4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Un article L. 4139-9-1 est créé dans le code de la défense, codifiant le dispositif de PF. L'article 37 de la loi n° 2013-1168 est abrogé au 1er janvier 2030.

Les dispositions de la loi n° 2013-1168 régissant le PMID sont modifiées. Ainsi, l'article 36 est modifié pour tenir compte de la création de l'article L. 4139-9-1.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Néant.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

Néant.

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Néant.

4.2.3. Impacts budgétaires

Les dispositifs de la promotion fonctionnelle (PF) et du pécule modulable d'incitation au départ (PMID) sont contingenté par arrêté interministériel.

Promotion fonctionnelle

Le départ des bénéficiaires d'une PF et d'un droit à pension de retraite à jouissance immédiate, ne génère pas de besoin de financement supplémentaire sur le titre 2 du ministère des armées hors compte d'affectation spéciale « Pensions ». Ces promotions sont en effet prononcées dans la limite des plafonds des effectifs autorisés pour chaque grade et chaque corps fixés annuellement avec le ministère chargé du budget. A partir du départ du militaire, l'Etat économise le versement de la solde qui était due jusqu'à la limite d'âge ainsi que les cotisations sociales « employeurs » (titre 2).

En 2022, le ministère des armées disposait d'un contingent de 50 PF[103]. La possibilité introduite à l'article 18 du présent projet de loi d'attribuer deux affectations à des officiers généraux au titre de la promotion fonctionnelle impliquera probablement de doubler ce contingent. Toutefois, comme expliqué *supra*, il n'en résultera aucun surcoût.

Pécule modulable d'incitation au départ

Le départ avec bénéfice du pécule permet à l'Etat d'économiser la solde qui aurait dû être versée jusqu'à la limite d'âge du militaire. Le coût du versement d'un pécule et d'une pension est en effet inférieur au coût du versement d'une solde à taux plein et d'une pension plus conséquente si le militaire était resté jusqu'à sa limite d'âge. Le surcoût budgétaire induit par la prorogation du dispositif du PMID jusqu'en 2030 est donc nul.

Par ailleurs, le fait de réduire, pour les officiers généraux, de trois à un an la condition d'éligibilité liée à la durée des services restant à accomplir avant l'atteinte de la limite d'âge s'accompagnera d'une réduction, à due concurrence, du montant du pécule versé dans cette situation[104]. Cet aspect de la mesure prévu par la présente disposition n'occasionne donc aucun besoin de financement supplémentaire.

Le surcoût budgétaire prévisible de la mesure relative au PMID tient entièrement au fait que la rénovation du dispositif implique d'augmenter le contingent de pécules sur la période 2024-2030. Le ministère des armées disposait d'un contingent de 223 PMID pour 2022. Ce contingent est fixé annuellement à 235 pour les années 2023 à 2025[105].

Cette nécessité de réviser à la hausse ce contingent est lié à plusieurs facteurs. D'une part, le dispositif de la pension afférente au grade supérieur (PAGS) s'éteindra en 2025[106]. Par ailleurs, le besoin de disposer des outils pour mener la « manœuvre de pivots » impose de conserver une aide au départ pour le personnel aux compétences obsolètes ou en passe de le devenir. Enfin, compte tenu du modèle RH de flux du ministère des armées, il est essentiel d'offrir jusqu'à un stade avancé de la carrière des perspectives d'avancement et de progression pour le personnel à potentiel et/ou disposant de compétences indispensables à la conduite des missions des armées et donc de pouvoir faire partir une partie de la ressource (conséquence de la contrainte du contingentement). Le ministère des Armées estime ainsi son besoin pour la période 2024-2030 à 275 PMID par an. Le surcoût associé est estimé à 5 M€.

[103] Arrêté du 17 novembre 2021 pris en application de l'article 37 de la loi n° 2013-1168 du 18 décembre 2013 modifiée relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

[104] Pour mémoire, le montant du PMID est fixé par voie règlementaire.

[105] Cf. art. 3 et 4 de l'arrêté du 23 septembre 2022 pris en application des articles 36 et 38 de la loi n° 2013-1168 du 18 décembre 2013 modifiée relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

[106] Le contingent de PAGS est fixé à 90 pour 2022, 70 pour 2023 et 30 en 2024 (cf. art. 2 de l'arrêté du 23 septembre 2022 pris en application des articles 36 et 38 de la loi n° 2013-1168 du 18 décembre 2013 modifiée relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SUR LES ARMEES

La gestion des ressources humaines des forces armées et formations rattachées et leur adaptation à la transformation des armées seront facilitées par le maintien des deux leviers de départ que constituent la PF et le PMID.

4.6. IMPACTS SOCIAUX

4.6.1. Impacts sur la société

Néant.

4.6.2. Impacts sur les personnes en situation de handicap

Néant.

4.6.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.6.4. Impacts sur la jeunesse

Néant.

4.6.5. Impacts sur les professions réglementées

Néant.

4.7. IMPACTS SUR LES PARTICULIERS

Les mesures proposées permettent de favoriser les transitions professionnelles des militaires, dont les limites d'âges sont plus basses que celles des fonctionnaires et plus précoces de celles

des salariés. Elles permettent de les initier plus tôt, favorisant une seconde carrière pour les intéressés.

4.8. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

La mesure a reçu un avis favorable du Conseil supérieur de la fonction militaire (CSFM), lors de la session du 9 mars 2023, ainsi que prévu par l'article L. 4124-1 et le 2° de l'article R. 4124-1 du code de la défense.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

L'application sera permanente à partir du lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Le présent article est applicable sur l'ensemble du territoire de la République française. Les dispositions créées sont intégrées au statut général des militaires, lequel est applicable de plein droit sur tout le territoire national. Il est également applicable de plein droit dans les départements et régions d'outre-mer, ainsi que dans les collectivités et territoires d'outre-mer et en Nouvelle-Calédonie.

5.2.3. Textes d'application

Le décret n° 2021-962 du 20 juillet 2021 régit actuellement la PF. Il sera remplacé par un nouveau décret en Conseil d'Etat qui définira les conditions dans lesquelles les officiers généraux, les officiers, les sous-officiers et les officiers mariniers pourront être promus au grade supérieur.

Le décret n° 2019-1294 du 4 décembre 2019 fixe les modalités du versement du PMID. Il sera remplacé par un nouveau décret simple qui précisera notamment les catégories de militaires éligibles, les conditions d'attribution, les modalités de calcul et, le cas échéant, les conditions de remboursement du pécule.

CHAPITRE II – RENSEIGNEMENT ET CONTRE-INGERENCE

Article 19 : Permettre l'accès des services de renseignement au casier judiciaire au titre des enquêtes administratives de sécurité

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Le service national des enquêtes administratives de sécurité du ministère de l'intérieur (SNEAS), la direction générale de la sécurité intérieure (DGSI), la direction du renseignement et de la sécurité de la Défense (DRSD) et la direction générale de la sécurité extérieure (DGSE) sont compétents pour mener des enquêtes administratives préalablement à des décisions de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation.

Ces enquêtes sont effectuées sur le fondement de l'article L. 114-1 du code de la sécurité intérieure, qui prévoit que : « *Les décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.*

Ces enquêtes peuvent donner lieu à la consultation de traitements automatisés de données à caractère personnel relevant de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. Les conditions dans lesquelles les personnes intéressées sont informées de cette consultation sont précisées par décret. (…) ».

La liste des décisions pouvant donner lieu à ces enquêtes administratives est ensuite fixée aux articles R. 114-1 à R. 114-5 du même code.

Dans ce cadre, il revient aux services d'apprécier le degré de confiance qu'il est possible d'accorder à la personne concernée ainsi que les vulnérabilités qu'elle présente. A ce titre, son honnêteté, voire sa probité, peuvent notamment s'apprécier en fonction de son passé judiciaire.

Or les enquêtes administratives faites sur le fondement de l'article L. 114-1 du code de la sécurité intérieure, à la différence de celles effectuées sur le fondement de l'article L. 114-2 du

même code (enquêtes préalables aux recrutements et affectations aux « *emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes ou d'une entreprise de transport de marchandises dangereuses soumise à l'obligation d'adopter un plan de sûreté ou d'un gestionnaire d'infrastructure* ») , ne peuvent être précédées de la consultation du bulletin numéro 2 du casier judiciaire.

