un réel tournant en la matière. La latence que propose la 5G, ses capacités en termes de connexions simultanées et la possibilité d'attribuer des parts de réseau à certaines activités pourraient constituer le véritable enjeu de la 5G si l'on en croit les opérateurs. En effet, les caractéristiques de la 5G permettraient d'en finir avec la pénibilité de certains emplois, d'élaborer des robots dotés d'un temps de réaction de l'ordre de la milliseconde et qui seraient capables d'interagir entre eux en temps réel, sans intervention humaine. Cela représenterait des gains de temps, d'efficacité et de productivité tels que l'ensemble du secteur en serait

[25] Anne-Marie IDRAC : « *Développement des véhicules autonomes : Orientations stratégiques pour l'action publique* » rapport commandé par le Gouvernement français, le 14 mai 2018
[26] Ibidem
[27] Arcep, *(op. cit.)*

transformé. Aujourd'hui certains groupes ont d'ores et déjà commencé des expérimentations afin de faire de la 5G le principal levier pour réguler et gérer leurs activités. C'est par exemple le cas de la raffinerie Shell Pernis, située sur le port de Rotterdam, dont les essais fructueux ont été relayés par KPN[28], un opérateur de télécommunications néerlandais. La technologie 5G a par exemple permis à la raffinerie de se doter de robots capables de déceler les fuites et d'intervenir sur les pipelines afin d'en limiter les conséquences, une évolution pratique étant donné que le site compte plus de 150 000 kilomètres de conduits à inspecter. Les capteurs installés de part et d'autres du port permettent également d'analyser, en temps réel, des données relatives à la pression ou à la température des pipelines et permettent de réaliser des opérations de maintenance prédictive par exemple. Dans ces conditions, difficile de ne pas être d'accord avec Sébastien SORIANO, président de l'Arcep, lorsqu'il annonçait « *être en retard sur la 4G, c'est dommage. Sur la 5G, c'est grave, systémique. Toutes les industries perdraient la possibilité de se moderniser* »[29].

C'est ainsi, la maîtrise des potentialités offertes par la 5G fait l'objet d'une attente considérable tant les promesses économiques et technologiques qui les accompagnent sont importantes. Que ce soit pour le Gouvernement ou les acteurs du secteur industriel, les innovations apportées par la 5G représentent des solutions et des innovations à côté desquelles il ne faut pas passer. En favorisant son déploiement sur l'ensemble du territoire, la France pourrait garantir sa souveraineté numérique et ne pas être un simple spectateur de la révolution qui est en train de se jouer dans le monde. La maîtrise des potentialités offertes par cette technologie conditionnera forcément le poids qu'auront les Etats dans l'économie internationale de demain. Au-delà des diverses annonces politiques, le Gouvernement français ne peut donc pas laisser l'Asie et l'Amérique du Nord faire main basse sur la 5G ; cette société, qui tend chaque jour vers davantage d'interconnexion, impose un réel soutien des pouvoirs publics quant au déploiement des réseaux 5G. Néanmoins, différentes recommandations et campagnes d'influence provenant de l'étranger, dans un premier temps, puis à l'échelle nationale ensuite, ont fait état de menaces et de risques qui pourraient accompagner l'arrivée de cette nouvelle technologie. Compte tenu des spécificités et de l'importance attachées aux réseaux et systèmes d'information et de communication, il était nécessaire, d'après le Gouvernement, de s'intéresser à la question.

---

[28] KPN : « *Shell and partners test industrial 5G applications in the port of Rotterdam* », communiqué de presse interne mis en ligne le le 6 novembre 2018, (https://overons.kpn/en/news/2018/kpn-shell-and-partners-test-industrial-5g-applications-in-the-port-of-rotterdam), (consulté le 6 mai 2019)

[29] S. DUMOULIN, (*op. cit.)*

B) La nécessaire prise en compte des enjeux de sécurité inhérents au déploiement de la 5G

Il convient, avant tout, de revenir brièvement sur la notion de cybermenace, telle que le Livre Blanc sur la Défense et la Sécurité nationale de 2008[30] l'a prise en compte pour la première fois.

En 2008, le Livre Blanc identifie les attaques informatiques comme des menaces pour la démocratie car les moyens d'information et de communication, qu'elles souhaitent paralyser ou au moins altérer, sont devenus « *les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner* »[31]. L'Etat s'organise alors pour faire face aux risques ; l'ANSSI est créée par un décret de 7 juillet 2009, elle sera rattachée au SGDSN et remplacera la Direction centrale de la sécurité des systèmes d'information. Cette agence s'est vue attribuer une double-mission : garantir, dans un premier temps, la sécurité des systèmes d'information en proposant les règles à mettre en place pour protéger ces systèmes et s'assurer de leur application. Assurer, dans un second temps, la défense des systèmes d'information en réalisant des veilles, des alertes et des plans de réaction en cas d'attaques informatiques, notamment sur les réseaux de l'Etat et des entités chargées d'activités indispensables ou dangereuses pour la Nation.

Pour ce qui est des principales menaces, le Livre Blanc sur la Défense et la Sécurité nationale de 2013 les identifie très clairement dans son chapitre 3, relatif à l'état du monde et plus particulièrement à l'amplification des menaces et des risques du fait de la mondialisation : « *Les systèmes d'information sont désormais une donnée constitutive de nos sociétés. Au-delà des facilités considérables qu'elle apporte, l'interconnexion des systèmes d'information est une source de vulnérabilités nouvelles. Déjà identifiés dans le précédent Livre blanc, les menaces et les risques induits par l'expansion généralisée du cyberespace ont été confirmés, qu'il s'agisse d'atteintes à des systèmes résultant d'actes intentionnels ou de ruptures accidentelles mettant en cause le fonctionnement d'une infrastructure numérique critique* »[32]. En d'autres termes, les menaces pesant sur les systèmes d'information et de communication français, et relevant par conséquent de la sécurité nationale, sont de deux ordres : premièrement, les attaques ou infiltrations dans les réseaux numériques à des fins d'espionnage ou dans le but de

[30] J.C Mallet : « *Défense et sécurité nationale. Le livre blanc* », Paris, O. Jacob/Éd. La documentation française (livre blanc de 2008)
[31] Ibidem
[32] Ministère de la défense, le Livre Blanc sur la Défense et la sécurité nationale, 29 avril 2013

porter atteinte à la souveraineté nationale, qu'elles proviennent d'acteurs étatiques ou non et qu'elles visent les systèmes de l'Etat ou ceux des entreprises françaises. Deuxièmement, il peut s'agir de ruptures accidentelles ou intentionnelles de ces systèmes, qui pourront entraîner une paralysie de la société et/ou une perte de contrôle sur des réseaux critiques qui garantissent le fonctionnement d'opérateurs d'importance vitale ou d'infrastructures stratégiques.

Voici l'éventail de risques et de vulnérabilités que se doit d'appréhender l'ANSSI afin d'assurer la permanence des systèmes d'information et de communication français. Les 1 869 signalements enregistrés par ses services en 2018[33] démontrent l'ampleur de sa mission.

Le déploiement de la 5G s'intègre inéluctablement dans la sphère de compétence de l'ANSSI, qui doit analyser et prévenir les éventuelles menaces que cette nouvelle génération pourrait entraîner. Toutefois, la question de l'existence de risques inédits a conduit les opérateurs télécoms et les acteurs intéressés par les problématiques de sécurité nationale à débattre durant plusieurs mois, pour finalement déboucher sur la promulgation de la 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 le 2 août 2019.

Malgré les stratégies de communication et les nombreux arguments déployés par les industriels, auxquels, il a été vu, certains ministères étaient plus que sensibles, la France a opté pour le renforcement du cadre juridique existant, quitte à altérer le rythme des déploiements et à prendre du retard quant à la couverture du territoire en 5G. Il semble donc particulièrement intéressant d'apprécier à la fois les arguments développés par les opérateurs mais aussi, et surtout, les travaux produits par les différents acteurs du domaine de la sécurité qui ont influencé l'opinion et une prise de décision en faveur de l'adoption de cette loi.

Dans un premier temps, la pression est venue de l'étranger, et plus précisément des Etats-Unis. Ainsi, dès février 2018 la chaîne de télévision américaine CNBC annonce que six responsables du renseignement américain mettent en garde contre l'achat de téléphone Huawei[34], qu'ils accusent d'espionnage. A ce moment, la nouvelle semble simplement découler de la rivalité commerciale entre les Etats-Unis (Apple) et la Chine (Huawei). Néanmoins, la Federal Communications Court (« Commission Fédérale des Communications ») prend la

[33] Agence nationale de la sécurité des systèmes d'information, rapport annuel d'activité pour l'année 2018, publié le 15 avril 2019

[34] S. SALINABAS : « *Six top US intelligence chiefs caution against buying Huawei phones* », CNBC, le 13 février 2018, (https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html), (consulté le 10 mai 2019)

décision de bloquer les ventes d'équipements Huawei aux opérateurs américains deux mois plus tard[35]. Pour motiver cette décision, l'institution se fonde sur le parcours de Ren ZHENGFEI, passé d'ancien ingénieur de l'armée chinoise à président-directeur général de Huawei, et ses liens avec le parti communiste chinois. Elle évoque également la Loi sur le renseignement national, que l'Empire du milieu a promulgué en juin 2017, et plus particulièrement son article 7 qui oblige tout individu et organisation à soutenir et aider les services de l'Etat afin de participer aux missions de renseignement national. C'est donc cette obligation de coopération pesant sur les entreprises chinoises qui va conduire les Etats-Unis à réagir pour protéger ses systèmes d'information et de télécommunication.

Il convient toutefois de rappeler que les Etats-Unis font clairement figure d'experts en la matière. En effet, la communauté internationale a encore en mémoire les déclarations d'Edward SNOWDEN, qui révélait, en 2013, les pratiques d'espionnage mises au point par les services de renseignement américains. Ces-derniers utilisaient notamment des failles dans les logiciels de mastodontes du numérique (Google, Facebook, Microsoft…) afin d'accéder à leurs serveurs pour y dérober les informations qui les intéressaient. Plus grave encore, le 22 juin 2013, le lanceur d'alerte déclare, au cours d'un entretien accordé au South China Morning Post, que ces mêmes agences étaient parvenues à infiltrer des routeurs Internet chinois, leur donnant accès aux données de « *centaines de milliers d'ordinateurs sans avoir besoin d'en pirater un seul* »[36]. Une semaine plus tard, le quotidien allemand Der Spiegel annonçait qu'une part sensible des données de communications issues des réseaux téléphoniques français était captée régulièrement par la NSA (un peu plus de 6 millions de données par jour en janvier 2013)[37]. L'affaire n'étonne personne mais éclate au grand jour : à l'instar des américains, il est possible d'avoir recours à certains équipements nécessaires au fonctionnement des systèmes d'information et de communication pour espionner ses ennemis, mais également ses alliés.

En août 2018, l'Australie décide d'exclure Huawei du processus de déploiement de la 5G sur son territoire[38], en raison des risques pour sa souveraineté qui pourraient découler du

---

[35] P-Y. DUGUA : « *Les Etats-Unis ferment le marché des télécoms aux chinois* », Le Figaro, le 18 avril 2018

[36] L. LAM et S. CHEN : « *Snowden reveals more US cyberspying details* », South China Morning Post, le 22 juin 2013, (https://www.scmp.com/news/hong-kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed), (consulté le 10 avril 2019)

[37] L. POITRAS et AL. : « *How the NSA targets Germany and Europe* », Der Spiegel, le 1er juillet 2013, (https://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html), (consulté le 10 avril 2019)

[38] S.N. : « *Huawei and ZTE handed 5G network ban in Australia* », BBC News, le 23 août 2018, (https://www.bbc.com/news/technology-45281495), (consulté le 1er mai 2019)

respect de la Loi sur le renseignement national par l'entreprise chinoise. La mesure est très vite reprise par le Japon et la Nouvelle-Zélande, qui craignent également d'être surveillés.

La campagne menée par les Etats-Unis commence alors à faire peser un sérieux risque sur les activités de Huawei, qui décide de réagir. C'est tout d'abord le Gouvernement chinois qui va s'exprimer, par l'intermédiaire de Shuang GENG, porte-parole du ministère des Affaires étrangères, afin de balayer les craintes fondées sur l'obligation de coopération entre les entreprises chinoises et les services de renseignement : « *l'article 8* [de la Loi sur le renseignement national] *indique clairement que les services de renseignement du pays doivent mener leur travail conformément à la loi, respecter et protéger les droits de l'homme et sauvegarder les droits et intérêts légitimes des particuliers et organisations. Je me demande si les personnes proférant des accusations concernant cette loi ont correctement lu ses articles. J'espère qu'ils la liront de manière complète et la comprendront avec précision, au lieu de faire des interprétations partiales et hors contexte* »[39]. D'autres arguments sont aussi utilisés, comme lors de l'audition des dirigeants de la branche française de Huawei par la commission d'enquête sénatoriale sur la souveraineté numérique, le 18 juillet 2019, durant laquelle Benjamin HECKER, directeur juridique du groupe, déclare : « *il s'agit d'une loi liée aux impératifs de sécurité nationale, il n'y a donc pas d'effet extraterritorial, comme avec le Cloud Act. Le Premier Ministre chinois l'a rappelé, ainsi que nos cabinets d'avocats le confirment ; le texte ne vise pas les entreprises ou individus situés hors de Chine a collaboré sur des enquêtes ayant lieu en Chine* ».

Il est toutefois trop tard pour que la communauté internationale n'entende et n'adhère aux propos défendus par la Chine. La riposte n'est pas très convaincante et le doute s'est installé, la faisabilité de telles pratiques étant avérée depuis l'affaire Snowden. Chaque pays se demande alors s'il doit laisser l'équipementier chinois, jugé le plus avancé quant à la 5G, s'installer sur son territoire. Il faut agir dans l'urgence, ce que ne vont pas manquer de relever les sénateurs français lorsque le Gouvernement tentera d'imposer un nouveau régime d'autorisation préalable pour les équipements 5G au moyen d'un amendement inséré, en cours de discussion, au sein du projet de loi sur la croissance et la transformation des entreprises en janvier 2019[40]. L'amendement sera rejeté par le Sénat, qui critiquera la méthode : « *C'est un*

[39] G. KE et Y. LIU : « La Chine exhorte à une compréhension complète et correcte de sa loi sur le renseignement », French People Daily, le 20 février 2019, (http://french.peopledaily.com.cn/Chine/n3/2019/0220/c31354-9547791.html), (consulté le 1er mai 2019)

[40] Amendement n°874 du projet de loi sur la croissance et la transformation des entreprises, déposé par le Gouvernement le 25 janvier 2019

vrai gros sujet, on ne peut pas le prendre comme ça au détour d'un fauteuil de Sénat, ce n'est pas possible. Il faut faire les choses sérieusement » plaidera par exemple Sophie Primas, présidente de la commission des Affaires économiques du Sénat[41]. La nécessité de procéder à des expertises sur la question va permettre aux parlementaires de pouvoir saisir l'ensemble des risques que pourrait induire le déploiement de la 5G sur le territoire. Deux inquiétudes vont alors émerger : avoir recours aux équipements de Huawei présente-il un risque ? Et, dans une moindre mesure, quelles sont les vulnérabilités intrinsèques à la technologie 5G ?

