Contexte réglementaire pour les opérateurs 5G

Franck Laurent[1] et Pascal Nourry[2]

[1] Juriste, Orange SA, franck1.laurent@orange.com
[2] Ingénieur, Orange SA, pascal.nourry@orange.com

Résumé. La virtualisation des réseaux est perçue comme étant une rupture technologique par le législateur, notamment dans le contexte de la 5G. A travers la nouvelle loi "5G"[1], le législateur a souhaité soumettre à une nouvelle autorisation préalable l'exploitation des équipements 5G. Il s'agit d'une mesure complémentaire à un contexte législatif déjà dense : socle historique du code des postes et des communications électroniques, lois de programmation militaire, réglementations relatives aux données personnelles, secret des correspondances, etc.
La présente contribution reviendra sur les mesures législatives existantes applicables dans le contexte de la virtualisation des réseaux 5G et apportera un oeil historique et technique sur ces mesures.

Mots-clé: 5G · SDN · NFV · législation

1 Introduction

Le présent article vise à donner un panorama de la législation française applicable aux opérateurs de communications électroniques en apportant à la fois un angle juridique et un angle technique.
Il introduit dans un premier temps le socle historique du code des postes et des communications électroniques. Ensuite, il traite la question des données personnelles. Puis, il aborde des spécificités du code pénal relatives au secret des correspondances. Par ailleurs, il explicite les impacts des dernières lois de programmation militaire sur les activités des opérateurs de communications électroniques. Ce préambule est nécessaire pour comprendre la genèse 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 dite loi "5G", promulguée le 1er août 2019 par le Président de la République[1].

2 Le Code des Postes et des Communications Electroniques (CPCE)

2.1 Un socle historique

L'un des actes fondateurs est la loi n° 52-223 du 27 février 1952 relative à la procédure de codification des textes législatifs concernant le service des postes,

Fig. 1. Opératrices au central téléphonique interurbain Paris Bonne Nouvelle. Juillet 1967 (source Orange/DGCI)

télégraphes et téléphones (les PTT - Postes, Télégraphes et Téléphones). À partir de 1962, il deviendra le code des postes et télécommunications [2].

Ce code va progressivement évoluer pour intégrer les nouveaux usages numériques, pour permettre l'ouverture du marché des télécommunications et pour préciser les attentes du législateur en matière de sécurité au sens large. Ce code deviendra le code des postes et des communications électroniques (CPCE) en 2004 [3] tel qu'il est connu aujourd'hui.

2.2 La sécurité, une obligation réglementaire et des enjeux économiques

L'article L32-1 du CPCE stipule que le ministre chargé des communications électroniques et l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) prennent des mesures raisonnables et proportionnées en vue d'atteindre les objectifs de respect par les opérateurs du secret des correspondances, de l'intégrité et de la sécurité des réseaux. L'article L33-1 du CPCE prévoit que l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur :
a) les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service qui incluent des obligations de notification à l'autorité compétente des atteintes à la sécurité ou à l'intégrité des réseaux et des services ;
b) les conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications ;
Ces règles sont retranscrites dans la partie réglementaire dans les articles D98-4

(disponibilité des réseaux) et D98-5 (I-secret des correspondances ; III- sécurité et intégrité des réseaux et des services).
Au delà de ces règles, il convient de garder en mémoire les enjeux économiques actuels pour les opérateurs et leurs clients en cas d'indisponibilité d'un réseau, en cas de piratage d'un réseau ou en cas de fraude. Les opérateurs doivent avoir dans leurs gènes la sécurité.
Par exemple dans le cas de la 5G, les opérateurs sont actifs en amont à travers des activités de recherche et les projets collaboratifs. Ils contribuent activement à la normalisation de la 5G à l'image du groupe S3 de 3GPP. Ils interviennent sur des documents structurants comme le document décrivant l'architecture sécurisée de la 5G [4]. En aval, les appels d'offre, les contrats avec les fournisseurs, les études d'architecture et des études d'ingénierie sur les futurs réseaux 5G incluent systématiquement un volet sécurité. L'article proposé au C&ESAR 2019 "Retour d'expérience sécurité sur le déploiement des technologies SDN/NFV" [5] peut l'illustrer. L'exploitation des réseaux n'est pas en reste avec une volonté de limiter les surfaces d'attaque, la mise en œuvre de différents niveaux de défense et la mise sous supervision sécurité des réseaux.