Le casier judiciaire est le relevé des décisions judiciaires et administratives qui concernent une personne physique ou morale. Il est divisé en 3 bulletins. Le B1 contient toutes les sanctions prononcées à l'encontre d'une personne par la justice ou par les autorités administratives. Il est réservé aux services judiciaires. Le B2 contient seulement une partie de ces décisions. Il est délivré aux administrations et à certains employeurs. Le B3 contient les condamnations les plus graves.

L'article 775 du code de procédure pénale prévoit que : « *Le bulletin n° 2 est le relevé des fiches du casier judiciaire applicables à la même personne, à l'exclusion de celles concernant les décisions suivantes : / 1° Les condamnations, les déclarations de culpabilité assorties d'une dispense de peine ou d'une dispense de mesure éducative ou d'une déclaration de réussite éducative, les compositions pénales et les mesures éducatives prononcées au stade de la sanction à l'égard d'un mineur ; / 2° Les condamnations dont la mention au bulletin n° 2 a été expressément exclue en application de l'article 775-1 ; / 3° Les condamnations prononcées pour contraventions de police ; / 4° Les condamnations assorties du bénéfice du sursis, avec ou sans probation, lorsqu'elles doivent être considérées comme non avenues ; toutefois, si a été prononcé le suivi socio-judiciaire prévu par l'article 131-36-1 du code pénal ou la peine d'interdiction d'exercer une activité professionnelle ou bénévole impliquant un contact habituel avec des mineurs, la décision continue de figurer au bulletin n° 2 pendant la durée de la mesure. Il en va de même des interdictions, incapacités ou déchéances prononcées, comme peine complémentaire, à titre définitif ainsi que de la peine complémentaire d'inéligibilité prévue au 2° de l'article 131-26 et aux articles 131-26-1 et 131-26-2 du même code, pendant la durée de la mesure ; / 5° Les condamnations ayant fait l'objet d'une réhabilitation de plein droit ou judiciaire ; / 6° Les condamnations auxquelles sont applicables les dispositions de l'article L. 263-4 du code de justice militaire ; / (…) 9° Les dispositions prononçant la déchéance de l'autorité parentale ; / 10° Les arrêtés d'expulsion abrogés ou rapportés ; / 11° Les condamnations prononcées sans sursis en application des articles 131-5 à 131-11 du code pénal, à l'expiration d'un délai de cinq ans à compter du jour où elles sont devenues définitives. Le délai est de trois ans s'il s'agit d'une condamnation à une peine de jours-amende. / Toutefois, si la durée de l'interdiction, déchéance ou incapacité, prononcée en application des articles 131-10 et 131-11, est supérieure à cinq ans, la condamnation demeure mentionnée au bulletin n° 2 pendant la même durée ; / 12° Les déclarations de culpabilité assorties d'une dispense de peine ou d'un ajournement du prononcé de celle-ci ; / 13° Les condamnations prononcées par des juridictions étrangères concernant un mineur ou dont l'utilisation à des fins autres qu'une procédure pénale a été expressément exclue par la juridiction de condamnation ; / 14° Les compositions pénales mentionnées à l'article 768 ; / 15° Sauf décision contraire du juge, spécialement motivée, les condamnations prononcées pour les délits prévus au titre IV du livre*

IV du code de commerce ; / 16° Les amendes forfaitaires mentionnées au 11° de l'article 768 du présent code. (…) »

Ainsi, si l'accès au traitement des antécédents judiciaires (TAJ), dont disposent déjà les services compétents pour mener des enquêtes administratives, constitue une source d'information précieuse sur les affaires judiciaires dans lesquelles la personne concernée a été impliquée, ce traitement ne comporte pas d'information sur les éventuelles condamnations ou relaxes prononcées ; ainsi, il ne permet pas de connaître les suites judiciaires consécutives à une éventuelle mise en cause de la personne concernée, ce qui ne met pas les services enquêteurs en situation de porter une appréciation parfaitement éclairée sur sa probité.

1.2. CADRE CONSTITUTIONNEL

D'une part, la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la consultation du bulletin numéro 2 du casier judiciaire doit être justifiée par un motif d'intérêt général et mise en œuvre de manière adéquate et proportionnée à cet objectif[107]. Il revient par ailleurs au législateur de fixer précisément les motifs des consultations ainsi que les restrictions et précautions dont ces consultations sont assorties telles que les finalités de l'enquête administrative ou l'information de la personne concernée[108].

En outre, le dispositif prévu par l'article L. 114-1 du code de la sécurité intérieure peut être rapproché de celui de l'article L. 114-2 du même code, autorisant la réalisation d'une enquête administrative préalablement à une « *décision de recrutement et d'affectation concernant les emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes ou d'une entreprise de transport de marchandises dangereuses soumise à l'obligation d'adopter un plan de sureté ou d'un gestionnaire d'infrastructure* ».

Or, dans ce cadre, le Conseil d'Etat, dans sa décision du 1er juin 2018, n° 412161, aux Tables, a considéré que ces dispositions ne portent pas d'atteinte excessive au droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) et que « *la possibilité d'effectuer, pour des raisons de sécurité, les enquêtes administratives prévues par l'article L. 114-2 du code de la sécurité intérieure ne constitue pas une sanction ayant le caractère d'une punition à l'égard de laquelle pourrait être invoqué l'article 16 de la Déclaration des droits de l'homme et du citoyen ;[…]* ».

D'autre part, l'article 9 de la Déclaration de 1789 protège la présomption d'innocence. Ce principe constitutionnel n'est pas méconnu par la seule consultation de traitement de données nominatives dès lors qu'elle s'effectue dans la stricte mesure exigée par la défense des intérêts

[107] Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité

[108] Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure

fondamentaux de la Nation. Par ailleurs, toute personne inscrite dans le fichier peut exercer son droit d'accès et de rectification des données la concernant[109]. Le principe de présomption d'innocence n'est pas davantage méconnu par la conservation des données, sauf décision contraire de l'autorité judiciaire, en cas de non-lieu ou de classement sans suite dès lors que ces décisions peuvent résulter de l'encombrement de la justice ou de la difficulté de recueillir des preuves.

1.3. CADRE CONVENTIONNEL

La Cour européenne des droits de l'homme juge que, pour ne pas méconnaître le droit à la vie privée garanti par l'article 8, la collecte de données personnelles doit poursuivre un but légitime et avoir un caractère proportionné au but identifié[110]. Tel est bien le cas de la mesure proposée qui permet aux services compétents de connaître les suites données à une affaire judiciaire.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

En application de l'article L. 114-1, les services de l'Etat compétents sont autorisés à consulter des fichiers de sécurité (fichiers de renseignement, de police ou de justice), pris en application de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. S'agissant des fichiers d'« *antécédents judiciaires* », ces services ont accès aux fichiers comportant des informations sur les personnes mises en cause dans une procédure pénale (fichier TAJ) mais n'ont paradoxalement pas accès au bulletin numéro 2 du casier judicaire national recensant la plupart des condamnations prononcées, à l'exception de quelques décisions limitativement listées par l'article 775 du code de procédure pénale.

En effet, l'accès au B2 est actuellement réservé aux administrations publiques de l'Etat saisies de demandes d'emplois publics, aux termes du 1° de l'article 776 du code de procédure pénale, ce qui n'ouvre l'accès au B2 qu'aux employeurs, catégorie dans laquelle n'entrent pas les services enquêteurs.

Il en résulte le risque de prendre des décisions administratives défavorables aux personnes concernées (refus de recrutement ou refus d'accès à un site entrainant un licenciement) sur la

[109] Ibid.

[110] CEDH, 22 juin 2017, Aycaguer c/France, n°8806/12, §38

base d'informations relatives à des procédures pénales qui ne seraient pas à jour de l'éventuel classement sans suite, ou au contraire d'autoriser le recrutement ou l'accès d'une personne à un site alors que le service enquêteur n'aurait pas été informé de la condamnation pénale prononcée.