Agnès PANNIER-RUNACHER, secrétaire d'Etat au numérique, l'a rappelé : « *tous les équipementiers seront soumis aux mêmes règles ; d'une part car la vulnérabilité ou la faille de sécurité n'est pas le propre d'un équipementier par rapport à un autre, d'autre part car il est impossible de savoir quels actionnariats et quelles stratégies auront les différents équipementiers dans 10 ans* »[42] et Catherine PROCACCIA, sénatrice et rapporteur de la proposition de loi au Sénat, a insisté : « *ce n'est pas une loi "anti Huawei" comme j'ai pu le lire dans de nombreux médias. La loi vise à sécuriser la 5G française contre tout ce qui pourrait compromettre sa sécurité, pas seulement contre Huawei* »[43].

Pourtant, inutile de s'en cacher, la campagne menée par les Etats-Unis fut un succès puisqu'il n'était pas évident qu'un tel dispositif juridique voit le jour, aussi tôt, sans l'intervention des américains. C'est Catherine PROCCACIA qui le reconnaît d'ailleurs : « *c'est évidemment lié à Huawei, sans aucun doute. Les critiques américaines interpellent forcément* »[44], ainsi que Cédric O, également Secrétaire d'Etat au numérique : « *dans le fond, le sujet des investissements de Huawei en France ne pose pas de problème ; Huawei qui vend des téléphones, cela ne nous dérange pas. Dans certains secteurs touchant à la sûreté de la France, cela peut poser plus de problème. Nous sommes très attentifs par rapport à la situation* »[45].

En réagissant aux accusations américaines dirigées contre Huawei avec précipitation et maladresse, la France s'est trahie : c'est bien la menace que représenterait l'entreprise chinoise

---

[41] G. JACQUOT : « *5G : heurté par la méthode, le Sénat rejette « l'amendement anti-Huawei » du Gouvernement* », Public Sénat, le 7 février 2019, (https://www.publicsenat.fr/article/parlementaire/5g-heurte-par-la-methode-le-senat-rejette-l-amendement-anti-huawei-du), (consulté le 12 avril 2019)

[42] Audition d'Agnès Pannier-Runacher, (*op. cit.*)

[43] A. ROBERT : « *Loi 5G : « ce n'est pas une loi anti-Huawei » selon la sénatrice Catherine Procaccia* », CNET, le 29 juillet 2019, (https://www.cnetfrance.fr/news/loi-5g-ce-n-est-pas-une-loi-anti-huawei-selon-la-senatrice-catherine-procaccia-39888471.htm), (consulté le 2 mai 2019)

[44] Ibidem

[45] Audition de Cédric O, Secrétaire d'Etat au numérique auprès du ministre de l'économie, par la commission de la culture, de l'éducation et de la communication du Sénat, le 24 juillet 2019

davantage que les caractéristiques intrinsèques à la technologie 5G qui a conduit à l'adoption de cette loi.

Outre la Loi sur le renseignement national de 2017, qu'il importe simplement d'évoquer désormais, la situation de Huawei comporte effectivement quelques zones d'ombres sur lesquelles il convient de revenir. Premièrement, les liens entre Huawei, et notamment son fondateur Ren ZHENGFEI, et le parti communiste. En juin 2019, l'Express dresse un portrait du magnat chinois des télécoms. On y apprend par exemple qu'entre 1998 et 2000, Huawei voit son chiffre d'affaires plus que doubler (passant de 1,2 milliards à 2,9 milliards d'euros) après avoir été désigné par le Parti pour développer le premier réseau de télécommunications de l'armée chinoise. Fort de ce chantier conséquent, l'entreprise décide alors d'exporter ses équipements. Pour soutenir ces activités à l'international, l'Etat chinois lui octroie un volume d'aides financières astronomique (le chiffre de 40 milliards de dollars est avancé par l'Express). Huawei parviendra à se hisser au rang de deuxième plus grand groupe de télécommunication du monde, derrière Ericsson, 13 ans plus tard. En échange de ces financements, Huawei aurait-il dissimulé des failles dans ses logiciels pour permettre aux services de renseignement chinois d'avoir accès aux données de ses clients ? Les Etats-Unis en sont convaincus. Sébastien Le Belzic, auteur du portrait de l'Express, rapporte qu'au cours d'un entretien avec un diplomate en poste à Pékin, celui-ci lui aurait avoué qu' « *imaginer qu'une entreprise, qui bénéficie des subsides de l'Etat pour se développer, puisse ne pas répondre aux ordres du Parti est un non-sens* »[46].

L'organisation du groupe et sa gouvernance reste, elle aussi, assez opaque. C'est ce qui ressort de l'audition des dirigeants de Huawei France, réalisée par la commission d'enquête du Sénat sur la souveraineté numérique de la France. Weiliang SHI, directeur général de l'entreprise, expliquait que la société était à 100% privé puisqu'elle appartient exclusivement à ses salariés et son fondateur (Ren ZHENGFEI ne détiendrait qu'1,14% du capital), ce qui garantirait l'absence d'ingérence de l'Etat chinois sur les activités de l'entreprise. 96 000 employés seraient donc les seuls propriétaires du groupe, et éliraient un Comité de 115 membres pour représenter leurs intérêts et désigner les membres des conseils d'administration et de surveillance. Il est toutefois possible de s'interroger sur l'origine des financements qu'impose

[46] S. Le BELZIC : « *Ren Zhengfei, l'œil de Pékin* », l'Express, numéro du 20 juin 2019, pp 84-87

un secteur aussi concurrentiel, technologique et gourmand en recherche et développement, qu'est celui des télécommunications.[47]

Enfin, un rapport réalisé par l'Open Source Center, une branche des services de renseignement américain dédié à l'analyse de sources publiques, établissait que certains membres de Huawei entretenaient des liens étroits avec le Guoanbu (le Ministère de la Sécurité de l'Etat chinois)[48].

Huawei a constamment nié collaborer avec l'Etat chinois, déployant à cet effet d'importantes campagnes de communication, qui peinent pourtant à trouver de l'écho au-delà des frontières. Bien qu'aucune preuve concrète n'ait été établie, l'intégrité de la firme chinoise a été remise en question plusieurs fois. En janvier 2017, des informaticiens officiant au siège de l'Union Africaine, à Addis-Abeda, se rendent compte que les serveurs de l'institution tournent à plein régime lorsque les locaux sont vides, entre minuit et deux heures du matin. Après quelques recherches, le service de sécurité informatique de l'organisation s'aperçoit que l'ensemble des données stockées chaque jour sont copiées et envoyées vers des serveurs basés à Shanghai, à 8000 kilomètres de distance. Huawei plaide alors pour une faille dans ces systèmes, ce qui ne sera néanmoins jamais démontré. Les fonctionnaires africains décideront de ne pas déclencher de crise diplomatique, se contentant de changer quelques infrastructures (nouveaux serveurs, utilisation de câble et non de Wifi pour certains outils informatiques sensibles) et de se passer des services des ingénieurs chinois[49]. Huawei s'est également retrouvé cité dans une affaire d'espionnage plus récemment encore. Le 8 janvier 2019, Stanislaw ZARYN, membre du cabinet du ministre chargé de la coordination des services spéciaux polonais, annonce en effet que deux individus viennent d'être arrêtés car pèsent sur eux des soupçons d'espionnage pour le compte de la Chine. Parmi les deux suspects, il est évoqué un « *homme d'affaires chinois travaillant pour un important groupe d'électroniques* »[50]. La description laissant peu de place au doute, Huawei finira par licencier l'individu en question 3

[47] Audition des dirigeants de Huawei France par la commission d'enquête du Sénat sur la souveraineté numérique de la France, le 18 juillet 2019

[48] Open Source Center : « *Huawei Annual Report Details Directors, Supervisory Board for First Time* », rapport annuel, publié le 5 octobre 2011, (https://fas.org/irp/dni/osc/huawei.pdf), (consulté le 26 juin 2019)

[49] J. TILOUINE & G. KADIRI : « *A Addis-Adeba, le siège de l'Union africaine espionné par Pékin* », le Monde, le 26 janvier 2018

[50] J. PLUCINSKA & K. WITENBERG : « *Poland arrests Huawei employee, Polish man on spying allegations* », Reuters, le 11 janvier 2019, (https://www.reuters.com/article/us-poland-security/poland-arrests-huawei-employee-polish-man-on-spying-allegations-idUSKCN1P50RN), (consulté le 16 mai 2019)

jours plus tard, en rappelant que le respect des réglementations nationales a toujours été une priorité pour le groupe.

Bien que Huawei représente inéluctablement un risque pour les réseaux, c'est davantage les vulnérabilités propres aux caractéristiques de la 5G qui ont inquiété certains acteurs intéressés par les questions de sécurité en France. Ainsi, Thomas GASSILLOUD et Pascal ALLIZARD, tous deux parlementaires, ont été chargés de rédiger des avis sur la proposition de loi 5G pour leurs commissions respectives (commission de la défense nationale et des forces armées de l'Assemblée nationale pour le premier, commission des affaires étrangères, de la défense et des forces armées du Sénat pour le second). Ils en arrivent au même constat : si Huawei représente une menace, l'arrivée de la 5G s'accompagne également de vulnérabilités nouvelles, qui font peser des risques inédits sur la sécurité et la résilience des réseaux de télécommunication et d'information.

Ces risques et menaces proviennent de l'architecture même des réseaux 5G. Présentée comme une technologie de rupture du fait de ses caractéristiques, ce nouveau standard de télécommunication aura recours à de nouveaux facteurs, parfois vecteurs de risques, afin de pouvoir apporter toutes les évolutions qu'il promet.

En premier lieu, contrairement aux équipements des générations précédentes qui n'avaient pour but que de transmettre les données entre les appareils connectés des utilisateurs et le cœur de réseau (l'élément critique qui traite les données, à partir duquel on peut réaliser des interceptions), les antennes 5G auront une vocation plus active. En effet, les évolutions promises par la 5G passent par une évolution des équipements qui composent son architecture. Avec la 5G, des « *fonctions sophistiquées* »[51] sont ainsi intégrées dans les équipements de bord de réseau ; ce n'est donc plus simplement le cœur de réseau qui traite la totalité des informations, mais également les antennes-relais. En d'autres termes, la 5G conduira à décentraliser les fonctions de traitement de données du cœur de réseau vers des équipements qui ne présentaient jusqu'alors aucun risque. Or, les caractéristiques propres à cette technologie ainsi que les défis posés par l'explosion du nombre d'objets connectés supposent une plus grande surface de réseaux que les générations précédentes, il y aura donc beaucoup plus d'antennes et de capteurs, et encore plus de risques. La prise en compte de ces deux paramètres

[51] Avis n° 569 (2018-2019) de M. Pascal ALLIZARD, fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat, déposé le 12 juin 2019

implique donc que les outils et technologies permettant de sécuriser les actuels cœurs de réseau contre les interceptions devront être étendus à tous les équipements de réseau 5G…

En second lieu, le déploiement de la 5G sera suivi d'une virtualisation des réseaux : une part des équipements physiques va être remplacée par des logiciels qui seront diffusés dans le cloud, et qui ne seront donc plus implantés dans les équipements, ce afin d'accroître la rapidité des traitements de données. Il sera donc beaucoup plus complexe de savoir où une fonction de traitement de données est implantée avec la 5G. Thomas GASSILLOUD le relève ainsi dans son avis : « *Très schématiquement, là où l'interception d'un flux d'information nécessite dans les réseaux de 4G un dispositif technique particulier, telle une « porte dérobée », il suffira de posséder les codes d'administrateur pour accéder aux logiciels et aux clouds des réseaux de 5G* »[52]. Cette virtualisation des réseaux permettra également aux équipementiers de réaliser des mises à jour plus souvent, ce qui conduira forcément les opérateurs à accroitre leurs efforts afin de s'assurer de la sécurité des réseaux en suivant et contrôlant des versions de logiciels qui évolueront plus rapidement qu'auparavant.

Le déploiement de la 5G présenterait donc un risque bien réel. Néanmoins, il semblait intéressant de contrebalancer ces études en prenant en compte les déclarations des opérateurs. J'ai eu la chance de pouvoir m'entretenir avec François VINCENT, membre de la Direction de l'Ingénierie Mobile de SFR, le 12 juillet 2019[53]. D'après lui, le déploiement de la 5G comportera bien des risques, mais il nuance toutefois les avis des parlementaires : « *il y a des risques réels, mais c'est davantage un choix qui dépend de l'environnement géopolitique actuel. En effet, sur le fond, la 5G, dans sa phase initiale (2020-2025) ne sera que très peu différente de la 4G. Il s'agira simplement d'une 4G plus performante en termes de débit mais la partie sensible, le cœur de réseau, restera la même. En France, aucun équipement Huawei n'a jamais eu accès au cœur de réseau car c'est l'ANSSI qui décide déjà. Cette nouvelle loi ne répond pas à des nouvelles vulnérabilités, en tout cas pour le moment, car ce sont les mêmes que pour la 4G actuellement.* »

La 5G, telle qu'elle sera déployée et présentée dans les cinq prochaines années, ne semble donc pas s'accompagner de nouvelles vulnérabilités. Néanmoins, tous sont d'accords pour reconnaître que la nécessité d'avoir recours à la décentralisation, la multiplication et la

[52] Avis n° 1830 (2018-2019) de M. Thomas GASSILLOUD, fait au nom de la commission de la défense de l'Assemblée nationale, déposé le 2 avril 2019

[53] Entretien réalisé avec M. François VINCENT, ingénieur auprès de la Direction de l'Ingénierie Mobile de SFR, le 12 juillet 2019 au siège social d'Altice France, (*voir annexe 2*)

virtualisation des réseaux, afin d'atteindre les potentialités promises par cette technologie, conduira à accroître les risques propres aux systèmes d'information et de communication. Bien que Thomas GASSILLOUD l'ait relevé très clairement dans son avis, « *c'est par son architecture même, davantage que par la nature des équipements, que la 5G présentera des vulnérabilités nouvelles* »[54], c'est pourtant le choix de l'équipementier, plus que l'architecture du réseau, qui a conduit le Gouvernement à réagir. Les opérateurs l'ont d'ailleurs bien compris puisque leurs stratégies d'influence étaient davantage dirigées contre les menaces que représenteraient Huawei (« Huawei n'a pas accès au cœur de réseau », « Huawei reçoit un agrément pour commercialiser ses équipements ») que pour promouvoir la mise au point des nouvelles techniques de contrôle qui permettraient de garantir la sécurité des informations circulant dans les réseaux compte tenu de leur architecture inédite.