2.3 Contrôle de sécurité

Depuis l'ajout de l'article L33-10 au CPCE en 2011 [6], le ministre chargé des communications électroniques (actuellement le Ministre de l'Économie et des Finances) peut imposer à tout opérateur de soumettre ses installations, réseaux ou services à un contrôle de leur sécurité et de leur intégrité. Ce contrôle est effectué par un service de l'Etat (typiquement l'ANSSI, l'Agence Nationale de Sécurité des Systèmes d'Information) ou par un organisme qualifié indépendant désigné par le ministre chargé des communications électroniques. A l'issue du contrôle de sécurité, les résultats sont communiqués au ministre.
Les modalités pratiques du dispositif sont précisées dans les articles R9-7 à R9-12 du CPCE.
Les futurs réseaux 5G, les socles SDN/NFV et leurs moyens d'administrations sont soumis à ce type de contrôle de sécurité.

3 Protection des données personnelles

3.1 Le cadre général

La loi informatique et libertés de 1978[27] a longtemps été une référence au-delà des frontières nationales. Elle a fait l'objet d'une mise à jour récente[28] afin de prendre en compte le nouveau Règlement Général sur la Protection des Données (RGPD) établi au niveau européen en 2016[29].

3.2 Le cadre particulier pour les opérateurs de communications électroniques

Un cadre complémentaire à la loi informatique et libertés de 1978 a été mis en place en 2001[30] dans le contexte des opérateurs de communications élec-

troniques et il a régulièrement évolué depuis. L'article L32-1 du CPCE stipule que le ministre chargé des communications électroniques et ARCEP prennent des mesures raisonnables et proportionnées en vue d'atteindre les objectifs de respect par les opérateurs de la protection des données à caractère personnel. Il s'agit aujourd'hui des articles L34-1 à L34-6 du CPCE. Le dispositif fait l'objet de précisions dans la partie règlementaire du CPCE à savoir les articles R10-12 à R10-22.

3.3 Quelles sont les données personnelles ?

Les données personnelles sont ici des informations permettant d'identifier un client comme les IMSI (International Mobile Subscriber Identity) ou le MSISDN (Mobile Station International Subscriber Directory Number) qui peuvent être associées à des informations techniques nécessaires au fonctionnement opérationnel des réseaux mobiles :

- profil technique de l'abonné (ex : offres souscrites),
- localisation de l'abonné (ex : réseau hôte en cas de roaming, l'antenne radio sur laquelle est rattaché l'abonné),
- les comptes rendus d'appels, au sens large, nécessaires pour la facturation (ex : qui appelle qui, à quelle heure).

Avec l'avènement de l'Internet, l'adresse IP affectée à un client (éventuellement complétée par un port source/destination et un horodatage) pour qu'il puisse "naviguer" sur Internet doit être vue comme une donnée personnelle.

4 Le code pénal

4.1 De l'atteinte à la vie privée

Cadre législatif Si l'articulation entre code pénal et sécurité des réseaux d'opérateur n'est pas trivial, il prend tout son sens dans le contexte de l'atteinte à la vie privée, notamment sous l'angle du secret des correspondances.
Ainsi l'article 226-3 introduit la notion d'autorisation préalable pour 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 de porter atteinte au secret des correspondances.
Il s'agit d'une disposition introduite en 1992[22], qui a su évoluer en même temps que la technique.

Sanctions dissuasives Est puni de 300 000 euros d'amende et de cinq ans d'emprisonnement le fait de ne pas disposer des autorisations nécessaires, y compris par négligence.