Un second paradoxe s'ajoute au premier : la consultation du casier judiciaire n° 2 est déjà possible préalablement au recrutement dans des emplois relevant du domaine des transports publics conformément à l'article L. 114-2 du code de la sécurité intérieure, mais est donc proscrit s'agissant d'emplois publics particulièrement sensibles en ce qu'ils conduisent par exemple à confier des armes (recrutement des militaires et des policiers notamment).

2.2. OBJECTIFS POURSUIVIS

Afin de remédier aux paradoxes mentionnés au 2.1., de pallier le risque d'autoriser le recrutement ou l'accès d'une personne à un site alors que le service chargé de l'enquête n'aurait pas eu connaissance d'une condamnation pénale prononcée à son encontre comme, à l'inverse, de prévenir tout risque de refuser un accès ou une habilitation sur la seule base d'une mise en cause judiciaire n'ayant finalement donné lieu à aucune condamnation pénale, il est nécessaire de permettre aux services enquêteurs d'accéder aux informations relatives aux condamnations effectivement prononcées par le juge pénal.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

L'accès des services enquêteurs aux condamnations prononcées par le juge pénal pourrait théoriquement être limité au seul B3 ; toutefois, ce dernier ne comporte que les condamnations pénales les plus graves. Ces informations n'offrent pas de données suffisantes pour apprécier la vulnérabilité et la probité de la personne faisant l'objet d'une enquête administrative.

A l'inverse, cet accès pourrait théoriquement concerner les informations figurant au B1, lequel contient toutes les sanctions prononcées à l'encontre d'une personne par la justice ou par les autorités administratives. Toutefois, l'accès à ce fichier est actuellement réservé aux seuls services judiciaires et il ne paraît pas nécessaire de modifier cet équilibre.

3.2. OPTION RETENUE

L'objectif de la modification de l'article L. 114-1 est de permettre aux services compétents (SNEAS, DGSI, ainsi que DRSD et DGSE pour le ministère des Armées) d'être rendus destinataires du bulletin numéro 2 du casier judiciaire, en plus des consultations déjà possibles des fichiers des condamnations pour acte de terrorisme ou des infractions à caractère sexuel

afin d'apprécier la vulnérabilité d'une personne, au regard de son éventuel passé judiciaire, dans sa globalité.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Le chapitre V du titre Ier du livre Ier du code de la sécurité intérieure est modifié.

Le présent article aligne ainsi le régime des enquêtes administratives préalables aux décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation (L. 114-1) sur celui applicable aux enquêtes prévues pour les décisions de recrutement et d'affectation concernant les emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes ou d'une entreprise de transport de marchandises dangereuses soumise à l'obligation d'adopter un plan de sûreté ou d'un gestionnaire d'infrastructure (L. 114-2).

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Dès lors que le traitement de données personnelles autorisé par la mesure est nécessaire, adéquat et proportionné aux finalités poursuivies, la disposition est en tout état de cause conforme à la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La disposition contribuera à conforter les conclusions des enquêtes administratives de sécurité et, partant, à sécuriser les décisions administratives de recrutement ou d'habilitation mentionnées à l'article L. 114-1 du code de la sécurité intérieure.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

La disposition prévoit un dispositif équilibré quant au droit des personnes en ce qu'il permet aux services compétents de connaître les suites données aux affaires judiciaires. Il ne méconnait pas davantage le respect de la présomption d'innocence pour les raisons indiquées précédemment.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions sont expressément étendues en Polynésie française, en Nouvelle-Calédonie, à Wallis-et-Futuna et dans les Terres australes et antarctiques françaises par le II et le III du présent article. Elles s'appliqueront donc sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

La présente mesure ne nécessite aucun texte d'application.

Article 20 : Garantir la prise en compte des intérêts fondamentaux de la Nation en cas d'activité privée par un ancien militaire, dans le domaine de la défense ou de la sécurité, en rapport avec une puissance étrangère

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Dans le contexte de résurgence des tensions et compétitions internationales, des Etats étrangers n'hésitent pas à rechercher activement, directement ou par l'intermédiaire d'entreprises agissant pour leur compte, la collaboration d'anciens militaires dont l'expertise technique ou le savoir-faire opérationnel présentent un intérêt stratégique pour le développement de leurs propres capacités militaires. Ce phénomène a pu être constaté dans plusieurs Etats occidentaux, notamment au Royaume-Uni et aux Etats-Unis mais également en France. Il concerne principalement les pilotes d'avions, qui détiennent des compétences techniques précieuses (décollage par catapulte, appontage, etc.). Ainsi, une dizaine de pilotes français ont fait l'objet d'approche par des Etats tiers au cours des dernières années. Les autorités britanniques ont, quant à elles, indiqué qu'une trentaine de leurs pilotes avaient été approchés.

Le recrutement d'anciens militaires dans ce cadre concerne essentiellement des activités de formation.

Alors que la France investit dans de nouvelles générations d'armement et renforce la montée en puissance opérationnelle de ses forces, il est indispensable de prévenir de telles pratiques, qui constitueraient un risque pour la défense nationale ainsi que pour la défense des alliés.

En l'état du droit, aucun dispositif organisé ne permet de faire obstacle au départ de militaires vers des structures étrangères les embauchant dans l'objectif même d'obtenir de leur part des informations ou savoir-faire à caractère stratégique.

La présente mesure vise à répondre à ce problème qui met en cause la sauvegarde des intérêts fondamentaux de la Nation.

1.2. CADRE CONSTITUTIONNEL ET CADRE CONVENTIONNEL

1.2.1. La sauvegarde des intérêts fondamentaux de la Nation constitue une exigence constitutionnelle pouvant justifier une atteinte à d'autres principes à valeur constitutionnelle

Il ressort de la jurisprudence du Conseil constitutionnel et du Conseil d'Etat que les « *exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* », au

premier rang desquelles figurent l'indépendance nationale et l'intégrité du territoire, qui en sont la finalité, mais également la protection du secret de la défense nationale et la libre disposition de la force armée, sont prises en compte par le juge dans son contrôle de proportionnalité en cas d'atteinte à d'autres principes à valeur constitutionnelle.

Il revient au juge d'assurer une « *conciliation qui ne soit pas déséquilibrée* » entre la sauvegarde des intérêts fondamentaux de la Nation et les autres exigences constitutionnelles[111].

1.2.2. Les dérogations à la liberté contractuelle doivent être justifiées par des motifs d'intérêt général

S'appuyant sur les dispositions de l'article 4 de la Déclaration des Droits de l'Homme et du Citoyen de 1789, le Conseil constitutionnel considère que : « *le législateur ne saurait porter aux contrats légalement conclus une atteinte qui ne soit justifiée par un motif d'intérêt général suffisant sans méconnaître les exigences résultant des articles 4 et 16 de la Déclaration de 1789* »[112].

1.2.3. Le Conseil constitutionnel reconnait une large marge d'appréciation au législateur dans la mise en œuvre du droit d'obtenir un emploi

Aux termes du cinquième alinéa du Préambule de la Constitution de 1946 : « *Chacun a le devoir de travailler et le droit d'obtenir un emploi. Nul ne peut être lésé, dans son travail ou son emploi, en raison de ses origines, de ses opinions ou de ses croyances* ».

Sur le fondement de ces dispositions, le Conseil constitutionnel a pu considérer que le législateur, qui est compétent en vertu de l'article 34 de la Constitution pour déterminer les principes fondamentaux du droit du travail, pouvait limiter la portée du droit à obtenir un emploi[113].

1.2.4. Le droit de l'Union européenne admet des dérogations à la libre circulation des travailleurs et à la liberté d'établissement pour des raisons de sécurité

[111] Mme Ekaterina B., épouse D., et autres, 10 novembre 2011, n° 2011-192 QPC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif et du droit à un procès équitable ; Loi relative au renseignement, 23 juillet 2015, n° 2015-713 DC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif, du droit à un procès équitable et du principe du contradictoire ; Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias, 10 novembre 2016, n° 2016-738 DC, à propos de la liberté d'expression et de communication ; La Quadrature du net, 9 juillet 2021, décision n° 2021-924 QPC, à propos du respect de la vie privée.

[112] Loi relative à l'orientation et à la formation professionnelle tout au long de la vie, 19 novembre 2009, n° 2009-592 DC.