Cette méfiance des décideurs publics envers la firme chinoise se devine également à travers la prise en compte d'un autre type de menace : une coupure accidentelle ou volontaire des réseaux. En effet, si l'atteinte la plus probable aux réseaux repose sur des tentatives d'interception de données, il convient de ne pas omettre l'interruption de connexion. La population serait très certainement interloquée puis bouleversée par la situation, ce qui pourrait conduire à des mouvements de panique. Mais la situation pourrait très vite empirer : une coupure de réseau survenant durant une crise (accident industriel, catastrophe naturelle, attaque terroriste…), aurait des effets dévastateurs puisqu'elle risquerait d'empêcher les différents acteurs chargés de prendre et diffuser les mesures qui s'imposeraient alors de communiquer entre eux. La chaîne de commandement pourrait être rompue, et la crise s'aggraver. Lors d'une visite de la Préfecture du Nord, à Lille, un membre du Service Interministériel Régional des Affaires civiles et Economiques de Défense et de la Protection Civile (SIRACED-PC) avait ainsi reconnu qu'une attaque qui altèrerait les réseaux combinée à un attentat ou un accident de grande ampleur constitue la menace la plus importante qui pèse sur le territoire aujourd'hui. Il est bien évident que tendre vers une société de plus en plus interconnectée telle que celle que promet la 5G conduira forcément à accroître l'importance et la gravité des dégâts qui résulteraient de pareille situation (absence de connexion entre les véhicules autonomes par exemple).

Il convient donc de savoir si la 5G pourrait accroître la probabilité d'assister à des dysfonctionnements dans le réseau, en raison notamment des nouveaux équipements et logiciels

[54] François VINCENT, (*op. cit.*)

qui l'accompagneront. Néanmoins, l'angle adopté par certains décideurs publics laisse penser, une nouvelle fois, qu'il s'agit d'une loi « anti-Huawei » et non d'un texte visant tous les équipementiers.

Le 18 avril 2019, Arthur DREYFUSS, Secrétaire Général de SFR, a réalisé un discours lors de la session de printemps de l'IDATE, un think tank européen spécialisé dans le numérique et les télécommunications. Il a profité de cette allocution pour revenir sur les nets avantages offerts par Huawei par rapport à ses concurrents[55]. Parmi ceux-ci, l'actuel président de la Fédération Française des Télécoms cite notamment : la fiabilité des produits avec notamment « *3 fois moins de pannes dues à un équipement radio en zone Huawei* » et « *presque 4 fois moins de cas d'indisponibilité de réseau répertoriés dans ces zones* » – la qualité des logiciels mis au point, tandis qu' « *il est possible de constater, lors de chaque mise à jour annuelle, un nombre d'anomalies critiques ou majeures très élevé chez certains concurrents*» – et enfin l'avance technologique dont dispose Huawei sur le marché, car « *en zone Huawei, les nouvelles fonctionnalités sont systématiquement disponibles 1 à 2 avant pour nos clients, ce qui finit par rendre l'application des orientations stratégiques en zone Nokia très complexe* ». Comme il avait été déjà évoqué, il importe de nuancer quelque peu ces propos, du fait notamment de la part d'équipements Huawei dans le total des équipements déployés par SFR (52%). Toutefois, certaines informations viennent confirmer cette avance dont jouit Huawei par rapport à ses concurrents. Ainsi, Huawei est la firme qui détient le plus de brevets technologiques avec 5 300 licences déposées en 2018 (soit 2 fois plus que l'entreprise seconde au classement) d'après le rapport annuel de l'Organisation mondiale de la propriété intellectuelle[56]. Dans le même esprit, un article d'Alternatives Economiques[57] de mai 2019 explique qu'il est impossible de se passer de Huawei aujourd'hui, dont les investissements en innovation et recherche et développement atteignent les 11 milliards d'euros par an.

Pourtant, les parlementaires chargés de rédiger les avis et rapports relatifs aux enjeux de sécurité liés au déploiement de la 5G en France ont développé des argumentaires à charge par rapport à la qualité et la fiabilité des équipements de Huawei.

---

[55] E. BEMBARON : « Les opérateurs télécoms français veulent faire payer les géants du net », Le Figaro,le 22 mai 2019

[56] World Intellectual Property Organization (Organisation mondiale de la propriété intellectuelle) : « *2018 Annual report on the number of technology patents filed worldwilde* », rapport annuel, publié en janvier 2019, (https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2018.pdf), (consulté le 2 avril 2019)

[57] J. DELEPINE : « *Huawei : la guerre technologique est déclarée* », Alternatives économiques, édition de mai 2019, n°390, pp 67-69

Ainsi, Catherine PROCACCIA, la sénatrice responsable du rapport réalisé au nom de la commission des affaires économiques, s'appuyant sur un moratoire vitrioleur réalisé par l'Institut Montaigne[58], a estimé que les risques d'accidents étaient bien plus élevés avec les équipements Huawei et fait état de « *plusieurs investigations* » qui « *ont mis en évidence des failles importantes dans les réseaux Huawei* », sans toutefois les citer. Reprenant une étude réalisée par les services de renseignement anglais[59], la Sénatrice évoque ainsi « *d'importants problèmes relatifs aux logiciels réalisés par le groupe* » qui accroitraient profondément les risques de dysfonctionnement des réseaux. Toutefois, à aucun moment Catherine PROCACCIA ne s'intéresse à la situation des autres équipementiers. Ainsi, son rapport, tel qu'il est rédigé, laisse penser qu'elle ne s'est pas inquiétée de savoir si les équipements produits par Ericsson, Nokia et Samsung présentaient des caractéristiques permettant d'attester d'une qualité et d'une fiabilité supérieures. Alors qu'Arthur DREYFUSS pointait du doigt les failles présentes dans les logiciels produits par Nokia durant l'écriture de son rapport, la Sénatrice ne s'est pas donnée la peine d'étendre ses investigations aux autres équipementiers.

Dans le même esprit, le Sénateur Franck MONTAUGE déclarait, lors de l'audition de Cédric O par la Commission d'enquête sur la souveraineté numérique de la France, le 20 juin 2019, qu'« *il n'apparait pas que le géant chinois des télécommunications ait autant d'avance sur ses concurrents qu'on puisse le croire. Il y a du retard chez certain, mais la course à la 5G est loin d'être déterminée* ». Pourtant, il n'existe pas un spécialiste de la question qui abonderait dans son sens, tant la supériorité de Huawei par rapport à ses concurrents est avérée et reconnue. Néanmoins, une chose est sûre, la 5G se développe déjà dans certains pays du monde, et il semblera compliqué de se passer de Huawei pour la déployer. Comme le déclarait Jean-Marc FOUR dans sa chronique du 19 mars 2019 : « *Huawei est le maître de l'infrastructure 5G, et avec 100 milliards de dollars de budget de recherche pour les cinq années à venir, ils ne pourront que progresser* »[60].

---

[58] M. DUCHATEL & F. GODEMENT : « *L'Europe et la 5G : le cas Huawei* », étude réalisée pour l'Institut Montaigne, mai 2019, (https://www.institutmontaigne.org/publications/leurope-et-la-5g-le-cas-huawei-partie-2), (consulté le 9 juin 2019)

[59] Huawei cybersecurity evaluation centre oversight board, rapport annuel de 2018, publié en janvier 2019, (https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019), (consulté le 4 juillet 2019)

[60] J-M. DUFOUR : « *Pourquoi Huawei peut gagner la bataille technologique* », France Inter, le 19 mars 2019

La 5G est porteuse d'autant de promesses que de vulnérabilités. Si son déploiement permettra de révolutionner certains usages et d'apporter des solutions recherchées à la fois par les industriels et les décideurs publics, il est également craint par les acteurs intéressés en raison des questions d'enjeux de sécurité pesant sur les réseaux radioélectriques, depuis la campagne de lobbying menée par les Etats-Unis à l'encontre de Huawei. Il convient néanmoins de s'en remettre une nouvelle fois aux lumières de François VINCENT, de la Direction Ingénierie Mobile de SFR : « *il y a ce fantasme des nouveaux usages, tout comme les risques inhérents aux infrastructures physiques et logiciels de la 5G sont exagérés. Pour les 5 prochaines années, ce que l'on appellera 5G ne sera qu'une montée en débit de la 4G, une sorte de 4,5G. Donc les usages que l'on promet mettront du temps avant d'être développés et les menaces que l'on attend mettront du temps avant d'être réelles. Finalement, c'est la 6G qui bouleversera notre quotidien, la 5G est une génération passerelle* »[61]. Toutefois, et pour reprendre ce que disait Thomas GASSILLOUD, « *le déploiement de la 5G en France est imminent* ». Dès lors, s'assurer que la France bénéficiera de toutes les potentialités offertes par cette technologie, tout en garantissant dans le même temps la sécurité des systèmes d'information et de communication, conduit forcément à s'intéresser au dispositif juridique qui encadrera le déploiement de cette nouvelle génération de standard de communication.

[61] François VINCENT, (*op. cit.)*

II) La nécessité d'adapter le dispositif juridique existant afin d'assurer le juste équilibre entre respect des objectifs de sécurité nationale et nécessaire déploiement des réseaux

Les opérateurs de télécommunications jouissent d'un statut particulier du fait de la nature de leurs activités, considérées, logiquement, comme d'importances vitales. L'objectif de garantir la résilience des réseaux qu'ils exploitent est l'une des principales raisons motivant la nécessité de les soumettre à un cadre juridique spécifique. Aujourd'hui, plusieurs dispositifs juridiques sont applicables aux opérateurs mais ils ont des finalités différentes : l'un trouve son fondement dans la protection du secret des correspondances et de la vie privée quand l'autre repose sur la protection des activités d'importance vitale. Toutefois, il ressort de l'exposé des motifs accompagnant la proposition de loi 5G que la base juridique sur laquelle repose le régime existant se trouvera dépassée par les nouveaux usages et les vulnérabilités inédites que promet la 5G. Tenter de faire adopter le nouveau régime juridique au moyen d'un simple amendement inséré dans une loi trahit par ailleurs la précipitation du Gouvernement mais aussi l'urgence de la situation. Pourtant, les opérateurs de télécommunications n'ont eu de cesse de rassurer les décideurs publics, voyant d'un mauvais œil l'apport d'une procédure administrative supplémentaire. A force d'opérations de communication, les opérateurs sont toutefois parvenus à alléger la version initialement débattue à l'Assemblée nationale. Dès lors, il importera d'apprécier le régime initial dans un premier temps, afin d'en comprendre les fondements mais aussi et surtout les failles qui ont poussé le législateur à intervenir (A). Puis, à partir de ces réflexions et des arguments développés par les opérateurs, il conviendra de démontrer que la loi 5G constitue un point d'équilibre entre d'une part la défense des intérêts de ces-derniers et, d'autre part, la prise en compte des risques et vulnérabilités découlant du déploiement de cette nouvelle technologie (B).

A) Un cadre juridique initial rendu désuet par les caractéristiques de la 5G ?

La prise en compte des différents enjeux de sécurité liés à la 5G – multiplication et virtualisation de l'architecture réseau, impératif de résilience des réseaux – ainsi que la campagne offensive menée par les Etats Unis ont conduit le législateur à intervenir pour prévenir les risques et vulnérabilités qui pourraient découler du déploiement de cette technologie. Néanmoins, la question de l'adaptation du dispositif juridique existant se pose : certains spécialistes plaident pour renforcer le régime propre aux équipements 4G, quand les opérateurs assurent que les dispositions législatives, en l'état, suffisent à garantir la sécurité des réseaux de télécommunications. L'actualité de ces-derniers mois laisse peu de place au suspens, la loi 5G ayant été promulguée en août 2019.

Comme le relève les rédacteurs de la proposition de loi 5G dans l'exposé des motifs accompagnant son dépôt « *Il convient de noter qu'il existe déjà un dispositif d'autorisation préalable pour les équipements radioélectriques dans le code pénal (article R. 226-3) mais celui-ci a pour objet principal la protection du secret des correspondances électroniques et de la vie privée. Il se concentre à cette fin sur les opérations de commercialisation et d'acquisition des seuls équipements de nature à permettre des atteintes au secret des correspondances électroniques* »[62]. Il semble néanmoins nécessaire de rappeler qu'il existe également un régime législatif spécifique qui pèse sur les opérateurs du fait de l'importance vitale attachée au secteur des télécommunications.

L'article R. 226-3 du code pénal prévoit que : « *La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'Etat, lorsque ces faits sont commis, y compris par négligence, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret*

[62] Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, enregistrée à la Présidence de l'Assemblée nationale le 20 février 2019

ou sans respecter les conditions fixées par cette autorisation »[63] est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende. La captation de données informatiques est donc prévue explicitement par le texte de l'article R. 226-3. De plus, la loi se réfère à l'article R. 226-15, qui nous intéresse particulièrement puisqu'il protège le secret des correspondances et condamne « *le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions* »[64] à 1 an d'emprisonnement et 45 000 euros d'amende. Toutefois, l'article R. 226-3 traite de « *la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques* » permettant l'interception de données informatiques, de sorte qu'il tend à s'appliquer davantage aux équipementiers qu'aux opérateurs de télécommunications, qui se contentent de les acquérir. En revanche, l'article R. 226-7 du code pénal est davantage pensé pour contrôler les activités de déploiement des opérateurs, puisqu'il prévoit que « *l'acquisition ou la détention de tout appareil ou dispositif technique figurant sur la liste mentionné à l'article R. 226-1* [qui renvoie lui-même aux dispositions de l'article R. 226-3 du même code] *est soumise à une autorisation délivrée par le Premier ministre, après avis de la commission mentionnée à l'article R. 226-2* »[65].

Le régime français repose donc sur un double système d'autorisation. Une autorisation de mise sur le marché des équipements destinés aux réseaux radioélectriques, afin de s'assurer de leur qualité, qui pèse sur les équipementiers (une sorte de certification). Puis une autorisation d'acquisition délivrée aux opérateurs afin qu'ils puissent déployer les équipements ayant déjà fait l'objet d'un contrôle en amont. Dans ces conditions, le système apparait sérieusement verrouillé en faisant intervenir le Gouvernement à chaque étape du processus, de l'achat de l'équipement à son installation. De plus, le Premier ministre peut compter sur l'avis d'une commission d'experts, mentionnée à l'article R. 226-2 du code pénal, avant de prendre la décision de délivrer ou non une autorisation.

Cette commission est composée « *du directeur général de l'ANSSI, d'un représentant du ministère de la justice, d'un représentant du ministère de l'intérieur, d'un représentant du ministère de la défense, d'un représentant du ministre chargé des douanes, d'un représentant du ministre chargé de l'industrie, d'un représentant du ministre chargé des*

[63] Article R. 226-3 du code pénal, alinéa 1er
[64] Article R. 226-15 du code pénal, alinéa 2
[65] Article R. 226-7 du code pénal

télécommunications, d'un représentant de la Commission nationale de contrôle des techniques de renseignement, d'un représentant du directeur général de l'Agence nationale des fréquences et deux personnalités désignées par le Premier ministre en raison de leur compétence »[66]. C'est l'ANSSI qui assure le secrétariat de cette commission consultative qui sera saisie pour chaque demande d'autorisation prévue par les articles R.226-3 et R.226-7. C'est dire si le rôle de cette commission, et forcément de l'ANSSI, est prépondérant dans la détermination des objectifs stratégiques relatifs à la sécurité des réseaux radioélectriques.