Cadre réglementaire L'arrêté du 9 mai 1994 fixant la liste d'appareils prévue par l'article 226-3 du code pénal[23] se contentait d'identifier : les Micro-émetteurs, les dispositifs permettant l'interception de tout signal de données ou de télécopie ou encore les dispositifs permettant le traitement des correspondances interceptées ou détournées des voies de télécommunications.
Cette liste a évolué en 2004[24], en 2012[25] puis en 2016[26] pour finalement concerner les appareils, à savoir tous dispositifs matériels et logiciels, de nature à permettre 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, opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 du code pénal.
Dans la pratique, l'ANSSI est chargée du traitement administratif et de l'évaluation technique des appareils concernés. Il convient de prendre en compte que l'ANSSI peut refuser de délivrer une autorisation si elle juge que le niveau de sécurité de l'appareil ne peut permettre de garantir le secret des correspondances. L'ANSSI peut également délivrer une autorisation en émettant des recommandations de mise en œuvre et/ou en conditionnant l'autorisation par des règles de mise en œuvre.

4.2 Focus sur les opérateurs de communications électroniques

Un propos liminaire est que la plupart des équipements réseaux sont concernés par la réglementation R.226-x, qu'ils soient déployés chez les opérateurs de communications électroniques ou dans les autres entreprises / administrations. En effet, l'esprit de la loi est de cibler la vente/détention, pas l'usage. Ainsi, une entreprise qui acquiert un routeur peut tomber dans ce régime d'autorisation préalable dès lors qu'il dispose de fonctions permettant de dupliquer un flux IP donné et de le transmettre à une adresse IP distante.
La plupart des appareils du cœur de réseau mobile sont soumis à cette autorisation préalable. Par exemple, dans le contexte de la 5G, l'AMF et l'UPF sont concernés, comme la MME et les S/P-GW le sont en 4G.
Si la loi se focalise sur les fonctions de nature à nuire au secret des correspondances, les demandes d'autorisation comprennent également des éléments sur le contexte de mise en œuvre de ces fonctions. Ainsi, sur un équipement dédié, le durcissement du système d'exploitation ou le niveau de sécurité des accès en administration font l'objet d'une attention particulière.
De même, dans le contexte de la virtualisation des fonctions réseaux, le durcissement du système hôte, la sécurisation de la couche de virtualisation, le chiffrement des données (stockage, flux internes VNF ou flux externes VNF) et l'éventuelle mutualisation avec des fonctions non soumises à autorisation R.226-x sont attentivement regardés - tout en restant dans le contexte de la philosophie de la loi à savoir le secret des correspondances.

4.3 Un cas d'école : Vodafone Greece

Les mésaventures de Vodafone Greece[33][34] permettent de comprendre les enjeux du secret des correspondances dans le contexte des réseaux mobiles.

La genèse En janvier 2003, Vodafone réceptionne un nouveau palier logiciel sur ses MSC Ericsson AXE implémentant partiellement des fonctions d'interception. Entre juin et août 2004, plusieurs packs «téléphones portables + SIM» prépayés sont achetés simultanément. Une partie va servir comme destinataire d'interceptions illégales. Une autre partie semble avoir un lien avec l'ambassade des États-Unis à Athènes ainsi qu'avec des appels aux États-Unis, dans le Mariland, où se trouve le siège de la National Security Agency (NSA).
En août 2004, un exécutable est introduit sur des MSC Ericsson AXE. L'exécutable a du être généré à partir d'un programme écrit en PLEX d'environ 6500 lignes et est compilé avec un compilateur propriétaire d'Ericsson. L'exécutable est complexe. Il permet l'interception de numéros de téléphone en détournant la fonction d'interception proposée par Ericsson sans laisser de trace. Il comporte en plus des fonctions pour masquer sa présence. Très peu de personnes étaient en mesure d'écrire un tel programme.

Mise en place des interceptions illégales Les jeux olympiques d'Athènes 2004 se tiennent au mois d'août et le scandale de la dette grecque couve. Les premiers numéros à intercepter sont configurés sur les MSC Ericsson.