[113] A propos du cumul emploi-retraites : Loi d'orientation autorisant le Gouvernement par application de l'article 38 de la Constitution, à prendre des mesures d'ordre social, 5 janvier 1982, n° 81-134 DC ; à propos de la réduction du temps de travail : Loi portant diverses mesures relatives aux prestations de vieillesse, du 28 mai 1983, n° 83-156 DC ; à propos de la mise à la retraite d'office de salarié exerçant au-delà de l'âge de la retraite à taux plein : M. Jacques N., 4 février 2011, n° 2010-98 QPC.

publique

Le Traité sur le fonctionnement de l'Union Européenne (TFUE) énonce les dispositions relatives à la liberté de circulation des travailleurs sur le territoire de l'Union Européenne et à la liberté d'établissement.

S'agissant de la libre circulation des travailleurs, l'article 45 prévoit que : « *1. La libre circulation des travailleurs est assurée à l'intérieur de l'Union. /(…) / 3. Elle comporte le droit,* ***sous réserve des limitations justifiées par des raisons d'ordre public, de sécurité publique et de santé publique****: / a) de répondre à des emplois effectivement offerts, b) de se déplacer à cet effet librement sur le territoire des États membres, c) de séjourner dans un des États membres afin d'y exercer un emploi conformément aux dispositions législatives, réglementaires et administratives régissant l'emploi des travailleurs nationaux, d) de demeurer, dans des conditions qui feront l'objet de règlements établis par la Commission, sur le territoire d'un État membre, après y avoir occupé un emploi. 4. Les dispositions du présent article ne sont pas applicables aux emplois dans l'administration publique.* ».

S'agissant de la liberté d'établissement, l'article 49 prévoit que : « *les restrictions à la liberté d'établissement des ressortissants d'un État membre dans le territoire d'un autre État membre sont interdites. Cette interdiction s'étend également aux restrictions à la création d'agences, de succursales ou de filiales, par les ressortissants d'un État membre établis sur le territoire d'un État membre. La liberté d'établissement comporte l'accès aux activités non salariées et leur exercice, ainsi que la constitution et la gestion d'entreprises, et notamment de sociétés au sens de l'article 54, deuxième alinéa, dans les conditions définies par la législation du pays d'établissement pour ses propres ressortissants, sous réserve des dispositions du chapitre relatif aux capitaux* ».

Néanmoins, l'article 52 dispose que : « *Les prescriptions du présent chapitre et les mesures prises en vertu de celles-ci ne préjugent pas l'applicabilité des dispositions législatives, réglementaires et administratives prévoyant un régime spécial pour les ressortissants étrangers, et* ***justifiées par des raisons d'ordre public, de sécurité publique et de santé publique*** ».

La notion de « sécurité publique » vise à la fois la sécurité intérieure d'un Etat membre et sa sécurité extérieure[114]. La première peut être en péril notamment lorsqu'il y a une *« menace directe pour la tranquillité et la sécurité physique de la population »*[115] pendant que la seconde, plus large, appréhende « *l'atteinte au fonctionnement des institutions et des services publics essentiels ainsi que la survie de la population, de même que le risque d'une perturbation grave des relations extérieures ou de la coexistence pacifique des peuples, ou encore l'atteinte aux intérêts militaires* [116] ».

[114] CJUE, 23 novembre 2010, Tsakouridis, C-145/09, pt 43.

[115] CJUE, 22 mai 2012, P.I., C-348/09, pt 28.

[116] CJUE, 24 juin 2015, H. T. c. Land Baden-Württemberg, C-373/13, pt 78.

1.2.5. Les exigences liées aux sanctions administratives et pénales

Dans sa décision n° 89-260 DC du 28 juillet 1999, le Conseil constitutionnel a considéré que : « *le principe de la séparation des pouvoirs, non plus qu'aucun principe ou règle de valeur constitutionnelle ne fait obstacle à ce qu'une autorité administrative, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction dès lors, d'une part, que la sanction susceptible d'être infligée est exclusive de toute privation de liberté et, d'autre part, que l'exercice du pouvoir de sanction est assorti par la loi de mesures destinées à sauvegarder les droits et libertés constitutionnellement garantis* ».

Au titre de ces droits et libertés constitutionnellement garantis, il est possible de distinguer les exigences procédurales des exigences de fond.

Les exigences procédurales[117] liées aux sanctions administratives et pénales

Les droits de la défense sont pris en compte préalablement au prononcé de sanctions sans qu'il soit besoin pour le législateur d'en rappeler l'existence

Le respect des droits de la défense, initialement consacré comme principe général du droit[118], puis comme principe fondamental reconnu par les lois de la République[119] constitue à présent une exigence à valeur constitutionnelle rattachée à l'article 16 de la Déclaration des droits de l'Homme et du Citoyen de 1789[120].

Ce principe ne concerne pas seulement les peines prononcées par le juge pénal mais s'applique à toute sanction ayant le caractère d'une punition y compris si le législateur a laissé le soin de la prononcer à une autorité de nature non judiciaire[121]. *Il implique « qu'aucune sanction ayant le caractère d'une punition ne puisse être infligée à une personne sans que celle-ci ait été mise à même de présenter ses observations sur les faits qui lui sont reprochés » et « s'impose aux autorités disposant d'un pouvoir de sanction sans qu'il soit besoin pour le législateur d'en rappeler l'existence »*[122].

L'impartialité objective et l'indépendance des tribunaux ne sont pas opposables aux sanctions prises par une autorité soumise au pouvoir hiérarchique du ministre

---

[117] Le Conseil d'Etat, dans son rapport de 1995 consacré aux pouvoirs de l'administration dans le domaine des sanctions, affirmait que « *les sanctions sont d'une nature essentiellement répressive. Elles procèdent d'une intention de punir un manquement à une obligation. Elles se fondent sur un comportement personnel considéré comme fautif* ». Elles se distinguent ainsi des mesures de police administrative en ce qu'elles visent à punir une personne qui a enfreint une réglementation préexistante et non à prévenir des troubles à l'ordre public.

[118] CE, 5 mai 1944, Dame Veuve Trompier-Gravier, Rec. p. 133.

[119] Loi relative au développement de la prévention des accidents du travail, 2 décembre 1976, n° 76-70 DC.

[120] Loi pour l'égalité des chances, 30 mars 2006, n° 2006-535 DC.

[121] Loi relative à la liberté de communication, 17 janvier 1989, n° 88-248 DC.

[122] M. Stéphane R. et autres, 24 octobre 2014, n° 2014-423 QPC.

La portée de ces principes a été singulièrement étendue sous l'influence de l'article 6§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[123] qui implique d'aller au-delà de l'impartialité subjective tenant à l'homme et à son comportement, mais de bien veiller à l'impartialité objective tenant aux fonctions exercées qui sont de nature, indépendamment de ses convictions personnelles, à faire douter de l'indépendance de celui qui les tient[124].

Néanmoins, le respect de ces principes s'impose lorsque la sanction est prononcée par une autorité administrative non soumise au pouvoir hiérarchique du ministre[125].

Le respect de l'impartialité objective et de l'indépendance ne s'impose pas aux autorités administratives placées sous la responsabilité d'un ministre en ce qu'elles ne sauraient être assimilées à un « tribunal » au sens de l'article 6§1[126].

Les exigences de fond liées aux sanctions administratives et pénales

> *Le principe de légalité des délits et des peines, qui s'applique aussi aux sanctions administratives, implique de préciser les obligations auxquelles est soumise une personne*

En matière de sanctions pénales, le Conseil constitutionnel juge que : « *le législateur tient de l'article 34 de la Constitution, ainsi que du principe de légalité des délits et des peines, l'obligation de fixer lui-même le champ d'application de la loi pénale et de définir les crimes et délits en termes suffisamment clairs et précis ; que cette exigence s'impose non seulement pour exclure l'arbitraire dans le prononcé des peines, mais encore pour éviter une rigueur non nécessaire lors de la recherche des auteurs d'infractions* »[127].

En matière de sanctions administratives, le Conseil constitutionnel juge « *qu'appliquée en dehors du droit pénal, l'exigence d'une définition des infractions sanctionnées se trouve satisfaite, en matière administrative, par la référence aux obligations auxquelles le titulaire d'une autorisation administrative est soumis en vertu des lois et règlements* »[128].