Bien qu'elle ait été déjà évoquée, il convient de revenir sur le rôle et la nature des missions de l'ANSSI. L'Agence nationale de sécurité des systèmes d'information a été créée par un décret de 2009[67], mais il faut attendre une loi du 18 décembre 2013 pour établir que « *le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'agence nationale de sécurité des systèmes d'information* »[68]. Rattachée au SGDSN, cette autorité administrative dispose d'une compétence et d'une expertise reconnue qu'elle met au profit des opérateurs importance vitale. Elle a la charge d'assurer la sécurité des réseaux radioélectriques, et plus généralement des systèmes d'information, en prévenant les tentatives de cyberattaques et en y répondant lorsque cela s'avère nécessaire. C'est par exemple l'ANSSI qui est intervenue lors de l'attaque NotPetya qui a notamment frappé Saint-Gobain en juin 2017[69]. Lors de l'audition du président de l'Arcep, Sébastien SORIANO, par la commission des affaires économiques du Sénat le 10 avril 2019, celui-ci était revenu sur la compétence de l'ANSSI, déclarant que : « *notre pays est mieux préparé et moins exposé que d'autres. Le SGDSN et l'ANSSI, depuis une dizaine d'années, travaillent très régulièrement avec les opérateurs, les équipementiers télécoms et l'Arcep. Tel est mon message sur la sécurité : nous ne partons pas de zéro, puisque les acteurs se connaissent et les procédures sont bien établies* »[70]. Il est vrai, le régime légal en place implique que l'ANSSI soit constamment en relation avec les opérateurs et leurs équipementiers, le but étant de parvenir à dégager des solutions techniques permettant

---

[66] Article R. 226-2 du code pénal

[67] Décret n°2009-834, portant création de l'Agence nationale de sécurité des systèmes d'information, pris le 7 juillet 2009

[68] Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

[69] A. CLAPAUD : « *NotPetya : Saint-Gobain tire la leçon et s'arme d'intelligence artificielle* », Industrie&Technologies, le 12 octobre 2018, (https://www.industrie-techno.com/article/notpetya-saint-gobain-tire-la-lecon-et-s-arme-d-intelligence-artificielle.53974), (consulté le 8 août 2019)

[70] Audition de Sébastien Soriano, Président de l'Autorité de régulation des communications électroniques et des postes, par la commission des affaires économiques du Sénat, en date du 10 avril 2019

d'assurer la sécurité et la résilience des réseaux radioélectriques sans entraver leur déploiement. C'est en raison de ses compétences, de son expertise et du rôle de premier plan que lui attribue l'article R. 226-2 du code pénal quant au traitement des dossiers de demande d'autorisation que l'ANSSI s'est imposée, au fil des ans, comme le premier partenaire des opérateurs dans leur mission de sécurisation des réseaux.

La liste des équipements dont la fabrication, l'importation, la détention, l'exposition, l'offre, la location, la vente ou l'acquisition est soumise à une demande d'autorisation, tel que le prévoient les articles R. 226-3 et R. 226-7 du code pénal, a été fixée par un arrêté du Premier ministre en date du 4 juillets 2012. Celui-ci dispose que les équipements relevant de l'article R. 226-3 et R. 226-7 sont « *les appareils, à savoir tous dispositifs matériels et logiciels, conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques* »[71]. L'arrêté dresse ensuite une liste non-exhaustive des équipements visés, parmi lesquels « *les appareils dont les fonctionnalités qui participent à l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement des correspondances ne sont pas activées, quel que soit le moyen d'activation* »[72], *« les appareils permettant, par des techniques non intrusives d'induction électromagnétique ou de couplage optique, d'intercepter ou d'écouter les correspondances transitant sur les câbles filaires ou les câbles optiques des réseaux de communications électroniques* »[73] ainsi que les « *dispositifs techniques, à savoir tous matériels ou logiciels, spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères, opérations ayant pour objet la captation de données informatiques* »[74].

Le Député Thomas GASSILLOUD a pu auditionner Guillaume POUPARD, Directeur général de l'ANSSI, dans le cadre de l'avis qu'il a réalisé au nom de la commission de la défense nationale et des forces armées. Le Directeur général de l'Agence a alors expliqué que l'article R. 226-3 visait, initialement, à protéger le secret des correspondances et le respect de la vie privée en empêchant la fabrication et l'acquisition d'appareils de surveillance (mouchard,

[71] Annexe 1 de l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévues par l'article 226-3 du code pénal
[72] Idem
[73] Idem
[74] Idem

micro-espion) par des personnes privées. De par l'évolution des usages numériques, la France a fait le choix d'étendre le champ d'application de cet article aux équipements de réseaux (les cœurs de réseaux) qui peuvent permettre l'interception de données informatiques, au lieu de prévoir un régime spécifique. Toutefois, Guillaume POUPARD reconnaît que les demandes d'autorisation de mise sur le marché et de déploiement de ces équipements de réseaux radioélectriques représentent aujourd'hui « *la plus grande part des dossiers instruits sur le fondement de l'article R. 226-3* »[75].

Afin de comprendre comment ce régime juridique est mis en œuvre, dans la pratique, j'ai pu m'entretenir avec Myriam MADORE, Directrice des obligations légales pour SFR, le 30 juillet 2019. Concrètement, elle est à la tête du service chargé de l'acquisition des équipements réseaux et des dépôts de demande d'autorisation de déploiement de ces-mêmes équipements auprès de l'ANSSI. Myriam MADORE estime que le dispositif en place est déjà suffisamment complet pour qu'on l'alourdisse davantage : « *Lorsqu'ils souhaitent accéder au marché français, les équipementiers doivent formuler une demande d'autorisation auprès de l'ANSSI. Si celle-ci est acceptée par le Premier ministre, après avis de l'Autorité, elle sera valable pour une durée de 6 ans. Les opérateurs, lorsqu'ils souhaitent acquérir des équipements réseaux en vue de les déployer, s'assurent que Huawei, Nokia ou Ericsson possèdent bien la certification leur permettant de vendre leurs dispositifs. Une fois l'appareil acheté, les opérateurs déposent eux aussi une demande auprès de l'ANSSI pour pouvoir l'exploiter, c'est-à-dire le déployer. L'autorisation délivrée aux opérateurs par le Premier ministre vaut quant à elle pour 3 ans. Ce cadre juridique est complet puisque le Gouvernement à la main sur chaque étape du processus, ce qui lui permet de s'assurer de la fiabilité des dispositifs à tout moment. Aujourd'hui, avec la 4G, Huawei n'a déjà pas accès aux cœurs de réseaux sur le fondement de cet article. Modifier cette procédure, alors que les opérateurs, les équipementiers et l'ANSSI la maîtrisent est un non-sens* ».[76]

Les opérateurs télécoms sont également soumis à un régime spécifique découlant de la nature de leurs activités, considérées comme d'importance vitale. C'est ainsi que l'arrêté du 28 novembre 2016 est venu fixer « *les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-*

[75] Thomas GASSILLOUD, (*op. cit.*)
[76] Entretien avec Myriam MADORÉ, Directrice des obligations légales de SFR, le 30 juillet 2019 à l'Altice Campus (*voir annexe 3*)

secteur d'activités d'importance vitale « Communications électroniques et Internet » »[77]. Cet arrêté liste ainsi les obligations pesant sur les opérateurs d'importance vitale du secteur, et notamment celle de mettre en œuvre une politique de sécurité des systèmes d'information (PSSI) qui arrête les procédures à respecter afin de garantir la résilience des réseaux radioélectriques dont ils ont la charge (gestion de crise en cas d'attaques informatiques, audit de sécurité, maintien en conditions de sécurité des ressources…). Cette PSSI, ainsi qu'un rapport annuel relatif à sa mise en œuvre, doivent être tenus à la disposition de l'ANSSI[78]. Cet arrêté contient également des mesures strictes de nature à minimiser la survenance d'une menace sur les réseaux (règles relatives aux droits d'accès, à l'homologation de certains équipements, aux accès à distance…). Une obligation se réfère explicitement à la problématique du déploiement des dispositifs par les opérateurs : les règles relatives à l'installation de services et d'équipements[79]. En vertu de cette mesure, l'opérateur est responsable du respect des indications suivantes : « *l'opérateur installe sur ses systèmes d'information les seuls services et fonctionnalités indispensables à leur fonctionnement ou leur sécurité* », « *l'opérateur ne connecte à ses systèmes que des équipements, matériels périphériques et supports amovibles qu'il a dûment répertoriés et qui sont indispensables au fonctionnement ou à la sécurité de ces systèmes* » et de « *l'analyse des contenus de chaque support amovible avant son utilisation, notamment à la recherche de code malveillant. L'opérateur met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques de code malveillant provenant de ces supports* »[80].

Il est plus que logique que des obligations spécifiques pèsent sur les opérateurs télécoms, en raison de l'ampleur de la crise qui découlerait d'un dysfonctionnement des réseaux ou d'une attaque visant à les altérer. Il est, de plus, intéressant de relever que les opérateurs télécoms ne sont pas des OIV spécifiques, puisqu'ils fournissent leur service à d'autres OIV. Pour toutes ces raisons, la loi de programmation militaire du 13 juillet 2018 a inséré un article L. 33-14 dans le code des postes et des communications électroniques, lequel prévoit que « *Pour les*

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

[78] Annexe 1 de 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 » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense

[79] Ibidem

[80] Ibidem

besoins de la sécurité et de la défense des systèmes d'information, les opérateurs de communications électroniques peuvent recourir, sur les réseaux de communications électroniques qu'ils exploitent, après en avoir informé l'autorité nationale de sécurité des systèmes d'information, à des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés »[81]. Ce qui accroît la capacité des opérateurs à prévoir les menaces et amenuise donc forcément les risques et vulnérabilités pesant sur les réseaux qu'ils exploitent.

La même loi de programmation militaire autorise également l'ANSSI à « *mettre en œuvre et à exploiter des systèmes de détection sur le réseau d'un opérateur dans le cas où elle aurait connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques ou des opérateurs d'importance vitale* » en insérant un article L. 2321-2-1 dans le code de la défense.

Aux vues du régime de demande d'autorisation pesant à la fois sur les équipementiers et sur les opérateurs télécoms ainsi que des précautions prises sur le fondement de la protection du secteur d'importance vitale que représente les communications électroniques et l'Internet, il convient de s'intéresser aux motifs qui ont poussé le Gouvernement a jugé que ce dispositif pourrait être rendu défaillant par l'arrivée de la 5G.

Il ressort des différents avis et rapports réalisés par les parlementaires en charge de la question (Eric BOTHOREL, Catherine PROCACCIA, Thomas GASSILLOUD et Pascal ALLIZARD) que la principale lacune du dispositif existant reposerait sur sa base juridique trop étroite et non-adaptée. Le fait que les demandes d'autorisation de mise sur le marché et d'exploitation des équipements réseaux soient prévues par l'article R. 226-3 du code pénal poserait problème puisque ce-même article a pour fondement la protection du secret des correspondances. Il ne serait donc pas adapté à la virtualisation des réseaux ni aux nouveaux usages que permettrait la 5G. Toutefois, il semble possible de contredire cet argument. Lors d'une visite des sénateurs du groupe Union Centriste sur le site d'Altice, en mai 2019, le Secrétaire Général de SFR a même avancé l'idée que cette base juridique serait même trop large. En visant tous les appareils ayant pour objet la captation de données informatiques, l'article 226-3 ne se cantonne pas à prendre uniquement en compte les équipements de cœurs de réseaux, comme il a pu être avancé. Bien que les antennes-relais et les capteurs ne comportent pas, aujourd'hui, de risque d'interception de données, ceux-ci tomberont sous le

[81] Article L.33-14 du code des postes et des communications électroniques

champ de cet article dès que les innovations technologiques rendront ces équipements de bord de réseaux plus sensibles. Thomas GASSILLOUD développe un argument allant dans le même sens. Selon lui, « *la base légale sur laquelle a été fondée la procédure de contrôle prévue à l'article R. 226-3, pour légitime qu'elle soit, se limite au secret de la correspondance et à la protection de la vie privée des personnes. Or, avec la 5G, cette base légale peut devenir insuffisante : quand deux automates se transmettront des informations, difficile d'y voir un élément de la vie privée à protéger au titre du secret de la correspondance* »[82]. Bien que le fondement de cette base légale soit effectivement la protection du secret des correspondances et de la vie privée, elle a évolué, comme l'a reconnu Guillaume POUPARD. L'article R. 226-3 tend désormais plus à permettre au Gouvernement de contrôler les appareils ou dispositifs techniques ayant pour objet la captation de données informatiques qu'à protéger le secret des correspondances. Là encore, l'argument fondé sur l'étroitesse de la base juridique ne tient pas, puisque le Gouvernement a plusieurs fois modifié l'article R. 226-3 afin de l'adapter aux évolutions technologiques. En effet, un arrêté du 11 août 2016 est ainsi venu allonger la liste des appareils et dispositifs techniques tombant sous le régime de l'article R. 226-3 du code pénal. Son article 1 précise que « *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* »[83] entrent désormais dans le champ d'application des articles 226-3 et 226-7 du code pénal. Cette modification est exclusivement fondée sur la prise en compte des risques que pourrait faire peser la 5G en raison de l'architecture de ses réseaux. Les antennes-relais et les capteurs, c'est-à-dire les équipements de bords de réseau, sont explicitement visés par cet article, ce qui prouve que la diffusion des vulnérabilités des cœurs de réseau aux équipements situés en périphérie a bien été appréhendée par le Gouvernement. Néanmoins, il est prévu que cet arrêté s'applique à compter du 1er octobre 2021, soit 1 an et demi au moins après les premiers déploiements 5G sur le territoire. C'est sur cette erreur de calendrier que les décideurs publics se fondent pour justifier la nécessité de mettre au point un dispositif juridique propre à la 5G.

Or, à l'image de ce que François VINCENT évoquait lors de notre entretien : durant les 5 premières années la 5G ne sera qu'une 4G avec des débits plus puissants, de telle sorte que

[82] Thomas GASSILLOUD, (*op. cit.*)

[83] Article 1 de l'arrêté du 11 août 2016 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal

l'architecture réseau restera identique au moins jusqu'à l'entrée en vigueur de l'arrêté de 2016. Néanmoins, certains spécialités émettent des doutes à ce propos, à l'image de Pascal ALLIZARD qui estime que « *l'entrée en vigueur tardive de l'extension de la liste aux équipements d'interface en bordure de réseau, notamment aux antennes-relais 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 raisonnement fait une nouvelle fois défaut. Les opérateurs télécoms ont en effet répondu qu'évoluer sur un secteur nécessitant des dépenses en investissement très conséquentes (10 milliards d'investissements privés en 2017[84]), implique qu'ils poursuivent des stratégies sur le très long terme. Il aurait paru invraisemblable que des milliards d'euros soient dépensés dans l'achat d'équipements non-certifiés par l'ANSSI. En effet, le déploiement des réseaux prenant du temps, l'exploitation de ces équipements par les opérateurs serait forcément tombée sous le coup de l'article R. 226-1. Une demande d'autorisation aurait donc dû être déposée pour chacun d'eux, avec le risque de se les voir refuser (ce qui aurait été forcément très probable compte tenu de la méthode employée) et de perdre des milliards d'euros de dispositifs inexploitables sur le territoire français.