Le bug Entre le 27 et le 29 novembre 2004, le logiciel d'écoute illégale est installé sur un 4ème MSC Ericsson AXE sans avoir de numéro à intercepter. La fonction ne sera pas utilisée de suite. Il faudra attendre le 24 janvier 2005 pour qu'un numéros de test soit placé sous écoute sur ce 4ème MSC. Du 24 au 25 janvier 2005, ce 4ème MSC génère des erreurs, des messages textes ne sont pas envoyés. Vodafone ouvre un ticket SAV auprès d'Ericsson avec un dump de l'exécutable.

L'épilogue tragique Le 4 mars 2005, Ericsson informe Vodafone de l'identification d'un exécutable tiers permettant des interceptions «illégales». Il faudra ensuite 4 jours à Vodafone pour identifier l'ensemble des MSC piratés et les numéros interceptés illégalement. Le résultat est catastrophique car une centaine de numéros sont concernés parmi lesquels ceux du premier ministre grec, des ministres, des hauts fonctionnaires et des hauts gradés de l'armé ainsi que des membres de leur famille.
Le directeur de Vodafone ordonne la désinstallation du logiciel tiers et informe les autorités grecques le 8 mars 2005.
Le 9 mars 2005, le responsable de la planification du réseau Vodafone est retrouvé pendu dans des circonstances étranges.

5 Les Lois de Programmation Militaire (LPM) et le code de la Défense

5.1 Contexte général des SAIV/OIV/SIIV

SAIV Une ordonnance de 2004[7] introduit la notion de "Défense économique", en particulier la notion de "protection des installations d'importance vitale" avec les nouveaux articles L1332-x. Un décret [8] et un arrêté [9] de 2006 viennent ensuite définir la notion de Secteur d'Activité d'Importance Vitale (SAIV) et identifier les SAIV concerné dont le secteur «Communications électroniques, audiovisuel et information».

OIV Ce même décret[8] définit également la notion d'Opérateur d'Importance Vitale (OIV) et sert de fondement aux articles R.1332-x du code de la Défense[10]. Si la liste des OIV est classifée, pour reprendre les propos récents de parlementaires[11][12], "on peut estimer que les principaux opérateurs de télécommunication, et notamment ceux exploitant des réseaux radioélectriques mobiles, figurent parmi ces OIV".

SIIV La LPM 2014-2019 [17] a introduit des dispositions relatives à la protection des infrastructures vitales contre la cybermenace dans le code de la Défense (articles L1332-6-x du code de la défense). Ces dispositifs ont été précisés dans la partie réglementaire en 2015 (articles R1332-41-x au code de la Défense) [18] en introduisant la notion de Système d'Information d'Importance Vitale (SIIV). Ainsi rédigés, ces articles donnent toute latitude au Premier ministre de fixer les règles de sécurité nécessaires à la protection des SIIV 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.

5.2 Règles sur les SIIV des opérateurs de communications électroniques

Un arrêté de 2016 [19] fixe ces règles de sécurité pour le sous-secteur d'activités d'importance vitale «Communications électroniques et Internet». Elles sont relativement complètes.
Elles portent aussi bien sur des règles organisationnelles (politique de sécurité SIIV, homologation du SIIV, cartographie des équipements, procédure de maintient en condition opérationnel de sécurité, indicateurs sur le niveau de sécurité, processus de gestion de crise) que techniques (identification et authentification des utilisateurs et des administrateurs du SIIV, gestion des droits d'accès, focus sur l'administration des équipements, les accès à distance, le cloisonnement et le filtrage). Une part importante des règles est enfin orientée sur la détection d'évènements de sécurité (journalisation, corrélation et analyse de journaux et système de détection qualifié).