Dans sa décision n° 255136 du 7 juillet 2004, le Conseil d'Etat a précisé que « *lorsqu'il est appliqué aux sanctions administratives, le principe de légalité des délits et des peines ne fait*

---

[123] L'article 6§1 de la CESDH pose le principe d'impartialité et d'indépendance des tribunaux en ces termes : « Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. »

[124] CE, 4 juillet 2003, n° 234353.

[125] Société Numéricâble SAS et autre, 5 juillet 2013, n° 2013-331 QPC ; Société Barnes et autre, 9 mars 2017, n° 2016-616/617 QPC.

[126] Voir en ce sens, CE, 27 mars 2000, n° 187703 à propos des pénalités fiscales ; CE, 21 décembre 2018, n° 424520, à propos des sanctions prononcées par l'ANAH.

[127] Loi portant adaptation de la justice aux évolutions de la criminalité, 2 mars 2004, n° 2004-492 DC.

[128] Décision n° 88-248 du 17 janvier 1989.

pas obstacle à ce que les infractions soient définies par référence aux obligations auxquelles est soumise une personne en raison de l'activité qu'elle exerce, de la profession à laquelle elle appartient ou de l'institution dont elle relève ; il implique, en revanche, que les sanctions soient prévues et énumérées par un texte. ».

> *La règle «* non bis in idem *» n'interdit pas le cumul de sanctions administratives et pénales*[129]

Aux termes de l'article 8 de la Déclaration de 1789 : « *La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée* ».

C'est sur le fondement de cet article que le Conseil constitutionnel considère que : « *Les principes ainsi énoncés ne concernent pas seulement les peines prononcées par les juridictions pénales mais s'étendent à toute sanction ayant le caractère d'une punition. Il découle du principe de nécessité des délits et des peines qu'une même personne ne peut faire l'objet de plusieurs poursuites tendant à réprimer de mêmes faits qualifiés de manière identique, par des sanctions de même nature, aux fins de protéger les mêmes intérêts sociaux* »[130].

- S'agissant du premier critère tiré de ce que les sanctions ne tendent pas à réprimer des mêmes faits qualifiés de manière identique

La jurisprudence du Conseil constitutionnel rappelle que la « *seule circonstance que plusieurs incriminations soient susceptibles de réprimer un même comportement ne peut caractériser une identité de faits au sens des exigences résultant de l'article 8 de la Déclaration de 1789 que si ces derniers sont qualifiés de manière identique* ». Le commentaire de cette décision souligne que « *Cette condition tenant à la qualification juridique des faits n'exige pas que les textes définissant les infractions soient strictement identiques* », mais elle «*exclut en revanche que des infractions dont les champs d'application sont très différents et ne se recoupent qu'accessoirement puissent être regardées comme portant sur des faits identiques* »[131].

Il a pu juger, s'agissant de sanctions applicables en cas d'émission de factures de complaisance, que ne pouvaient être regardées comme identiques « *la majoration prévue à l'article 1729 du code général des impôts [qui] sanctionne des manœuvres frauduleuses ayant conduit à éluder*

[129] Si l'article 4 du 7ème protocole additionnel à la Convention européenne de sauvegarde des droits de l'homme garantit ce droit en prévoyant que « *nul ne peut être poursuivi ou puni pénalement par des juridictions du même Etat en raison d'une infraction pour laquelle il a déjà été acquitté ou condamné par un jugement définitif conformément à la loi et à la procédure pénale de l'Etat* », il peut être relevé que la France a émis la réserve suivante au moment de la ratification : « *seules les infractions relevant en droit français de la compétence des tribunaux statuant en matière pénale doivent être regardées comme des infractions au sens des articles 2 à 4 du présent protocole* ». Cette réserve est appliquée par le juge interne (cf. C. cass, 22 janvier 2014 n° 12-83.579).

[130] Par exemple, Société Specitubes, 3 décembre 2021, n° 2021-953 QPC.

[131] M. Jean-Guy C. et autre, 7 mai 2020, n° 2020-838/839.

l'impôt dû par le contribuable. » et les dispositions visant *« , à réprimer le seul recours à des factures de complaisance, indépendamment du fait que des droits aient ou non été éludés »*[132].

- S'agissant du deuxième critère tiré de ce que les répressions ne relèvent pas de corps de règles protégeant les mêmes intérêts sociaux

Ce critère a été décliné expressément dans la décision n° 2019-783 QPC du 17 mai 2019 aux termes de laquelle : « *la sanction financière prononcée par la Commission nationale des comptes de campagne et des financements politiques intervient à l'issue de l'examen par cette commission, sous le contrôle du Conseil constitutionnel, des comptes de campagne de chacun des candidats à l'élection du Président de la République. En conférant à cette sanction un caractère systématique et en prévoyant que son montant est égal au dépassement du plafond des dépenses électorales, le législateur a entendu assurer le bon déroulement de l'élection du Président de la République et, en particulier, l'égalité entre les candidats au cours de la campagne électorale. En revanche, en instaurant une répression pénale des mêmes faits, qui exige un élément intentionnel et permet de tenir compte des circonstances de l'infraction et d'adapter la sévérité de la peine à la gravité de ces faits, le législateur a entendu sanctionner les éventuels manquements à la probité des candidats et des élus.* ».

- S'agissant du troisième et dernier critère tiré de ce que les sanctions doivent être de nature différente

En dehors des cas concernant des sanctions pécuniaires particulièrement importantes, le Conseil constitutionnel conclut systématiquement à l'existence de sanctions de nature différente lorsque l'une d'entre elles seulement comportent une peine d'emprisonnement[133].

Les sanctions sont soumises au principe de proportionnalité des peines

En cas de cumul de sanctions, il est jugé que *: « Si l'éventualité que deux procédures soient engagées peut conduire à un cumul de sanctions, le principe de proportionnalité implique qu'en tout état de cause le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues. »*[134].

1.3. ÉLEMENTS DE DROIT COMPARE

Des mécanismes de contrôle des départs des militaires ou anciens militaires ayant occupé et souhaitant exercer une activité lucrative pour le compte d'un Etat étranger ou d'une entreprise étrangère existent dans d'autres Etats.

[132] Décision n° 2021-942 QPC du 21 octobre 2021.

[133] par exemple : Loi pour une sécurité globale préservant les libertés, 20 mai 2021, n° 2021-817 DC ; Société Clos Teddi et autre, 30 mars 2017, 2016-621 QPC ; M. Pierre M., 29 septembre 2016, 2016-570 QPC.

[134] Par exemple, Société Specitubes, 3 décembre 2021, n° 2021-953 QPC.

Aux Etats-Unis, l'article I, section 9, clause 8, de la Constitution prévoit que « *Aucun titre de noblesse ne sera conféré par les États-Unis, et aucune personne qui tiendra d'eux une charge rémunérée ou de confiance ne pourra, sans le consentement du Congrès, accepter des présents, émoluments, charges ou titres quelconques, d'un roi, d'un prince ou d'un État étranger*. »

Cette clause a été interprétée par les juridictions américaines comme interdisant la réception d'honoraires de consultation, de cadeaux, de frais de voyage ou de salaire par tout le personnel militaire retraité, officier et enrôlé, régulier et de réserve de la part d'un gouvernement étranger, à moins que le consentement du Congrès ne soit obtenu au préalable[135].

L'article 37 section 908 du « United States Code » prévoit à ce titre que « *(a) le Congrès consent à ce que les personnes suivantes acceptent un emploi civil (et la rémunération de cet emploi) pour lequel le consentement du Congrès est requis par le dernier paragraphe de la section 9 de l'article I de la Constitution, relatif à l'acceptation d'émoluments, de charges ou de titres d'un gouvernement étranger :*

(1) Les membres retraités des services en uniforme.

(2) Les membres d'une réserve des forces armées, à l'exception des membres servant sur une période excédant 30 jours.

(3) Membres du corps de réserve du service de santé publique.

(b) Approbation requise - Une personne décrite au paragraphe (a) ne peut accepter un emploi ou une compensation décrits dans ce paragraphe que si le Secrétaire concerné et le Secrétaire d'État approuvent cet emploi. »

Sont considérés comme des émoluments la rémunération d'un emploi provenant d'institutions éducatives ou commerciales étrangères qui sont possédées, exploitées ou contrôlées par un gouvernement étranger car ces entités sont considérées comme une extension du gouvernement étranger.