Le Gouvernement pouvait modifier la date d'entrée en vigueur de l'arrêté de 2016, afin que les équipements déployés aux bords de réseaux tombent sous le coup de l'article R. 226-3 dès l'arrivée de la 5G. Si le Gouvernement a préféré opter pour la promulgation d'une nouvelle loi spécifique à cette technologie, c'est que celle-ci apporte des garanties supplémentaires à l'article R. 226-3 du code pénal, y compris dans sa version de 2021. Catherine PROCACCIA apporte un début de réponse dans son rapport du 19 juin 2019 : « *La virtualisation et le fait que l'architecture du réseau dépendra en partie de son usage ont pour conséquence qu'une analyse centrée uniquement sur les caractéristiques techniques propres des équipements, tels qu'ils sont fournis par les équipementiers, ne suffit plus à couvrir l'ensemble des enjeux de sécurité, et qu'une analyse complémentaire des modalités d'exploitation (opérations de configuration et de*

[84] Arthur D. Little : « l'économie des Télécoms en 2018 », étude réalisée pour la Fédération Française des Télécoms, publiée en Décembre 2018, (https://www.fftelecoms.org/app/uploads/2018/12/etude_arthur_d_little_fftelecoms_2018_.pdf), (consulté le 1er avril 2019)

supervision du réseau, recours à la sous-traitance) adoptées par chaque opérateur devient indispensable »[85].

B) La mise en place d'un nouveau dispositif juridique entre pression des opérateurs et prise en compte de risques et vulnérabilités inédits

Le 1er août 2019, la promulgation de la loi 5G a eu pour effet d'insérer une section 7 intitulée « Régime d'autorisation préalable de l'exploitation des réseaux radioélectriques » au chapitre 2 du titre 1er du livre II du code des postes et des communications électroniques. Comprenant 5 articles, cette loi vient poser le nouveau cadre juridique relatif au déploiement des équipements de réseaux mobiles par les OIV. Il semble dès lors primordial d'étudier le nouveau régime d'autorisation mis en place par l'Etat. Dégagé suite à la constitution d'une Commission mixte paritaire, le texte final a toutefois subi quelques modifications par rapport à la version initialement votée par l'Assemblée nationale, auxquelles il conviendra de s'intéresser.

« *La présente proposition de loi prévoit ainsi un régime d'autorisation préalable, fondé sur des motifs de défense et de sécurité nationale, des équipements des réseaux de communications électroniques mobiles qui seront déployés pour diffuser la 5G* »[86], c'est par ces mots qu'Eric BOTHOREL ouvrait les travaux de la commission des affaires économiques de l'Assemblée nationale. Tel est le premier changement majeur opéré par le législateur : se fonder non plus sur la protection du secret des correspondances, mais sur des motifs de défense et de sécurité nationale. C'est effectivement ce qui ressort de l'alinéa 4 de l'article L. 34-11, qui prévoit qu' « e*st soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures, qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils*

[85] Rapport n° 579 (2018-2019) de Mme Catherine Procaccia, fait au nom de la commission des affaires économiques du Sénat, déposé le 19 juin 2019

[86] Rapport n° 1832 de M. Eric BOTHOREL, fait au nom de la commission des affaires économiques, déposé le 3 avril 2019

installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils »[87].

De ce changement de base juridique découle un des apports majeurs, et très décrié par les opérateurs, de ce texte. En effet, à première vue, seule « *l'exploitation des appareils permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile* », est soumise à autorisation préalable du Premier ministre. De sorte que l'impératif de protection des intérêts de la défense et de la sécurité nationale ne reposerait que sur les opérateurs et plus sur les équipementiers, comme c'était le cas. En effet, l'alinéa 5 de l'article L. 34-11 du code des postes et des communications électroniques, vient confirmer que « *l'autorisation mentionnée au premier alinéa du présent I n'est requise que pour l'exploitation, directe ou par l'intermédiaire de tiers fournisseurs, d'appareils par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public* »[88]. Ce nouveau régime d'autorisation pèsera donc seulement sur les OIV. Il s'agit là d'une décision difficilement compréhensible, puisqu'il aurait été plus aisé d'étendre le champ d'application de l'article L. 34-11 aux équipementiers, étant donné que les experts du renseignement mettaient en garde contre la possibilité, pour Huawei ou Cisco, d'intégrer volontairement des failles dans leurs équipements afin de permettre d'intercepter des données numériques. Cela signifierait donc que les antennes-relais de Huawei ne comportent pas de risque, en l'état, puisqu'elles seront toujours disponibles sur le marché sans être soumises à un quelconque régime d'autorisation préalable. Certes, s'il est avéré que ces antennes-relais sont désormais de nature à pouvoir capter des données, elles tomberont logiquement sous le coup de l'article R. 226-3 du code pénal ; mais cela aurait également pu être le cas pour les opérateurs et l'article R. 226-7.

Myriam MADORE évoque un autre désagrément qu'implique la décision du législateur : « *avec la 4G, l'ANSSI refuse que les opérateurs lui demandent un avis avant de procéder à un appel d'offre en vue d'acheter des équipements soumis à l'article R. 226-7. Pour l'ANSSI, le recours à cette procédure pourrait conduire à des atteintes au principe de libre concurrence, puisque les opérateurs n'achèteraient pas d'équipements s'ils ont de bonnes raisons de penser que l'autorisation de les exploiter leur serait refusée. Donc, dès qu'un nouvel*

[87] Alinéa 4, paragraphe I de l'article L. 34-11 du code des postes et des communications électroniques
[88] Alinéa 5, paragraphe 1 de l'article L. 34-11 du code des postes et des communications électroniques

appareil est en phase de conception, on sait qu'on devra attendre que celui-ci puisse être commercialisé (R. 226-3), avant de l'acheter, et très souvent l'ANSSI a du retard. Des logiciels qui permettraient d'améliorer les usages des consommateurs sont donc laissés de côté des mois après leur conception et jusqu'à ce qu'ils obtiennent l'autorisation R. 226-3. Même si les articles R. 226-3 et R. 226-7 ne sont pas corrélés dans la pratique, les opérateurs savent qu'il y a moins de risque de se voir refuser l'exploitation d'un équipement qui a déjà été contrôlé et autorisé. Avoir de la visibilité c'est essentiel dans un domaine comme le nôtre, puisqu'il implique des milliards d'euros d'investissement, pour des infrastructures qui doivent durer dans le temps et qui sont donc très onéreuses »[89]. Quels effets sur la politique d'achat des opérateurs pourraient donc découler de ce choix législatif ? Il est évident que cela risque de freiner leurs investissements, et donc ralentir inéluctablement le déploiement de la 5G sur le territoire. Cela pousse également les opérateurs a privilégié des équipementiers qui n'ont pas été visés par les débats portant sur la sécurité des réseaux, à l'image de Nokia et d'Ericsson, pourtant plus chers et en retard en terme d'innovation.

De plus, serait-il possible de voir le Premier ministre donner son aval à un opérateur pour l'exploitation d'un équipement, et refuser celle d'un opérateur concurrent pour le même équipement qui serait exploité dans une zone géographique similaire ? Ce risque est là encore bien présent d'après les opérateurs. En effet, d'après la loi 5G, la décision de refus du Premier ministre « *est motivée sauf lorsque la communication des motifs pourrait être de nature à porter atteinte à l'un des secrets ou intérêts protégés par les dispositions des a à f du 2° de l'article L. 311-5 du code des relations entre le public et l'administration* »[90]. D'après le code des relations entre le public et l'administration, la décision pourrait donc se passer de motivation lorsqu'elle risquerait de porter atteinte « *au secret des délibérations entre le Gouvernement et des autorités responsables relevant du pouvoir exécutif* », « *au secret de la défense nationale* », « *à la conduite de la politique extérieure de la France* » ou encore « *à la sécurité de l'Etat, à la sécurité publique, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations* »[91]. Or, compte tenu du fondement juridique de l'article L. 34-11 du code des postes et des communications électroniques, il devrait être assez rare d'obtenir des décisions de refus motivée ; ce qui entraîne un pouvoir conséquent de l'Administration sur le choix des équipementiers par les opérateurs. En l'état actuel de la loi, le Premier ministre pourrait très bien refuser toutes les demandes d'autorisation d'exploitation

[89] Myriam MADORÉ, (*op. cit.*)
[90] Alinéa 1er, article L. 34-12 du code des postes et des communications électroniques
[91] Alinéa 2, article L. 311-5 du code des relations entre le public et l'administration

d'un équipement Huawei sans avoir à motiver ses décisions. Une Administration centrale toute puissante dans un secteur économique aussi concurrentiel, qui plus est lorsqu'elle y détient des parts, est assez dommageable et critiquable.

L'article L. 34-12 permet d'en apprendre davantage à propos des critères que doit prendre en compte le Premier ministre pour refuser l'octroi d'une autorisation d'exploitation. La demande pourra ainsi ne pas être accordée par ce dernier « *s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale résultant du manque de garantie du respect des règles relatives à la permanence, à l'intégrité, à la sécurité, à la disponibilité du réseau, ou à la confidentialité des messages transmis et des informations liées aux communications* »[92]. Sur ce point, l'article est clair et n'apporte pas de révolution spécifique. Toutefois, son 2nd alinéa, qui précise quant à lui les paramètres qui permettront au Premier ministre et à l'ANSSI d'évaluer le risque qui pourrait justifier le refus d'autorisation, est davantage ambigu. Parmi certains critères peu surprenants, à l'image du « *niveau de sécurité des appareils* » ou des « *modalités de déploiement et d'exploitation envisagées par l'opérateur* », il est précisé que le Premier ministre tiendra compte du « *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* »[93]. Cette précision trahit une nouvelle fois les intentions du législateur. Bien qu'elle ne vise pas spécifiquement Huawei, et qu'elle conduise également à mettre en garde contre Cisco (qui aurait déjà laissé la NSA introduire des failles de sécurité dans ses équipements pas le passé, d'après l'affaire Snowden[94]), cette recommandation pousse forcément à apprécier Nokia et Ericsson, firmes finlandaise et suédoise, différemment. Si ces deux pays ne sont clairement pas les principaux responsables de cyberattaques ou de pratiques d'espionnage, il convient de rappeler ce que déclarait Agnès PANNIER-RUNACHER lors de son audition par la commission des affaires économiques du Sénat : « *on ne sait pas si aujourd'hui un pays avec lequel nous sommes alliés sera amené à changer de stratégie dans 10 ou 20 ans, ce texte est fait pour protéger nos réseaux de tout le monde* »[95]. Guillaume POUPARD le relevait également un mois auparavant sur France Inter « *le monde de l'espionnage ne s'arrête pas à nos ennemis* »[96]. Il semble donc

[92] Alinéa 1er, article L. 34-12 du code des postes et des communications électroniques
[93] Alinéa 2, article L. 34-12 du code des postes et des communications électroniques
[94] B. SNYDER : « *Snowden : the NSA planted backdoors in Cisco products* », Infoworld, 15 mai 2014, (https://www.infoworld.com/article/2608141/snowden--the-nsa-planted-backdoors-in-cisco-products.html), (consulté le 7 août 2019)
[95] Audition d'Agnès PANNIER RUNACHER (*op. cit.)*
[96] Intervention de Guillaume Poupard, patron de l'Agence nationale de sécurité des systèmes d'information : « *Entre les états, la guerre du futur se fera en partie sur Internet* », France Inter, le 15 avril 2019

étonnant de voir apparaître cette précision dans le texte final, d'autant que la France ne produit pas d'équipement de réseau ; le législateur n'aurait donc pas été tenté d'élaborer un texte discriminatoire. Il aurait donc été préférable de ne pas inscrire ce critère, et d'obliger l'ANSSI a considéré chaque équipement comme vecteur du même risque. C'est d'ailleurs ce que les sénateurs avaient préconisé de faire, puisque la mention « non membre de l'Union européenne » avait été remplacée par « étranger » dans le texte qu'ils avaient voté[97]. De plus, le Gouvernement n'a pas a dicté la politique d'achat des opérateurs, notamment au nom de la liberté d'entreprendre. Pourtant, le dispositif qu'il a prévu de mettre en place tend à conduire ces-derniers à favoriser certains équipementiers plutôt que d'autres, au détriment une nouvelle fois des consommateurs et de la libre concurrence.

C'est d'ailleurs l'un des arguments que reprenait Catherine PROCCACIA lorsqu'elle a présenté la version du texte modifié que le Sénat venait d'adopter, le 26 juin 2019. Après d'importantes campagnes de lobbying menées par les opérateurs et la Fédération Française des Télécoms, les sénateurs ont en effet apporté des modifications importantes au texte adopté par l'Assemblée nationale, permettant de le rééquilibrer. Catherine PROCCACIA et les sénateurs ont en effet été sensibles aux arguments des opérateurs, puisque lors de la présentation du texte de l'Assemblée nationale, amendé par la commission des affaires économiques, celle-ci a déclaré que « *en l'état, le texte pourrait risquer de ralentir les déploiements, de rehausser leur coût et de perturber le jeu de la concurrence entre équipementiers. Pire, il pourrait remettre en cause le service aux usagers, y compris sur la 4G* »[98]. Ces arguments sont, pratiquement mots pour mots, ceux développés par les opérateurs pour critiquer les effets de la loi 5G. Ainsi, certaines obligations, votées par les députés, ont disparu du texte amendé par les sénateurs.