5.3 Compléments spécifiques aux opérateurs de communications électroniques

La LPM 2019-2025[20] a introduit de nouvelles dispositions relatives à la cyberdéfense. Elle a notamment ajouté l'article L33-14 du CPCE. Il mentionne que les opérateurs de communications électroniques peuvent recourir, sur les réseaux de communications électroniques qu'ils exploitent, après en avoir informé l'ANSSI, à des dispositifs de détection d'évènements de sécurité. Il peut s'agir par exemple de sondes Netflow utilisées par les opérateurs de communications électroniques pour détecter des attaques de déni de service.
Dans ce cas, l'ANSSI peut fournir des marqueurs aux opérateurs de communications électroniques afin de détecter des évènements de nature à porter atteinte à la sécurité des systèmes d'information.
Les modalités réglementaires ont été précisées en 2018 (articles R9-12-1 à R9-12-8 du CPCE)[21].

6 Loi 5G

6.1 Quels changements avec la 5G?

Les usages La 5G est présentée comme étant à la croisée des chemins. Tout d'abord, elle vise à faire converger de multiples usages et à en créer de nouveaux qui vont bien au delà de l'usage "loisir" du mobile perçu par le grand public. Il y a bien sûr la voix, y compris les appels vers les services d'urgence. Il y aussi une promesse de débits au delà de 1Gb/s pour naviguer sur Internet et regarder des contenus audiovisuels. Mais il s'agit aussi des voitures connectées, des usines 2.0 ou encore de la télémédecine. Dans leurs rapports relatifs à la loi "5G", les rapporteurs [12][14] mentionnent enfin un intérêt de l'Etat pour compléter les réseaux régaliens historiques dédiés de type TETRAPOL (par exemple Rubis pour la Gendarmerie, Acropol pour la Police, Antarès pour les services d'incendie et de secours) par des réseaux privés prioritaires sur les réseaux civils (exemple : PMR/PC Storm).

La cyberguerre Le théâtre d'opération des Armées se déplace depuis plusieurs années dans le cyberespace. Les nations développées ont défini des doctrines en la matière et elles les font évoluer au gré des expériences acquises. La France a ainsi rendu public début 2019 certains éléments de sa doctrine militaire offensive dans le cyberespace[15].

Des évolutions techniques majeures Tous les rapporteurs de la loi "5G" convergent sur les risques associés à la virtualisation des réseaux dans le contexte de la 5G. Ce changement technologique et organisationnel, déjà amorcé par les opérateurs de communications électroniques dans le contexte de la 4G et des plate-formes Voix, est perçue comme anxiogène par le législateur. Il peut cependant aussi être perçue comme une opportunité, y compris sous l'angle de

la sécurité avec la possibilité d'automatiser des déploiements sécurisés de VNF ou des audits de sécurité récurrents. Les infrastructures virtualisées permettent également un déploiement simplifié de composants sécurités (pare-feu, IDS, IPS) sous la forme de VNF.

Une évolution du paysage industriel mondial Il est difficile de ne pas aborder ici la montée en puissance de l'industrie chinoise avec comme fer de lance dans le domaine des équipements de communications électroniques ZTE et Huawei. Cette section ne reviendra pas sur les postures des différentes parties prenantes. Elle est déjà bien résumée dans les rapports des parlementaires[11][12][13][14]. Cette section se contentera de rappeler certains exemples publics sans prendre partie :

- 2004 : Compromission des équipements Ericsson déployés par Vodafone en Grèce.
- 2012 : Révélations de Snowden sur les techniques de la NSA pour compromettre les équipements réseaux et les pare-feu Cisco, Juniper, Fortinet, Huawei, etc.
- 2015 : CVE-2015-7755 concernant la présence d'un bout de code "non identifié" par Juniper dans ScreenOS. Cette porte dérobée permet, lors de l'accès en CLI (SSH ou Telnet), de s'authentifier en root en utilisant un mot de passe particulier quelque soit le login.

Le risque d'ingérence d'un État sur un équipementier de cet État est probablement réel, mais ne doit pas masquer les capacités avérées d'autres États à compromettre les équipements produits par cet équipementier[16]. Il ne s'agit que d'une question de temps, de moyens et de motivation.