En cas de non-respect de cette clause, le gouvernement peut demander le recouvrement des sommes perçues et le ministère peut également procéder à la suspension de la pension. Cette clause a pour but de prévenir la corruption et de préserver l'indépendance des Etats-Unis face aux tentatives d'influence étrangère exercées sur ses agents[136].

[135] « The Emoluments Clauses of the U.S. Constitution », Congressional Research Service (CRS), janvier 2021.

[136] « The Foreign Emoluments Clause: Article I, Section 9, Clause 8 », Seth Barrett Tillman, National Constitution Center, https://constitutioncenter.org/the-constitution/articles/article-i/clauses/759.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Comme évoqué au point 1.1, en l'état du droit, aucun dispositif ne permet de faire obstacle au départ de militaires vers des structures étrangères ou des entreprises sous contrôle étranger les embauchant dans l'objectif même d'obtenir de leur part des informations ou savoir-faire à caractère stratégique.

En effet, si les dispositions de l'article L. 4122-5 du code de la défense instituent la commission de déontologie des militaires, sa mission consiste à veiller à la prévention de la commission du délit de prise illégale d'intérêts.

En outre, le code pénal sanctionne le fait de livrer ou de rendre accessibles à une entité étrangère des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la Nation (articles 411-6 à 411-8). La consommation de ces infractions suppose de relever la fourniture, active ou passive, de toute information stratégique dont l'exploitation par une entité étrangère peut porter atteinte à la France.

L'expertise ou le savoir-faire portant sur les modes opératoires ou les spécifications techniques, notamment dans le domaine de la défense, sont couverts par la liste des informations ou objets susceptibles d'entrer dans le champ de ces infractions, celles-ci visant expressément la livraison de renseignements ou de procédés[137].

Il faut cependant établir la matérialité de cette livraison ou cette mise à disposition d'informations pour engager des poursuites pénales. Par ailleurs, ces dispositions qui répriment les faits de trahison n'ont aucun impact, en amont, sur le départ effectif des intéressés vers ces entreprises ou puissances étrangères et le risque qu'il engendre.

Il est vrai que l'article 411-5 réprime le fait d'entretenir des intelligences avec une entité étrangère et l'article 411-7 le fait de recueillir ou de rassembler des informations ou supports en vue de la livraison à une entité étrangère.

Toutefois, les infractions d'intelligences avec une entité étrangère requièrent la démonstration d'un dol, c'est-à-dire que l'auteur a agi volontairement en ayant pleinement conscience de nouer une relation avec une entité étrangère et que cette entente emporte un risque d'atteinte aux intérêts fondamentaux de la Nation (411-5), ou encore que l'auteur a collecté des informations en vue de les livrer à une entité étrangère alors que ces informations sont de nature à porter atteinte à ces intérêts (411-7). La caractérisation de ces infractions pourrait théoriquement être réalisée avant le départ des militaires ou anciens militaires vers l'étranger ; encore faut-il, d'une part, être en capacité de recueillir des éléments de preuve de nature à asseoir les poursuites

[137] Voir par exemple, Cass. crim., 24 juin 1985, n° 83-92.873 : JurisData n° 1985-001833 ; Bull. crim. 1985, n° 247, pour un secret de fabrique.

pénales. Encore faut-il également que l'entretien d'intelligences ou le recueil d'informations interviennent en amont de ce départ.

L'article 411-5 suppose la constatation d'un comportement positif de nature à concrétiser une relation d'entente avec cette entité et caractériser que cette relation est en elle-même de nature à porter atteinte aux intérêts fondamentaux de la Nation. Cette infraction repose sur une certaine dose d'évidence qui pourrait être difficile à établir s'agissant par exemple d'un compétiteur stratégique ou d'un ancien agent plaidant la bonne foi.

L'article 411-7 implique la collecte et/ou la conservation matérielle de données (sur support informatique par exemple). Cette infraction n'est pas adaptée à la seule délivrance d'un savoir-faire opérationnel ou aux activités de consultance, sauf à établir que la personne a constitué un dossier ou photocopié des manuels, des spécifications techniques en vue de livrer ces informations stratégiques à une entité étrangère.

Ainsi, seule l'institution d'un contrôle préventif, assortie de sanctions en cas de méconnaissance des dispositions en cause (prenant notamment la forme de la création d'un délit-obstacle, dont la constatation sera aisée), serait de nature à prévenir efficacement le risque que des militaires soient recrutés par une puissance étrangère pour l'exploitation de leur savoir-faire opérationnel.

Elle nécessite l'intervention du législateur au titre de l'article 34 de la Constitution en ce que ce contrôle met en cause « *les garanties fondamentales accordées aux fonctionnaires civils et militaires de l'Etat* », « *la détermination des crimes et délits ainsi que les peines qui leur sont applicables* » ainsi que « *les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » et « *les sujétions imposées par la Défense nationale aux citoyens en leur personne et en leurs biens* ».

2.2. OBJECTIFS POURSUIVIS

L'objectif poursuivi est d'instituer un contrôle préventif de l'administration concernant les départs des militaires, qui disposent de compétences ou de savoir-faire sensibles, vers des puissances ou des entreprises sous contrôle étranger afin d'éviter des divulgations de nature à porter atteinte aux intérêts fondamentaux de la Nation.

L'enjeu réside dans l'effectivité de ce dispositif en agissant sur :

- la définition de l'étendue des fonctions occupées soumises à ce contrôle ;
- la définition de l'étendue des entreprises concernées par ce contrôle ;
- la durée pendant laquelle ce contrôle sera exercé ;
- les critères sur le fondement desquels l'administration pourra s'opposer au départ de l'intéressé ;
- les sanctions qu'encourt l'intéressé en cas de méconnaissance ou d'absence de déclaration préalable auprès du ministre.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Au regard des enjeux et des problématiques qui sont en cause, seule l'institution d'un contrôle préventif de l'administration, assorti de sanctions, à l'instar de ce que prévoit la législation américaine, apparaît pertinente (cf. item « nécessité de légiférer » *supra*).

Une option envisagée consistait à instituer un régime d'autorisation préalable par le ministre, sans laquelle la personne concernée ne pouvait commencer à exercer l'activité envisagée au bénéfice d'une puissance étrangère.

Toutefois, ce dispositif présentait plusieurs inconvénients.

D'une part, il porte une atteinte plus grande à la liberté d'entreprendre, constitutionnellement protégée, qu'un régime déclaratif.

D'autre part, il impose au ministre de statuer expressément sur chacune des demandes d'autorisation portées devant lui. En effet, dès lors que la finalité du dispositif est la préservation des intérêts fondamentaux de la Nation, le silence gardé sur de telles demandes vaut nécessairement rejet[138].

A l'inverse, le régime déclaratif n'appelle de décision explicite du ministre que si le projet du militaire doit être empêché ; il permet ainsi à l'administration de concentrer son instruction sur les situations potentiellement les plus problématiques, sans risquer de retarder les projets professionnels de militaires ne soulevant aucune difficulté.

3.2. DISPOSITIF RETENU

Le dispositif retenu a pour objet d'instituer un régime de déclaration préalable au départ des intéressés.

Il a pour effet d'imposer au militaire, titulaire de fonctions particulièrement sensibles et qui souhaite exercer une activité en échange d'un avantage personnel ou d'une rémunération au profit d'un Etat étranger ou d'une entreprise ou d'une organisation ayant son siège en dehors du territoire national ou sous contrôle étranger, de le déclarer préalablement au ministre de la défense, en respectant un délai minimal de préavis fixé par décret en Conseil d'Etat.

[138] Conformément au 4° de l'article L. 231-4 du code des relations entre le public et l'administration, qui prévoit que, « *par dérogation à l'article L. 231-1, le silence gardé par l'administration pendant deux mois vaut décision de rejet (…) dans les cas, précisés par décret en Conseil d'Etat, où une acceptation implicite ne serait pas compatible avec (...) la protection de la sécurité nationale, la protection des libertés et des principes à valeur constitutionnelle et la sauvegarde de l'ordre public* ».