S'agissant de l'atteinte à la liberté d'entreprendre et du risque pour les opérateurs de se voir dicter leur politique d'achat par le Gouvernement, le Sénat a décidé de supprimer un paramètre qui devait figurer dans le dossier de demande d'autorisation d'exploitation remis par les opérateurs. L'Assemblée nationale souhaitait que le périmètre géographique d'exploitation pour lequel l'autorisation était sollicitée soit mentionné dans le dossier[99], ce que les opérateurs

[97] Texte n° 120 (2018-2019), relatif à la proposition de loi visant à protéger les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, modifié par le Sénat le 26 juin 2019

[98] Sénat : « *Loi 5G : les sénateurs rééquilibrent le texte* », communiqué de presse, le 19 juin 2019, (https://www.senat.fr/presse/cp20190619.html), (consulté le 5 août 2019)

[99] Texte n° 257 (2018-2019), relatif à la proposition de loi visant à protéger les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, adopté par l'Assemblée nationale le 10 avril 2019

refusaient au nom de la liberté d'entreprendre. Il ressort des débats intervenus au Sénat, lors du vote en séance publique, que la rapporteur du texte, Catherine PROCCACIA, a repris les motifs invoqués par les opérateurs pour supprimer cette obligation, estimant que « *le Gouvernement n'a pas à dicter l'emplacement de chaque équipement que les opérateurs souhaitent exploiter* »[100]. Sur ce point, la commission mixte paritaire a donné raison aux sénateurs et les opérateurs ont donc eu gain de cause, puisque cette obligation de mention n'apparaît plus dans le texte finalement adopté. Selon Myriam MADORE, cette volonté initiale des députés fait échos à un événement survenu en octobre 2018, repris par un article de Challenges quelques mois plus tard : « *lors de l'inauguration de l'Altice Campus, en octobre, la direction a décidé de procéder à un test 5G grandeur nature et réalisé en conditions réelles. L'opération, baptisée « SFR allume la 5G », s'est déroulée à Balard, dans le Sud de Paris, à quelques dizaines de mètres du ministère des armées* »[101], sauf que l'armée n'a sûrement que très peu apprécié d'apprendre la survenance de ce test, puisqu' « *une règle tacite contraint les opérateurs à ne pas utiliser de matériel chinois en région parisienne, et jamais sur le cœur de réseau* »[102], ce qu'a pourtant décidé de faire SFR, cette opération ayant été réalisée au moyen d'appareils fournis par Huawei[103]. C'est très certainement cet événement qui a conduit le Gouvernement à vouloir contrôler le périmètre géographique d'exploitation des opérateurs. C'est en effet l'une des obligations qui était prévue par l'amendement inséré dans le projet de loi PACTE. Toutefois, à l'heure actuelle, le décret fixant « *les modalités d'octroi de l'autorisation, les conditions dont elle peut être assortie ainsi que la composition du dossier de demande d'autorisation* »[104] n'a pas encore été pris. Serait-il possible que les décideurs publics fassent de la mention du périmètre géographique d'exploitation l'une des mentions obligatoires que les opérateurs devront faire figurer au sein de leur dossier de demande d'autorisation d'exploitation ? La réponse devrait intervenir bien assez tôt, le décret étant attendu pour les prochains mois.

Les opérateurs ont critiqué un autre point du texte initialement voté par les députés : la rétroactivité de la mesure. Les députés sont en effet partis du constat que la 5G ne serait, dans un premier temps, qu'une 4G plus puissante prise en charge par les mêmes équipements de

---

[100] Catherine PROCACCIA, (*op. cit.*)
[101] Myriam MADORÉ, (*op.cit.*)
[102] G. FONTAINE : « *Espionnage : le grand dilemme des opérateurs télécoms face au chinois Huawei* », Challenges, le 24 janvier 2019, (https://www.challenges.fr/high-tech/telecoms/huawei-le-grand-dilemme-des-operateurs-telecoms_638566), (consulté le 31 mai 2019)
[103] Ibidem
[104] Alinéa 3, paragraphe II de l'article L. 34-12 du code des postes et des communications électroniques

réseau, qu'il convenait donc de contrôler. Le texte qu'ils avaient adopté le 10 avril 2019 prévoyait un article 3 qui précisait que le nouveau dispositif juridique tendait à s'appliquer à tous les équipements mentionnés à l'article 34-11 du code des postes et des communications électroniques « *installés depuis le 1er février 2019* »[105]. Il s'agissait là d'un véritable point de discorde avec les opérateurs, qui critiquait cette disposition sur deux points.

Premièrement, ceux-ci ont rappelé aux parlementaires et au Gouvernement qu'ils s'étaient engagés, dans le cadre du « New Deal Mobile », à apporter la 4G au sein de zones blanches (zones géographiques à très faible densité démographique), en respectant des délais ambitieux. Ce plan, passé entre le Gouvernement et les opérateurs le 14 janvier 2018, engage ces-derniers à couvrir des zones si peu peuplées qu'ils y perdent de l'argent compte tenu du volume d'investissement que cela implique. Demander aux opérateurs de formuler des demandes d'autorisation pour des équipements déjà installés conformément au droit en vigueur reviendrait à ralentir considérablement les déploiements. En effet, les équipements sont conçus pour ne pas être interopérables, de sorte qu'un appareil qui serait refusé par l'ANSSI pour des motifs allant au-delà de ses caractéristiques propres conduirait à démonter l'ensemble de l'antenne réseau, priver les usages de couverture mobile, réaliser une nouvelle demande d'exploitation, puis réinstaller une antenne conforme. Toutes ces étapes pour un équipement 4G, dont le cœur de réseau a déjà été contrôlé et dont les dispositifs situés en bords de réseau ne font porter aucun risque sur les réseaux radioélectriques. Cela aurait été un non-sens incroyable à l'heure où Julien DENORMANDIE est constamment interrogé sur les désagréments liés à une couverture mobile de mauvaise qualité sur le territoire[106].

Deuxièmement, l'application rétroactive du nouveau dispositif juridique aurait conduit les opérateurs à fournir un très grand nombre de dossiers de demande d'autorisation dans un court laps de temps, afin d'être certain que l'exploitation des équipements installés depuis le 1er février 2019 soit bien conforme aux attentes du Premier ministre. Cela aurait forcément eu pour effet d'engorger l'ANSSI, dont les délais de réponse sont déjà fortement critiqués par les opérateurs aujourd'hui. J'ai par exemple pu demander à Myriam MADORE ce qu'elle pensait du travail de cette autorité et de quel œil voyait-elle l'attribution de missions supplémentaires : « *la qualité du travail de l'ANSSI est reconnue ; aujourd'hui les cyberattaques sont constantes*

[105] Article 3 du texte n° 257 (2018-2019), relatif à la proposition de loi visant à protéger les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, adopté par l'Assemblée nationale le 10 avril 2019

[106] Question du député Yannick FAVENEC BECOT à Julien DENORMANDIE, séance de questions au Gouvernement de l'Assemblée nationale du 16 juillet 2019

et se complexifient chaque jour, ce qui pousse les membres de l'autorité à développer des méthodes d'analyse et de contrôle constamment différentes, à faire évoluer leur travail en fonction des mutations des menaces. Cela a un impact sur les délais et ce sont les opérateurs qui en sont lésés. Aujourd'hui on doit déposer une demande pour chaque équipement et chaque logiciel qui pourrait présenter un risque, et on doit redéposer un dossier de demande lorsqu'un logiciel n'est plus affecté aux mêmes équipements ou aux mêmes fonctions. En tout, chaque année, on doit réaliser des demandes pour 300 configurations différentes d'équipements et logiciels, qui sont valables pour 3 ans. Cela fait donc un grand nombre de dossiers a traité. Tellement que nous sommes parfois obligés d'avoir recours à des procédés proches du ridicule. Lorsque nous recevons des versions améliorées d'équipements déjà installés, nous réalisions des demandes d'autorisation pour pouvoir les exploiter, afin d'opérer un remplacement sur nos sites pour disposer d'un meilleur service. Pourtant, il arrive très régulièrement que nous soyons contraints d'envoyer également des demandes de renouvellement d'autorisation pour des équipements que l'on souhaiterait remplacer, mais l'ANSSI ne nous a pas encore octroyé l'autorisation d'exploiter nos équipements plus modernes. C'est ahurissant, cela contribue à engorger l'ANSSI puisqu'elle reçoit plus de demandes, pour des sites identiques. Mais si nous n'enverrions pas nos demandes de renouvellement, nous devrions cesser l'exploitation de l'équipement et rompre le signal, priver les usagers de leur connexion mobile. Car si nous poursuivons l'exploitation d'un équipement sans autorisation, nous risquons de devoir le démonter à nos frais en plus d'avoir une amende à payer. Il est compliqué d'imaginer comment l'ANSSI pourrait gérer des demandes supplémentaires, d'autant plus lorsqu'elles sont liées à de nouveaux appareils physiques et logiciels »[107].

Les sénateurs ont entendu ces remarques et ont insisté pour annuler l'effet rétroactif de la loi 5G. Les sénateurs ont donc inscrit le fait que l'article L. 34-11 du code des postes et des communications électroniques soit uniquement applicable aux appareils « *de cinquième génération et des générations ultérieures* » dans la lettre de la loi, et ce par deux fois[108]. Sur ce point également, les opérateurs télécoms ont obtenu gain de cause.

Le Sénat a également ajouté une disposition qui n'était pas défendue par les opérateurs, mais qui est pourtant essentielle dans le processus de rééquilibrage du texte : « *obliger le Premier ministre à proportionner sa décision aux conséquences qu'elle pourrait avoir sur les*

[107] Myriam MADORÉ, (*op. cit*.)
[108] Alinéa 1er, paragraphe I de l'article L. 34-11 du code des postes et des communications électroniques et alinéa 3, paragraphe I de l'article L. 34-11 du code des postes et des communications électroniques

déploiements et l'accès des usagers aux services »[109]. En droit, et en fait, il s'agit d'une garantie fondamentale supplémentaire contre l'arbitraire du Gouvernement pour les opérateurs téléphoniques. En effet, la loi 5G attribue au Premier ministre une prérogative puissante et exceptionnelle : la possibilité de refuser une demande d'exploitation, ce qui pousserait l'opérateur à revoir sa politique d'investissement (au moins sur la zone) et les usagers à se passer d'un service pourtant essentiel aujourd'hui. Il importe d'ailleurs de relever que lors d'une visite de l'Association des Maires Ruraux de France au siège de l'Altice Campus (siège social de SFR), en juillet 2019, ceux-ci avaient précisé que la couverture mobile des territoires ruraux était une priorité, puisque l'état du réseau était l'une des premières demandes des personnes souhaitant s'installer sur leurs communes. Dès lors, les sénateurs ont souhaité mesurer ce pouvoir du premier ministre, rééquilibrer les rapports de force en instaurant un principe de proportionnalité. Bien qu'il s'agisse d'un sujet relevant de la défense et de la sécurité nationale, un fondement qui permet généralement de prendre des mesures parmi les plus liberticides, le proportionner aux risques et conséquences qu'une décision de refus pourrait entraîner semble être un excellent garde-fou juridique. Cette obligation est désormais posée par l'alinéa 3 de l'article L. 34-12 : « *Un tel refus ne peut être décidé que si les risques de ralentissement du rythme de déploiement des appareils sur le territoire national, de renchérissement des coûts de ce déploiement et de remise en cause de l'accès des utilisateurs finaux aux services qui en résultent sont proportionnés au risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale* »[110]. Ce principe de proportionnalité devrait donc permettre d'éviter d'assister à des refus fondés sur un risque trop minime. Il permet, de plus, d'apporter des garanties et assurances supplémentaires au respect de la liberté d'entreprendre. Afin de laisser une certaine marge de manœuvre au Gouvernement, ce principe est corrélé à un autre apport des sénateurs : la possibilité d'assortir l'autorisation d'exploitation aux opérateurs visés par l'article L. 34-11 à des conditions[111]. Il paraît opportun d'ajouter un « oui mais », ce qui limitera inéluctablement les cas de refus. Sur ce point, les sénateurs ont réalisé un travail remarquable, rééquilibrant considérablement le texte initialement voté par les députés.

Dans un tout autre esprit, les opérateurs réclamaient davantage de simplification en ce qui concerne l'articulation entre les articles R. 226-3 et L. 34-11. Les sénateurs ont une nouvelle fois été réceptifs à cette demande, puisqu'ils ont inséré un article qui n'était pas prévu par le dispositif élaboré par l'Assemblée nationale. L'article 4 de la loi 5G complète ainsi l'article R.

[109] Sénat, (*op. cit*.)
[110] Alinéa 3 de l'article L. 34-12 du code des postes et des communications électroniques
[111] Alinéa 2, paragraphe II de l'article L. 34-12 du code des postes et des communications électroniques.

226-3 par ces mots : « *Le présent article n'est pas applicable à la détention ou à l'acquisition par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, des appareils soumis à une autorisation du Premier ministre en application de la section 7 du chapitre II du titre Ier du livre II du code des postes et des communications électroniques* »[112]. En fusionnant deux régimes d'autorisation, les sénateurs simplifient effectivement le travail des opérateurs mais aussi celui de l'ANSSI. Les opérateurs peuvent donc une nouvelle fois se réjouir de l'impact positif de leurs stratégies d'influence.

Enfin, attentifs aux arguments développés par les opérateurs, les sénateurs ont tenu à s'assurer que cette proposition de loi n'entrave pas le rythme des déploiements sur le territoire. Ils ont donc fait paraître dans la loi l'obligation, pour le Gouvernement, de leur fournir un rapport annuel analysant « *les impacts de ce régime sur les opérateurs et l'ensemble de leurs prestataires et sous-traitants, sur le rythme et le coût des déploiements des équipements de quatrième et cinquième générations sur l'ensemble du territoire, sur l'accès des usagers aux services de communications électroniques rendus grâce aux réseaux radioélectriques mobiles et évalue le nombre d'appareils n'ayant pas pu être installés ou ayant dû être retirés à la suite d'une décision de refus* »[113]. Cette dernière modification substantielle du texte apportera aux parlementaires le recul nécessaire afin d'observer et analyser les effets de cette loi sur l'activité des opérateurs, dont ces-derniers n'ont eu de cesse de critiquer les dispositions. Ce texte apparaît alors comme un compromis, que la sénatrice PROCCACIA résume par ces mots : « *il faut rehausser le niveau de sécurité des réseaux en raison des usages critiques que permettra la 5G. Mais il ne faut pas que cette exigence se fasse au détriment des usagers, en particulier des entreprises, qui seront la première cible de la 5G. En somme, nous entendons éviter que le Gouvernement ne dévie de la trajectoire qu'il s'est fixée dans sa feuille de route sur la 5G* »[114].

[112] Article 4 de la Loi n° 2019-810, 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 du 1er août 2019 parue au JO n° 0178 du 2 août 2019

[113] Article 5 de la Loi n° 2019-810, 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 du 1er août 2019 parue au JO n° 0178 du 2 août 2019

[114] Catherine PROCACCIA, (*op. cit.*)

CONCLUSION

Entre potentialités économiques et risques inédits, la technologie 5G divise les différentes parties prenantes quant au traitement qu'il convient de lui apporter. Ce nouveau standard est très attendu par les usagers, qu'ils soient industriels ou simples consommateurs, les opérateurs, mais aussi par certains ministères. La 5G promet ainsi de nouveaux usages (télémédecine, agriculture connectée), le développement de nouveaux écosystèmes économiques (véhicules autonomes, industrie intelligente), un nombre incroyable de potentialités, et partant, de nombreuses retombées économiques. Avec un débit multiplié par 100, un temps de latence divisé par 10 et une capacité de connectivité beaucoup plus importante, la 5G devrait pouvoir préparer le terrain de l'ère de l'Internet des objets. En offrant de nouvelles opportunités, comme la possibilité de diviser le réseau en tranches qui seront affectées à des activités spécifiques, la 5G est annonciatrice de grands bouleversements pour le quotidien de chacun. Toutefois, de par son architecture, la 5G s'accompagne également de vulnérabilités et de risques nouveaux qui pèsent sur la résilience des réseaux. A l'heure où les cyberattaques se multiplient, protéger les intérêts de la défense et de la sécurité nationale de l'Etat est fondamental afin d'assurer la souveraineté de la France dans le cyberespace mais aussi dans le monde. De plus, l'importance du numérique dans notre société interconnectée devrait continuer à croître en même temps que la 5G amplifiera son emprise sur notre quotidien. Dès lors, s'assurer que les réseaux et systèmes d'information fonctionnent en continu et qu'ils ne subissent ni panne ni dysfonctionnement est un enjeu prioritaire de défense et de sécurité nationale.