6.2 Cadre européen

La Commission européenne a communiqué sa posture le 26 mars 2019[35].

Analyse des risques La Commission européenne a encouragé chaque État membre à procéder à une évaluation nationale des risques liés aux infrastructures des réseaux 5G et à partager cette analyse. L'analyse doit traiter les risques techniques et les risques non techniques, notamment ceux liés au recours de fournisseurs ou de sous-traitants qui pourraient être sous l'ingérence de pays tiers. En juillet 2019, 24 des 28 états membres avaient partagés leur analyse à l'ENISA[36]. L'ENISA en retour doit mettre à disposition une évaluation des risques à l'échelle de l'Union Européenne pour le 1er octobre 2019.

Renforcement des exigences sécurité vis à vis des opérateurs Les États membres sont invités à actualiser les exigences de sécurité existantes à destination des opérateurs de communications électroniques notamment lors de

l'octroi des fréquences destinées à la 5G. Parmi ces mesures devrait figurer l'obligation renforcée, pour les fournisseurs et les opérateurs, de garantir la sécurité des réseaux. La Commission européenne ouvre la porte aux États membres à l'exclusion de leurs marchés, pour des raisons de sécurité nationale, des entreprises ("the right of the Member States to exclude providers or suppliers from their markets for national security reasons").

Boîte à outil La Commission européenne doit élaborer et adopter une «boîte à outils» recensant les mesures à prendre pour atténuer les risques relevés dans les évaluations réalisées au niveau national et de l'Union Européenne d'ici la fin de l'année 2019.

6.3 Pourquoi une nouvelle loi?

Le gouvernement a jugé le contexte trop restrictif des articles A.226-3 et R.226-x du code pénal (voir section 4). Le gouvernement a également considéré que le contexte des SIIV (voir section 5) ne répondait pas aux attendus.

La problématique du RAN Le cadre actuel des autorisations R.226-x ne permet pas d'adresser certains appareils du réseau mobile.
Le gouvernement a bien essayé d'étendre le périmètre dans la loi de programmation militaire 2014-2019 [17] en remplaçant les mots « conçus pour réaliser les opérations » par les mots plus génériques « de nature à permettre la réalisation d'opérations » à l'article 226-3 du code pénal.
Il a ensuite publié l'arrêté du 11 août 2016 [26] visant à aligner l'arrêté sur les mots génériques « de nature à permettre la réalisation d'opérations » et à introduire « 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 », ciblant les équipements eNodeB/gNodeB.
Mais, factuellement, la majorité des équipements eNodeB/gNodeB ne disposent pas de fonctions "de nature" à nuire au secret des correspondances et de fait ne sont pas concernés par cette réglementation.

L'esprit de la Loi Les articles 226-3 et R.226-x du code pénal entrent dans le contexte de l'atteinte à la vie privée, contexte important, mais sans commune mesure avec les intérêts de la Nation.

Cas particulier des SIIV Concernant les SIIV, elle est à la main des OIV et reste générique. Un SIIV concerne un système d'information et pas un appareil particulier du système d'information. Elle n'offre pas la même souplesse ni les mêmes garanties pour le gouvernement que les modalités des autorisations R.226-7.