La même obligation s'applique dans les dix années suivant la cessation des fonctions sensibles.

Le dispositif ne s'appliquera pas à tous les militaires qui projettent d'exercer une activité lucrative pour un Etat étranger ou une entreprise étrangère. Il est, au contraire, doublement limité :

1/ Du point de vue des fonctions passées occupées par le militaire : il ne peut s'agir que de fonctions présentant, indépendamment du grade, une sensibilité particulière ou requérant des compétences techniques spécialisées. La disposition renvoie au règlement le soin d'en préciser la liste, qui pourra ainsi être actualisée de manière souple en fonction de l'évolution des enjeux pour les intérêts fondamentaux de la Nation.

A ce titre, paraissent devoir être soumis à ce contrôle les emplois de pilotes de chasse, ainsi que certains emplois sensibles relevant :

- du commandement dans le domaine naval (notamment s'agissant des sous-marins) ;
- de la cyberdéfense ;
- du secteur du nucléaire.

Un décret en Conseil d'Etat définira ainsi les domaines d'emplois dont relèvent ces fonctions, lesquelles seront précisées par un arrêté du ministre de la défense. Cet arrêté ne sera pas publié, dès lors qu'il comportera la liste des fonctions les plus sensibles pour les intérêts fondamentaux de la Nation au sein des armées.

Cette dispense de publication (qui fait écho à la dispense de publication de la liste des opérateurs d'importance vitale, prévue à l'article R. 1332-3 du code de la défense) répond ainsi aux exigences inhérentes à la protection des intérêts de la défense nationale. Les militaires concernés seront individuellement informés du fait qu'ils occupent ou ont occupé ces fonctions sensibles et qu'ils entrent, par conséquent, dans le champ de l'obligation de déclaration. Cette information leur sera délivrée :

- pour les militaires en activité, dès leur prise de fonctions sensibles, ou, pour ceux les exerçant déjà à la date d'entrée en vigueur de la loi, en cours d'affectation ;
- pour les anciens militaires ayant déjà quitté les armées à la date d'entrée en vigueur de la loi et ayant exercé de telles fonctions sensibles au sein des armées au cours des dix années précédentes, l'information pourra leur être délivrée à l'occasion des rappels les concernant en tant que réservistes soumis à l'obligation de disponibilité (article L. 4231-2 du code de la défense).

2/ Du point de vue des emplois que le militaire ou ancien militaire souhaite exercer pour le compte d'un Etat étranger ou d'une société étrangère.

S'agissant du périmètre des entreprises concernées, le choix a été fait de retenir le même que celui retenu par les articles 411-6 à 411-8 du code pénal relatifs aux atteintes aux intérêts fondamentaux de la Nation, pour des raisons de cohérence et d'effectivité du dispositif global.

Néanmoins, le dispositif ne s'appliquera que si l'emploi projeté dans l'une de ces entreprises ou Etats relève du domaine de la défense ou de la sécurité.

En effet, il n'est pas exclu qu'en sus de la méconnaissance du dispositif projeté, une méconnaissance d'un des articles précités du code pénal, par la livraison de connaissances techniques, soit caractérisée. Or, il faut permettre à l'autorité administrative d'exercer, avec efficacité, ses prérogatives tirées de l'article 40 du code de procédure pénale afin que l'ensemble des infractions pénales relevées puissent être sanctionnées par le juge. Le champ d'application de ces dispositions parait alors devoir être aligné.

Le dispositif retenu prévoit que l'obligation de déclaration s'applique dans les dix années suivant la cessation des fonctions sensibles précédemment exercées. Ces dispositions sont inspirées de celles prévues par l'article 9-2 de l'ordonnance n° 58-1270 du 22 décembre 1958 portant loi organique relative au statut de la magistrature concernant le départ des magistrats vers les entreprises privées.

La durée de dix ans a été retenue car elle permet d'assurer une conciliation équilibrée entre les droits et libertés du militaire ou de l'ancien militaire (liberté contractuelle, libre circulation) et l'exigence constitutionnelle tenant à la sauvegarde des intérêts fondamentaux de la Nation à laquelle participe la protection, pour une durée nécessairement longue, de savoir-faire militaires dans des domaines très sensibles. Par ailleurs, au terme du délai de dix ans, l'intérêt des compétiteurs étrangers au recrutement d'anciens militaires sera atténué compte tenu de la perte des connaissances acquises par ces derniers avec l'écoulement du temps.

Il prévoit, en outre, que le ministre des armées peut s'opposer à l'exercice de cette activité lorsqu'il estime que celui-ci comporte le risque d'une divulgation par l'intéressé de renseignements, procédés, objets, documents, données informatisées ou fichiers auxquels il a eu accès dans le cadre de ses fonctions et que cette divulgation est de nature à porter atteinte aux intérêts fondamentaux de la Nation. A l'instar de ce qui a été souligné précédemment, la rédaction s'aligne sur celle des articles 411-6 à 411-8 du code pénal.

Cette opposition prononcée par l'autorité administrative pourra être fondée sur un faisceau d'indices tels que le degré d'expertise de l'intéressé, la nature des activités de l'opérateur étranger qu'il souhaite rejoindre, les relations des actionnaires avec des puissances étrangères hostiles ou non-alliées, comme la qualité et l'intensité des relations diplomatiques avec l'Etat considéré. Le ministre prendra sa décision au vu :

- des éléments fournis dans sa déclaration par le militaire, à qui il reviendra de décrire avec précision la nature des missions qui sont susceptibles de lui être confiées dans le cadre de l'emploi auquel il aspire ;
- des informations ou renseignements que lui donneront les états-majors, directions et services du ministère (en particulier la direction générale de l'armement, les services spécialisés de renseignement ou la direction générale des relations internationales et stratégiques), sur la sensibilité opérationnelle des informations et savoir-faire détenus

par le militaire et la qualité de la relation bilatérale avec l'Etat étranger en cause (en particulier, le degré de coopération militaire entretenu, le cas échéant, dans le domaine concerné) ;

- le cas échéant, des observations complémentaires, écrites ou orales du demandeur, qu'il appartiendra au ministre de solliciter s'il envisage de lui opposer une décision de refus pour des motifs ne figurant pas dans la demande initiale.

Ainsi, au cas par cas, le ministre pourra s'opposer au départ d'un militaire détenteur d'un savoir-faire spécifique vers un opérateur étranger, par exemple si l'Etat en question est en un compétiteur stratégique et/ou si le projet professionnel génère un risque fort d'atteinte aux intérêts fondamentaux de la Nation. A l'inverse, si l'Etat dont l'opérateur étranger relève est partie à une alliance militaire avec la France impliquant des coopérations techniques régulières dans le domaine considéré, le ministre ne s'opposera pas au départ du militaire.

En cas de méconnaissance de l'obligation de déclaration préalable auprès du ministre de la défense ou de l'opposition prononcée par le ministre, il prévoit que cela emporte nullité de plein droit du contrat conclu en vue de l'exercice de l'activité privée ainsi que la possibilité pour l'autorité administrative de prononcer des sanctions administratives avec le retrait des décorations obtenues ou des retenues sur pension, ne pouvant excéder 50 % du montant de la pension, pour la durée d'exercice de l'activité illicite, dans la limite de dix ans.

La disposition portant sur la nullité du contrat s'inspire de l'article 23 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique qui prévoit qu'en cas d'avis d'incompatibilité émis par la Haute Autorité pour la transparence de la vie publique (HATVP) les actes et contrats conclus en vue de l'exercice de cette activité « cessent de produire leurs effets » (lorsque la HATVP avait été saisie par l'intéressé lui-même) ou « sont nuls de plein droit » (lorsque la Haute Autorité a été saisie par son président dans les deux mois suivant la connaissance de l'exercice non autorisé d'une activité privée par l'intéressé). Cet article a été jugé conforme à la Constitution[139], au regard notamment du principe de la liberté d'entreprendre, au regard de l'objectif d'intérêt général de prévention des conflits d'intérêts. Cette sanction trouvera en particulier une effectivité si le contrat est conclu et exécuté au profit d'une entité étrangère sur le territoire national. Il convient en effet de préciser qu'en ce qui concerne les contrats de droit étranger exécutés en France, les dispositions législatives proposées constitueront une loi de police opposable[140].