Certes, des dispositifs juridiques relatifs à la mise sur le marché des équipements réseaux et leur exploitation par les opérateurs existaient déjà et semblaient adaptés au déploiement de la 5G sur le territoire. Néanmoins, la virtualisation et la multiplication des réseaux entraîneront des risques supplémentaires qui ont conduit le Gouvernement a changé de paradigme juridique. Initialement fondé sur la protection du secret des correspondances, le nouveau régime mis en place par la loi 5G repose désormais sur des motifs de défense et de sécurité nationale.

Compte tenu de la rupture que devrait entraîner la 5G, il était logiquement nécessaire d'adapter le cadre juridique. Toutefois, en réagissant dans la précipitation aux campagnes d'influences américaines, les décideurs publics ont mis au point une première version imparfaite et incomplète de la loi, qui ne tenait pas compte des contraintes auxquelles sont

confrontées les opérateurs et qui risquait de léser les industriels français dans cette course technologique. Il aura fallu que les opérateurs réalisent de vastes actions de lobbying pour que le texte soit finalement rééquilibré par les sénateurs puis adopté en commission mixte paritaire.

Certains opérateurs, selon les dires de Myriam MADORE, directrice des obligations légales de SFR, ont néanmoins fait part de leur intention de saisir le juge constitutionnel afin de faire annuler cette proposition de loi, au moins en partie, qu'ils jugent beaucoup trop attentatoire à leur liberté d'entreprendre et leur liberté contractuelle. Sans avoir la prétention de répondre au nom du Conseil constitutionnel, il y a de fortes chances pour que ce recours n'aboutisse pas en raison du principe de proportionnalité inséré dans la loi par les sénateurs. Toutefois, le décret d'application qui précisera le contenu des dossiers de demande d'autorisation des opérateurs télécoms n'a pas encore été pris, c'est pourtant ce texte qui permettra de saisir l'ambition réelle du Gouvernement : garantir la sécurité des réseaux sans distinction quant à l'origine des équipementiers et de leurs sous-traitants, ou priver Huawei du marché français.

Le déploiement de la 5G est également vecteur d'un autre débat sécuritaire, touchant cette fois-ci à la santé. Cette technologie fonctionnera en effet différemment par rapport aux précédentes générations de standard de communication, notamment et principalement en raison des fréquences qu'elle utilisera, et qui seront orientées directement vers les terminaux mobiles. Afin d'envoyer ses ondes 5G, il conviendra d'avoir recours à de nouvelles antennes-relais intelligentes qui seront installées massivement dans le mobilier urbain[115]. Ce sont ces hautes fréquences qui font polémique, puisque le Gouvernement et les agences sanitaires ne disposent pas, aujourd'hui, d'étude scientifique sur le sujet. L'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) a été chargée d'une mission sur le sujet par le Gouvernement[116], mais elle n'a pas encore rendu ses conclusions. Néanmoins, 170 scientifiques provenant de 37 pays différents ont signé une pétition commune afin de demander un moratoire sur la 5G[117]. Une nouvelle loi pourrait intervenir sur ce point et conduire l'Agence nationale des Fréquences à prévoir de nouvelles limites d'expositions du public aux ondes s'il s'avère que celles-ci créent des risques et des vulnérabilités supplémentaires sur la santé des Hommes, cette fois-ci.

---

[115] C. LEMKE : « La 5G est-elle dangereuse pour la santé », Sciences et Avenir, le 1er juillet 2019, (https://www.sciencesetavenir.fr/high-tech/reseaux-et-telecoms/5g-et-danger-pour-la-sante-l-article-pour-tout-comprendre_135033), (consulté le 12 août 2019)

[116] O. MONOD : « Le développement de la 5G est-il dangereux pour la santé ? », Libération, le 15 février 2019

[117] Ibidem

ANNEXES

Annexe n°1 :

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

Tableau 1 - Extrait Rapport n° 579 (2018-2019) de Mme Catherine PROCACCIA, déposé le 19 juin 2019

Annexe n°2 :

Entretien réalisé avec M. François VINCENT, ingénieur auprès de la Direction de l'Ingénierie Mobile de SFR, le 12 juillet 2019 au siège social d'Altice France :

Maxence CHALLUT : **Quels domaines profiteront des nouveaux usages permis par la 5G** ?

François VINCENT : On parle beaucoup de « Smart City » mais c'est un terme fourre-tout. Concrètement, la 5G va permettre aux objets d'interagir avec nos terminaux et d'autres objets du quotidien avec une latence très faible, cela développera énormément d'usages liés au développement des villes mais aussi de l'Industrie, ou de n'importe quelle activité économique. Aujourd'hui la 5G apparaît, par exemple, comme un bon moyen de réduire et réguler notre consommation énergétique. Après j'entends parler de taxis volants ou de téléchirurgie régulièrement ; il convient de rappeler que le survol de Paris est interdit, par exemple, et qu'une opérattion de téléchirurgie peut être réalisée grâce à la Fibre.

M-C : **Pourquoi la 5G est-elle annoncée comme une technologie de rupture en matière de potentialités économiques et en termes de risques et vulnérabilités ?**

F-V : On dit que la 4G a permis de connecter les hommes ; la 5G permettra de connecter les objets entre eux. Il y a ce fantasme des nouveaux usages ainsi que des risques inhérents aux infrastructures physiques et logiciels de la 5G qui sont exagérés. Pour les 5 prochaines années, ce que l'on appellera 5G ne sera qu'une montée en débit de la 4G, une sorte de 4,5G. Donc les usages que l'on promet mettront du temps avant d'être développés et les menaces que l'on attend mettront du temps avant d'être réelles. Finalement, c'est la 6G qui bouleversera notre quotidien, la 5G est une génération passerelle.

M-C : **Selon vous, quelles sont les améliorations que met en place la proposition de loi 5G par rapport à la sécurité des réseaux ?**

F-V : il y a des risques réels, mais c'est davantage un choix qui dépend de l'environnement géopolitique actuel. En effet, sur le fond, la 5G, dans sa phase initiale (2020-2025) ne sera que très peu différente de la 4G. Il s'agira simplement d'une 4G plus performante en termes de débit mais la partie sensible, le cœur de réseau, restera la même. En France, aucun équipement Huawei n'a jamais eu accès au cœur de réseau car c'est l'ANSSI qui décide déjà. Cette nouvelle loi ne répond pas à des nouvelles vulnérabilités, en tout cas pour le moment, car ce sont les mêmes que pour la 4G actuellement.

M-C : **A travers vos connaissances et votre expérience dans les télécoms, quels sont les avantages et inconvénients de ce nouveau dispositif ?**

F-V : Ce dispositif est complet, il faut le relever, mais trop contraignant par rapport à l'objectif poursuivi et à la réalité des risques. Le contexte actuel impose de garantir la résilience des réseaux, et cet impératif ne peut qu'aller en s'accentuant dans le futur, je pense donc qu'il était primordial qu'on dispose d'un texte précis. Nous avons besoin de visibilité compte tenu des investissements que cela implique, et sur ce point c'est une bonne chose que la loi soit sortie avant la mise aux enchères des fréquences. Mais le Gouvernement semble dire : « n'achetez pas un équipement non-européen même s'il est moins cher ou plus performant. Achetez européen, les équipements seront plus sûrs ». De ce point de vue la loi est très critiquable, parce qu'elle va entraver nos activités alors qu'elle semble être une simple réponse politico-diplomatique sur certains points.

Annexe n°3 :

Entretien avec Mme Myriam Madoré, Directrice des obligations légales de SFR, le 30 juillet 2019 au siège social d'Altice France :

Maxence CHALLUT : **Pouvez-vous revenir sur le dispositif mis en place par l'article R. 226-3 du code pénal, ainsi que les modalités de son application ?**

Myriam MADORÉ : Lorsqu'ils souhaitent accéder au marché français, les équipementiers doivent formuler une demande d'autorisation auprès de l'ANSSI. Si celle-ci est acceptée par le Premier ministre, après avis de l'Autorité, elle sera valable pour une durée de 6 ans (R. 226-3). Les opérateurs, lorsqu'ils souhaitent acquérir des équipements réseaux en vue de les déployer, s'assurent que Huawei, Nokia ou Ericsson possèdent bien la certification leur permettant de vendre leurs dispositifs. Une fois l'appareil acheté, les opérateurs déposent eux aussi une demande auprès de l'ANSSI pour pouvoir l'exploiter, c'est-à-dire le déployer (R. 226-7). L'autorisation délivrée aux opérateurs par le Premier ministre vaut quant à elle pour 3 ans. Ce cadre juridique est complet puisque le Gouvernement à la main sur chaque étape du processus, ce qui lui permet de s'assurer de la fiabilité des dispositifs à tout moment. Aujourd'hui, avec la 4G, Huawei n'a déjà pas accès aux cœurs de réseaux sur le fondement de cet article. Modifier cette procédure, alors que les opérateurs, les équipementiers et l'ANSSI la maîtrisent est un non-sens.

M-C : Justement, pourquoi avoir modifié ce dispositif s'il était complet ?

M-M : Je pense qu'il y a une grosse part de fantasme, due aux prises de position américaines et au contexte géopolitique actuel. Un événement qui s'est déroulé sur le territoire national a aussi conduit le Premier ministre à s'intéresser à la question. Lors de l'inauguration de l'Altice Campus, en octobre, la direction a décidé de procéder à un test 5G grandeur nature et réalisé en conditions réelles. L'opération, baptisée « SFR allume la 5G », s'est déroulée à Balard, dans le Sud de Paris, à quelques dizaines de mètres du ministère des armées… Dès le lendemain la question de laisser Huawei avoir accès aux réseaux 5G était posée.

M-C : Selon vous, la proposition de loi 5G apporte-t-elle des garanties supplémentaires en termes de sécurité ?

M-M : Non, c'est une surcharge administrative. Il faut savoir que le champ d'application du dispositif actuel va être étendu pour prendre en compte tous les équipements 5G d'ici 2021 (les antennes-relais seront comprises). La loi 5G vient dire la même chose mais plus tôt. Le Gouvernement répond que la 5G aura déjà commencé à être déployée quand le dispositif fondé sur la protection du secret des correspondances sera élargi, mais à ce moment-là les équipements 5G ne seront pas encore déployés, on utilisera encore les mêmes équipements réseau 4G qu'aujourd'hui. C'est une posture gouvernementale prise dans l'urgence, elle comporte donc beaucoup de failles.

M-C : **Pouvez-vous revenir plus en détail sur ces failles justement ?**

M-M : Avec la 4G, l'ANSSI refuse que les opérateurs lui demandent un avis avant de procéder à un appel d'offre en vue d'acheter des équipements soumis à l'article R. 226-7. Pour l'ANSSI, le recours à cette procédure pourrait conduire à des atteintes au principe de libre concurrence, puisque les opérateurs n'achèteraient pas d'équipements s'ils ont de bonnes raisons de penser que l'autorisation de les exploiter leur serait refusée. Donc, dès qu'un nouvel appareil est en phase de conception, on sait qu'on devra attendre que celui-ci puisse être commercialisé (R. 226-3), avant de l'acheter, et très souvent l'ANSSI a du retard. Des logiciels qui permettraient d'améliorer les usages des consommateurs sont donc laissés de côté des mois après leur conception et jusqu'à ce qu'ils obtiennent l'autorisation R. 226-3. Même si les articles R. 226-3 et R. 226-7 ne sont pas corrélés dans la pratique, les opérateurs savent qu'il y a moins de risque de se voir refuser l'exploitation d'un équipement qui a déjà été contrôlé et autorisé. Avoir de la visibilité c'est essentiel dans un domaine comme le nôtre, puisqu'il implique des milliards d'euros d'investissement, pour des infrastructures qui doivent durer dans le temps et qui sont donc très onéreuses.

M-C : **Vous venez de parler de l'ANSSI, avec qui vous travaillez régulièrement justement. Que pensez-vous de la charge supplémentaire de travail qui pèsera sur cette Agence, et de sa capacité à mener à bien ses nouvelles missions ?**

M-M : La qualité du travail de l'ANSSI est reconnue ; aujourd'hui les cyberattaques sont constantes et se complexifient chaque jour, ce qui pousse les membres de l'autorité à développer des méthodes d'analyse et de contrôle constamment différentes, à faire évoluer leur travail en fonction des mutations des menaces. Cela a un impact sur les délais et ce sont les opérateurs qui en sont lésés. Aujourd'hui on doit déposer une demande pour chaque équipement et chaque logiciel qui pourrait présenter un risque, et on doit redéposer un dossier de demande lorsqu'un logiciel n'est plus affecté aux mêmes équipements ou aux mêmes fonctions. En tout, chaque année, on doit réaliser des demandes pour 300 configurations différentes d'équipements et logiciels, qui sont valables pour 3 ans.

Cela fait donc un grand nombre de dossiers a traité. Tellement que nous sommes parfois obligés d'avoir recours à des procédés proches du ridicule. Lorsque nous recevons des versions améliorées d'équipements déjà installés, nous réalisions des demandes d'autorisation pour pouvoir les exploiter, afin d'opérer un remplacement sur nos sites pour disposer d'un meilleur service. Pourtant, il arrive très régulièrement que nous soyons contraints d'envoyer également des demandes de renouvellement d'autorisation pour des équipements que l'on souhaiterait remplacer, mais l'ANSSI ne nous a pas encore octroyé l'autorisation d'exploiter nos équipements plus modernes. C'est ahurissant, cela contribue à engorger l'ANSSI puisqu'elle reçoit plus de demandes, pour des sites identiques. Mais si nous n'enverrions pas nos demandes de renouvellement, nous devrions cesser l'exploitation de l'équipement et rompre le signal, priver les usagers de leur connexion mobile. Car si nous poursuivons l'exploitation d'un équipement sans autorisation, nous risquons de devoir le démonter à nos frais en plus d'avoir une amende à payer. Il est compliqué d'imaginer comment l'ANSSI pourrait gérer des demandes supplémentaires, d'autant plus lorsqu'elles sont liées à de nouveaux appareils physiques et logiciels.

M-C : **Les textes qui permettront à la loi d'entrer en vigueur n'ont pas encore été pris, que redoutez-vous ?**

M-M : Honnêtement je ne sais pas. C'est à ce moment-là que l'on comprendra quelles étaient les réelles motivations du Gouvernement. Il y a des risques, notamment qu'aucune demande d'exploitation d'un équipement Huawei n'aboutisse, et que le Gouvernement ne motive pas sa décision en se cachant derrière la protection du secret de la défense nationale. Néanmoins, certains opérateurs ont déjà demandé à des professeurs de droit constitutionnel de s'intéresser à la question, notamment sur l'aspect disproportionné de la mesure par rapport à l'atteinte aux libertés d'entreprendre et de contracter, mais je ne peux pas approfondir le sujet.