6.4 Le contenu de la loi

Un nouveau régime d'autorisation préalable La Loi "5G" introduit un nouveau régime d'autorisation préalable pour l'exploitation sur le territoire national des appareils, à savoir dispositifs matériels ou logiciels, constituant le réseau 5G. Elle cible les opérateurs réseau mobile en France.
La liste des appareils concernés fait l'objet d'un arrêté non publié à la date de rédaction du présent article. Néanmoins, il est possible de dire sans prendre trop de risque qu'il devrait couvrir toutes les fonctions 5G définies par 3GPP en reprenant de façon non ambiguë la terminologie du standard. Il couvre donc notamment les gNodeB, palliant de fait à la limitation de la réglementation dite "R.226".
Les modalités de la demande d'autorisation sont décrites dans un décret en Conseil d'Etat, là encore non publié à la date de rédaction du présent article. Le dossier de demande d'autorisation "5G" devrait s'inspirer des demandes d'autorisation R.226-7. La principale différence, conformément à cette Loi, est que la demande d'autorisation se focalise sur les conditions d'exploitation. Ainsi la demande d'autorisation devra décrire sur les moyens mis en œuvre pour administrer l'appareil par l'opérateur, par des sous-traitant ou par des fournisseurs (SAV, installation initiale/mise à jour, etc.) qui doivent eux-mêmes être identifiés.
La demande d'autorisation sera traitée par les services compétents du Premier ministre à savoir l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). Le Premier ministre peut refuser l'octroi de l'autorisation s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale. Le Premier ministre prend en considération, pour l'appréciation de ce risque, le niveau de sécurité des appareils, leurs modalités de déploiement et d'exploitation envisagées par l'opérateur et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un Etat non membre de l'Union européenne.

Des sanctions dissuasives Est puni de 300 000 euros d'amende et de cinq ans d'emprisonnement le fait d'exploiter des appareils sans autorisation préalable ou sans respecter les conditions fixées par l'autorisation.

Une simplification administrative Les équipements qui disposeront de la présente autorisation d'exploitation seront dispensés d'une demande d'autorisation R.226-7.

Un planning ambitieux La Loi est rétroactive aux appareils installés depuis le 1er février 2019.
Elle prévoit un délai de 2 mois pour la publication de l'arrêté fixant la liste des appareils concernés et pour la publication du décret fixant les modalités des demandes d'autorisation. La Loi ayant été promulguée le 1er août et publiée le 2 août 2019, l'arrêté et le décret auraient dû être publiés à la date de rédaction

de cet article - mais ce n'est manifestement pas le cas.
La Loi prévoit enfin que les opérateurs réseau mobile ont jusqu'au 2 décembre 2019 pour déposer les autorisations sur les appareils 5G installés depuis le 1er février 2019.

6.5 La mise en œuvre

Compte tenu de l'avancement de l'arrêté et du décret, il est à la date de rédaction de cet article trop tôt pour faire un retour d'expérience sur ce nouveau régime d'autorisation préalable à l'exploitation d'équipements 5G.
Il est néanmoins possible de noter que le législateur a inscrit dans la Loi l'obligation pour le Gouvernement de remettre au Parlement un rapport annuel sur l'application de cette Loi, et cela dès le 1er juillet 2020.

7 Conclusion

Les opérateurs de communications électroniques sont soumis, depuis l'ouverture du marché en France, à des obligations réglementaires en matière de sécurité des réseaux. Ces obligations se sont renforcées au fil des années. Il s'agit d'une part de prendre en compte l'omniprésence des communications électroniques dans notre vie quotidienne, mais aussi dans les OIV/SIIV. Il s'agit d'autre part d'intégrer les menaces "cyber" croissantes qui pèsent sur les opérateurs de communications électroniques avec des attaques de plus en plus sophistiquées.
La Loi 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 s'inscrit dans cette logique. Elle cible tout particulièrement les appareils réseau 5G en introduisant une nouvelle autorisation préalable à l'exploitation des appareils réseaux 5G pour les opérateurs de communications électroniques.
Les opérateurs ont eu l'occasion d'exprimer leurs craintes relatives aux modalités de mise en œuvre de cette loi, au regard du planning de déploiement de la 5G très ambitieux du Gouvernement et de l'ARCEP.
Il sera intéressant de suivre dans le futur les éventuels impacts sur le déploiement de la 5G en France et son adéquation avec les enjeux stratégiques identifiés par le législateur et par le Gouvernement.
Il faudra également suivre les suites données par la Commission européenne à sa réflexion sur la sécurité de la 5G.

References

1. LOI n°2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (NOR: ECOX1907688L)
2. Décret n°62-273 du 12 mars 1962 portant révision du code des postes, télégraphes et téléphones

3. LOI n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle (NOR: ECOX0300083L)
4. 3GPP TS33.501 - 3rd Generation Partnership Project;
   Technical Specification Group Services and System Aspects;
   Security architecture and procedures for 5G system
5. Retour d'expérience sécurité sur le déploiement des technologies SDN/NFV, G. Veille et J.-M. Farin, C&ESAR 2019
6. Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques portant notamment sur la transposition du nouveau cadre européen des communications électroniques (NOR: INDX1116689R)
7. Ordonnance n°2004-1374 du 20 décembre 2004 relative à la partie législative du code de la défense (NOR: DEFX0400190R)
8. Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale (NOR: PRMX0500312D)
9. Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs (NOR: PRMX0609332A)
10. Décret n°2007-585 du 23 avril 2007 relatif à certaines dispositions réglementaires de la première partie du code de la défense (Décrets en Conseil d'Etat) (NOR: DEFD0751862D)
11. Rapport n°1832 de M. Eric BOTHOREL, fait au nom de la commission des affaires économiques, déposé le 3 avril 2019 dans le contexte de l'examen de la proposition de Loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.
12. 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, déposé le 12 juin 2019 dans le contexte de l'examen de la proposition de Loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.
13. Rapport n°579 (2018-2019) de Mme Catherine PROCACCIA, fait au nom de la commission des affaires économiques, déposé le 19 juin 2019 dans le contexte de l'examen de la proposition de Loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.
14. Avis n°1830 de M. Thomas GASSILLOUD, fait au nom de la commission de la défense, déposé le 2 avril 2019 dans le contexte de l'examen de la proposition de Loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.
15. Éléments publics de doctrine militaire de lutte informatique offensive, Ministère des Armées/ComCyber, 18 janvier 2019
    https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-de-florence-parly/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive
16. U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks
    U.S. spies suspect Huawei of being able to embed computer exploits because they've already done it themselves By Jeremy Hsu, 26 Mar 2014
    https://spectrum.ieee.org/tech-talk/computing/hardware/us-suspicions-of-chinas-huawei-based-partly-on-nsas-own-spy-tricks
17. 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 (NOR: DEFX1317084L)

18. Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense (NOR: PRMD1502905D)
19. 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 (NOR: PRMD1630591A)
20. LOI n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense (NOR: ARMX1800503L)
21. Décret n°2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques (NOR: PRMD1828335D)
22. LOI n° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes (NOR: JUSX8900010L)
23. Arrêté du 9 mai 1994 fixant la liste d'appareils prévue par l'article 226-3 du code pénal (NOR: INDP9400540A)
24. Arrêté du 29 juillet 2004 fixant la liste d'appareils prévue par l'article 226-3 du code pénal (NOR: PRMX0407500A)
25. Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal (NOR: PRMD1230326A)
26. Arrêté du 11 août 2016 modifiant l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal (NOR: PRMD1621601A)
27. LOI n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
28. LOI n°2018-493 du 20 juin 2018 relative à la protection des données personnelles (NOR: JUSC1732261L)
29. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données)
30. LOI n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne
31. Moon sur l'Open Platform for NFV (OPNFV)
https://wiki.opnfv.org/display/moon/Moon+Project+Proposal
32. Moon sur GitHub
https://github.com/opnfv/moon/tree/master/tools/openstack
33. The Athens Affair by Vassilis Prevelakis and Diomidis Spinellis, IEEE Spectrum, 44(7):26–33, July 2007
https://spectrum.ieee.org/telecom/security/the-athens-affair
34. A death in Athens: Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee?
by James Bamford (September 28, 2015). The Intercept
https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/
35. La Commission européenne recommande une approche commune de l'UE concernant la sécurité des réseaux 5G, le 26 mars 2019
https://europa.eu/rapid/press-release_IP-19-1832_fr.htm

36. Sécurité des réseaux 5G: les États membres de l'UE achèvent leurs évaluations nationales des risques, le 19 juillet 2019
https://ec.europa.eu/commission/presscorner/detail/fr/statement_19_4266