LEXIQUE

Par ordre chronologique d'apparition :

- Cinquième génération de standards de télécommunications mobiles (5G)
- Autorité de régulation des communications électroniques et des potes (Arcep)
- Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Secrétariat Général de la Défense et de la Sécurité nationale (SGDSN)
- Opérateur d'importance vitale (OIV)
- Service Interministériel Régional des Affaires civiles et Economiques de Défense et de la Protection Civile (SIRACED-PC)
- Politique de sécurité des systèmes d'information (PSSI)

TABLE DES MATIÈRES

BIBLIOGRAPHIE

❖ LOIS ET AMENDEMENTS :

- Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale
- Amendement n°874 du projet de loi sur la croissance et la transformation des entreprises, déposé par le Gouvernement le 25 janvier 2019
- Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, enregistrée à la Présidence de l'Assemblée nationale le 20 février 2019
- Loi n° 2019-810, 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 du 1er août 2019 parue au JO n° 0178 du 2 août 2019

❖ DÉCRETS ET ARRÊTÉS :

- Décret n°2009-834, portant création de l'Agence nationale de sécurité des systèmes d'information, pris le 7 juillet 2009
- Annexe 1 de l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévues par l'article 226-3 du code pénal
- Article 1 de l'arrêté du 11 août 2016 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal
- Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Communications électroniques et Internet » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense

- Annexe 1 de 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 » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense

❖ ARTICLES DE LOI :

- Code de la défense :

- Article L. 1332 du code de la défense

- Code pénal :

- Article R. 226-2 du code pénal
- Article R. 226-3 du code pénal
- Article R. 226-7 du code pénal
- Article R. 226-15 du code pénal

- Code des postes et des communications électroniques :

- Article L. 33-14 du code des postes et des communications électroniques
- Article L. 34-11 du code des postes et des communications électroniques
- Article L. 34-12 du code des postes et des communications électroniques

- Code des relations entre le public et l'administration :

- Article L. 311-5 du code des relations entre le public et l'administration

❖ ACTIVTÉS PARLEMENTAIRES :

▪ RAPPORTS PARLEMENTAIRES ET TRAVAUX PRÉPARATOIRES :

- Rapport d'information n°1017 (2018-2019) de MM Alexandre FRESCHI et André CHASSAIGNE, fait au nom de la commission des affaires européennes, déposé le 31 mai 2018
- Rapport n° 1832 de M. Eric BOTHOREL, fait au nom de la commission des affaires économiques, déposé le 3 avril 2019
- Texte n° 257 (2018-2019), relatif à la proposition de loi visant à protéger les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, adopté par l'Assemblée nationale le 10 avril 2019
- Avis n° 569 (2018-2019) de M. Pascal ALLIZARD, fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat, déposé le 12 juin 2019
- Rapport n°579 (2018-2019) de Mme Catherine PROCACCIA, fait au nom de la commission des affaires économiques du Sénat, déposé le 19 juin 2019
- Texte n° 120 (2018-2019), relatif à la proposition de loi visant à protéger les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, modifié par le Sénat le 26 juin 2019

▪ AUDITIONS PARLEMENTAIRES :

- Audition de Sébastien Soriano, Président de l'Autorité de régulation des communications électroniques et des postes, par la commission des affaires économiques du Sénat, en date du 10 avril 2019
- Audition d'Agnès Pannier-Runacher, Secrétaire d'Etat auprès du ministre de l'économie et des finances, par la commission des affaires économiques du Sénat sur la proposition de loi visant à préserver les intérêts de la défense et de

la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques, le 4 juin 2019

- Audition des dirigeants de Huawei France par la commission d'enquête du Sénat sur la souveraineté numérique de la France, le 18 juillet 2019
- Audition de Cédric O, Secrétaire d'Etat au numérique auprès du ministre de l'économie, par la commission de la culture, de l'éducation et de la communication du Sénat, le 24 juillet 2019

  - QUESTIONS AU GOUVERNEMENT :

- Questions relatives à la politique du Gouvernement sur le maintien des services publics sur le territoire, le 29 avril 2019, à l'Assemblée national
- Question du député Yannick Favenec Becot à Julien Denormandie, séance de questions au Gouvernement de l'Assemblée nationale du 16 juillet 2019

❖ PUBLICATIONS OFFICIELLES :

- Open Source Center : « *Huawei Annual Report Details Directors, Supervisory Board for First Time* », rapport annuel, présenté le 5 octobre 2011, (https://fas.org/irp/dni/osc/huawei.pdf), consulté le 26 juin 2019
- Ministère de la défense, le Livre Blanc sur la Défense et la sécurité nationale, présenté le 29 avril 2013
- Ministère des Solidarités et de la Santé : « *Présentation du plan pour l'égal accès aux soins dans les territoires* », présenté le 13 octobre 2017
- Anne-Marie IDRAC : « *Développement des véhicules autonomes : Orientations stratégiques pour l'action publique* » rapport commandé par le Gouvernement français, présenté le 14 mai 2018
- Autorité de régulation des communications électroniques et des postes : « *5G, une feuille de route ambitieuse pour la France* », présenté le 16 juillet 2018
- Huawei cybersecurity evaluation centre oversight board, rapport annuel de 2018, présenté en janvier 2019, https://www.gov.uk/government/publications/huawei-cyber-security-

evaluation-centre-oversight-board-annual-report-2019), consulté le 4 juillet 2019

- Institut national de la statistique et des études économiques, présentation du tableau de l'économie française, présenté en janvier 2019
- World Intellectual Property Organization (Organisation mondiale de la propriété intellectuelle) : « *2018 Annual report on the number of technology patents filed worldwilde* », rapport annuel, présenté en janvier 2019, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2018.pdf), consulté le 2 avril 2019
- Agence nationale de la sécurité des systèmes d'information, rapport annuel d'activité pour l'année 2018, présenté le 15 avril 2019

❖ ETUDES :

- J.C Mallet : « *Défense et sécurité nationale. Le livre blanc* », Paris, O. Jacob/Éd. La documentation française, le livre blanc de 2008
- P. HART : « *5G : The twelve trillion dollar technology* », étude réalisée pour ISH Markit, le 3 mai 2017, (https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf), consulté le 18 mai 2019
- Arthur D. Little : « L'économie des Télécoms en 2018 », étude réalisée pour la Fédération Française des Télécoms, publiée en décembre 2018, (https://www.fftelecoms.org/app/uploads/2018/12/etude_arthur_d_little_fftelecoms_2018_.pdf), consulté le 1er avril 2019
- M. DUCHATEL & F. GODEMENT : « *L'Europe et la 5G : le cas Huawei* », étude réalisée pour l'Institut Montaigne, mai 2019, (https://www.institutmontaigne.org/publications/leurope-et-la-5g-le-cas-huawei-partie-2), consulté le 9 juin 2019

❖ ARTICLES ET COMMUNIQUES DE PRESSE :

- L. LAM et S. CHEN : « *Snowden reveals more US cyberspying details* », South China Morning Post, le 22 juin 2013, ((https://www.scmp.com/news/hong-

kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed), consulté le 10 avril 2019

- L. POITRAS : « *How the NSA targets Germany and Europe* », Der Spiegel, le 1er juillet 2013, (https://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html), consulté le 10 avril 2019
- B. SNYDER : « *Snowden : the NSA planted backdoors in Cisco products* », Infoworld, 15 mai 2014, (https://www.infoworld.com/article/2608141/snowden--the-nsa-planted-backdoors-in-cisco-products.html), consulté le 7 août 2019
- E. POURNARAS & D. HELBING « *Society : Build a digital democracy* », 2 novembre 2015, Nature n°527, pages 33-34
- S. SALINABAS : « *Six top US intelligence chiefs caution against buying Huawei phones*», CNBC, le 13 février 2018, (https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html), consulté le 10 mai 2019
- P-Y. DUGUA : « *Les Etats-Unis ferment le marché des télécoms aux chinois* », Le Figaro, le 18 avril 2018
- S.N. : « *Huawei and ZTE handed 5G network ban in Australia* », BBC News, le 23 août 2018, (https://www.bbc.com/news/technology-45281495), consulté le 1er mai 2019
- A. CLAPAUD : « *NotPetya : Saint-Gobain tire la leçon et s'arme d'intelligence artificielle* », Industrie&Technologies, le 12 octobre 2018, (https://www.industrie-techno.com/article/notpetya-saint-gobain-tire-la-lecon-et-s-arme-d-intelligence-artificielle.53974), consulté le 8 août 2019
- KPN : « *Shell and partners test industrial 5G applications in the port of Rotterdam* », communiqué de presse interne mis en ligne le le 6 novembre 2018, (https://overons.kpn/en/news/2018/kpn-shell-and-partners-test-industrial-5g-applications-in-the-port-of-rotterdam), consulté le 6 mai 2019
- O. SHAOXIA : « *5G network remote animal surgery succesfully implemented in Fuzhou* », Technology-Info, le 10 janvier 2019, (https://technology-

info.net/index.php/2019/01/10/5g-network-remote-animal-surgery-successfully-implemented-in-fuzhou/) , consulté le 6 mai 2019

- J. PLUCINSKA & K. WITENBERG : « *Poland arrests Huawei employee, Polish man on spying allegations* », Reuters, le 11 janvier 2019, (https://www.reuters.com/article/us-poland-security/poland-arrests-huawei-employee-polish-man-on-spying-allegations-idUSKCN1P50RN), consulté le 16 mai 2019
- D. STRUMPF & AL. « *Huawei Targeted in U.S. Criminal Probe for Alleged Theft of Trade Secrets* », The Wall Street Journal, le 16 janvier 2019
- G. FONTAINE : « *Espionnage : le grand dilemme des opérateurs télécoms face au chinois Huawei* », Challenges, le 24 janvier 2019, (https://www.challenges.fr/high-tech/telecoms/huawei-le-grand-dilemme-des-operateurs-telecoms_638566), consulté le 31 mai 2019
- G. JACQUOT : « *5G : heurté par la méthode, le Sénat rejette « l'amendement anti-Huawei » du Gouvernement* », Public Sénat, le 7 février 2019, (https://www.publicsenat.fr/article/parlementaire/5g-heurte-par-la-methode-le-senat-rejette-l-amendement-anti-huawei-du), consulté le 12 avril 2019
- S. DUMOULIN : « *Huawei : les Etats-Unis mettent la pression sur l'Europe* », Les Echos, le 12 février 2019 (https://www.lesechos.fr/tech-medias/hightech/huawei-les-etats-unis-mettent-la-pression-sur-leurope-963897), consulté le 20 mai 2019
- O. MONOD : « Le développement de la 5G est-il dangereux pour la santé ? », Libération, le 15 février 2019
- G. KE et Y. LIU : « La Chine exhorte à une compréhension complète et correcte de sa loi sur le renseignement », French People Daily, le 20 février 2019, (http://french.peopledaily.com.cn/Chine/n3/2019/0220/c31354-9547791.html), consulté le 1er mai 2019
- S.N. « *China performs first 5G-based remote surgery on human brain* », Chinay Daily, le 18 mars 2019, (http://www.chinadaily.com.cn/a/201903/18/WS5c8f0528a3106c65c34ef2b6.html), consulté le 6 mai 2019

- J-M. DUFOUR : « *Pourquoi Huawei peut gagner la bataille technologique* », France Inter, le 19 mars 2019
- Intervention de Guillaume Poupard, patron de l'Agence nationale de sécurité des systèmes d'information : « *Entre les états, la guerre du futur se fera en partie sur Internet* », France Inter, le 15 avril 2019
- J. DELEPINE : « *Huawei : la guerre technologique est déclarée* », Alternatives économiques, édition de mai 2019, n°390, pp 67-69
- S. DUMOULIN : « *Le monde fabuleux de la 5G* », Les Echos, le 05 mai 2019, (https://weekend.lesechos.fr/business-story/innovation/0600742311487-le-monde-fabuleux-de-la-5g-2247013.php), consulté le 20 mai 2019
- E. BEMBARON : « *Les opérateurs télécoms français veulent faire payer les géants du net* », Le Figaro, le 22 mai 2019
- O. LASCAR : « *AgriTech : le numérique pour révolutionner l'agriculture* », Sciences et Avenir, le 23 mai 2019, (https://www.sciencesetavenir.fr/high-tech/sommet-start-up/agritech-le-numerique-pour-revolutionner-l-agriculture_133905), consulté le 10 juin 2019
- Sénat : « *Loi 5G : les sénateurs rééquilibrent le texte* », communiqué de presse, le 19 juin 2019, (https://www.senat.fr/presse/cp20190619.html), consulté le 5 août 2019
- S. Le BELZIC : « *Ren Zhengfei, l'œil de Pékin* », l'Express, numéro du 20 juin 2019, pp 84-87
- C. LEMKE : « La 5G est-elle dangereuse pour la santé », Sciences et Avenir, le 1er juillet 2019, (https://www.sciencesetavenir.fr/high-tech/reseaux-et-telecoms/5g-et-danger-pour-la-sante-l-article-pour-tout-comprendre_135033) consulté le 12 août 2019
- M. RASCAN : « *Le CETA, controversé accord de libre-échange avec le Canada, approuvé à l'Assemblée* », Le Monde, le 23 juillet 2019
- A. BOXALL : « *How the Monaco Grand Prix inspired the country to win the 5G race* », Digital Trends, le 27 juillet 2019, (https://www.digitaltrends.com/mobile/5g-in-monaco-with-huawei-interview/), consulté le 1er août 2019

- A. ROBERT : « *Loi 5G : « ce n'est pas une loi anti-Huawei » selon la sénatrice Catherine Procaccia* », CNET, le 29 juillet 2019, https://www.cnetfrance.fr/news/loi-5g-ce-n-est-pas-une-loi-anti-huawei-selon-la-senatrice-catherine-procaccia-39888471.htm), consulté le 2 mai 2019

❖ DISCOURS :

- Extrait du discours prononcé par David Cameron, ancien Premier Ministre du Royaume-Uni, à la tribune du Centrum für Büroautomation, Informationstechnologie und Telekommunikation (CeBIT), le 9 mars 2014, à Hanovre
- Extrait du discours de Börje Ekholm au World Economic Forum : « *How 5G could speed up global growth ?* », le 12 janvier 2018, à Davos
- Discours d'ouverture de Richard FERRAND, Président de l'Assemblée nationale, « Lobbying : quelle place et quels enjeux pour la démocratie ? », colloque organisé par Sylvain WASERMAN, Vice-président de l'Assemblée nationale, au titre de la délégation chargée des représentants d'intérêts et des groupes d'études, les 15 et 16 mai 2019

❖ ENTRETIENS :

- Entretien réalisé avec M. François VINCENT, ingénieur auprès de la Direction de l'Ingénierie Mobile de SFR, le 12 juillet 2019 au siège social d'Altice France
- Entretien avec Mme Myriam MADORÉ, Directrice des obligations légales de SFR, le 30 juillet 2019 au siège social d'Altice France