[139] Décision n° 2013-676 DC du 9 octobre 2013, cons. 55 et 56.

[140] Voir, en ce sens, C . Cass., crim., 2 octobre 2018, N° 11-88.040 15-80.735, Ryanair : *« qu'il convient de rappeler que le pays où s'exerce l'activité du travailleur peut imposer l'application des lois de police dont la définition est donnée à l'article 9 du règlement CE numéro 593/2008 sur la loi applicable aux obligations contractuelles (Rome I): «une loi de police est une disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application, quelle que soit par ailleurs la loi applicable au contrat d'après le présent règlement».*

Les dispositions portant sur les retenues sur pension s'inspirent de l'article L. 124-20 du code général de la fonction publique qui prévoit ce type de sanctions pour les agents publics civils en cas de méconnaissance de l'avis de la HATVP.

Le prononcé des sanctions administratives ainsi prévues ne pourra intervenir qu'à l'issue de la mise en œuvre d'une procédure contradictoire, sans que la loi ait à le prévoir expressément, s'agissant d'un principe général du droit.

Enfin, l'article sanctionne pénalement le fait d'exercer une telle activité sans avoir procédé à l'obligation de déclaration préalable auprès du ministère de la défense (cinq ans d'emprisonnement et 75 000 euros d'amende). La sanction pénale sera ainsi encourue soit que la personne n'ait pas respecté son obligation de déclaration auprès du ministre avant de commencer à exercer un emploi dans le domaine de la défense et de la sécurité auprès d'un Etat ou d'une entreprise étrangère, soit qu'elle l'ait fait en méconnaissance d'une opposition prononcée par le ministre de la défense. La création de ce délit-obstacle, constitué par un manquement à une obligation objective aisément vérifiable, garantit l'effectivité du dispositif de contrôle préalable.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Le présent article crée deux nouveaux articles (L. 4122-11 et L. 4122-12) dans le chapitre II du titre II du livre Ier de la partie 4 du code de la défense.

L'article L. 4122-11 institue ce contrôle préventif ainsi que les sanctions administratives prévues en cas de méconnaissance de l'obligation de déclaration préalable ou de l'opposition du ministre de la défense.

L'article L. 4122-12 prévoit une peine d'emprisonnement de cinq ans et de soixante-quinze mille euros d'amende en cas de méconnaissance de l'article L. 4122-11.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

La mesure ne peut avoir d'impact que sur les entreprises à l'étranger ou sous contrôle étranger. Cet impact sera en tout état de cause limité, compte tenu du faible nombre de personnes concernées par le contrôle institué par la mesure.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Le périmètre des emplois soumis au nouveau régime de déclaration préalable sera précisé par voie réglementaire.

Les principaux emplois qui seront concernés sont les personnels intervenant dans le Cyber, dans la maintenance aéronautique, dans le pilotage d'aéronefs, dans le domaine du nucléaire, dans le domaine du commandement naval.

A titre informatif, le rapport de la commission de déontologie des militaires pour 2021 indique que le nombre de dossiers déposés s'est élevé à 270 en 2021. Près de 40% de ces militaires sont approchés par des entreprises privées en raison de leur savoir-faire. Le rapport ajoute que, « *depuis 2019, sur les 754 dossiers examinés par la commission en procédure normale, 34 (4,5 %) ont concerné des entreprises étrangères, parfois pour un recrutement en France* ».

Au regard de la nature des nouvelles dispositions, ces demandes nécessiteront une charge de travail supplémentaire soutenable pour les services administratifs du ministère des armées, étant rappelé que le régime déclaratif (et non d'autorisation préalable) leur permettra de se concentrer sur les situations soulevant des difficultés avérées.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Le dispositif a reçu un avis favorable du Conseil supérieur de la fonction militaire le 9 mars 2023.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article entrera en vigueur le lendemain du jour de publication de la loi au *Journal officiel* de la République française.

Concrètement, il s'appliquera à compter de la date d'entrée en vigueur du décret précisant la liste des domaines d'emplois concernés et de l'arrêté du ministre de la défense fixant la liste des fonctions soumises à la procédure de déclaration préalable.

Les anciens militaires ayant déjà commencé, à cette date, l'exercice d'un emploi dans le domaine de la défense et de la sécurité pour le compte d'un Etat ou d'une entreprise étrangère ne seront pas soumis à l'obligation de déclarer leur activité auprès du ministre.

En revanche, tout militaire ou ancien militaire qui, postérieurement à cette même date, a le projet d'exercer un tel emploi, devra préalablement le déclarer au ministre, s'il a exercé au cours des dix années précédentes l'une des fonctions sensibles mentionnées par l'arrêté. Cette obligation lui sera opposable sous réserve d'avoir été individuellement informé qu'il entre dans le champ d'application de l'obligation déclarative.

5.2.2. Application dans l'espace

Le présent article est applicable sur l'ensemble du territoire de la République française. En effet, en tant qu'elles concernent le domaine de la défense, les dispositions sont applicables de plein droit sur tout le territoire, y compris dans les collectivités relevant de l'article 74 de la Constitution.

5.2.3. Textes d'application

Un décret en Conseil d'Etat viendra définir la liste des domaines d'emplois concernés, au sein desquels un arrêté non publié précisera les fonctions précises dont les titulaires ou anciens titulaires entreront dans le champ de l'obligation, ainsi que les modalités procédurales d'application.

Article 21 : Permettre la communication par l'autorité judiciaire aux services de renseignement des éléments d'une procédure ouverte pour crime et délit de guerre ou crime contre l'humanité

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

1.1.1. Les dérogations au secret de l'enquête et de l'instruction

Principe cardinal de la procédure pénale française, le secret de l'enquête et de l'instruction vise à garantir l'efficacité et la sérénité des investigations. Il permet également de protéger la présomption d'innocence des personnes mises en cause et la vie privée des plaignants.

Si ce principe général est posé au premier alinéa de l'article 11 du code de procédure pénale, le législateur a prévu de pouvoir y déroger dans des cas qu'il a strictement encadrés, notamment pour permettre au procureur de la République de communiquer afin d'éviter la propagation d'informations parcellaires ou inexactes sur une enquête pénale en cours[141] ou encore pour permettre à l'administration fiscale d'être informée d'éléments permettant de soupçonner une fraude à l'impôt[142].

Le législateur a, par ailleurs, également tenu compte de la nécessité d'un partage d'informations entre l'autorité judiciaire et des services de renseignement ou services spécialisés. Le procureur de la République antiterroriste (PRAT) et le juge d'instruction peuvent ainsi communiquer aux services spécialisés de renseignement visés à l'article L. 811-2 du code de la sécurité intérieure (dits du premier cercle[143]), de leur propre initiative ou à la demande de ces services, des éléments figurant dans des procédures et nécessaires à l'exercice de leur mission relative à la prévention du terrorisme, pour autant que les informations soient issues de procédures d'enquête ou d'instruction ouvertes en matière de terrorisme (article 706-25-2 du code de procédure pénale[144]).

[141] Article 11 alinéa 3 du code de procédure pénale.

[142] Article L. 101 du livre des procédures fiscales.

[143] Services visés à l'article R. 811-1 du code de la sécurité intérieure : « la direction générale de la sécurité extérieure, la direction du renseignement et de la sécurité de la défense, la direction du renseignement militaire, la direction générale de la sécurité intérieure, le service à compétence nationale dénommé " direction nationale du renseignement et des enquêtes douanières " et le service à compétence nationale dénommé " traitement du renseignement et action contre les circuits financiers clandestins". »

[144] Disposition créée par la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique et modifié par la loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée.

Plus récemment, la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, a prévu deux nouvelles dérogations inscrites à l'article 706-105-1 du code de procédure pénale.

D'une part, l'autorité judiciaire peut désormais transmettre à certains services visés à l'article L. 2321-2 du code de la défense, de sa propre initiative ou à la demande de ces services, des éléments de toute nature nécessaires à l'exercice de leur mission en matière de sécurité et de défense des systèmes d'information[145].

D'autre part, l'autorité judiciaire peut également transmettre à certains services de renseignement, visés aux articles L. 811-2 (dits du premier cercle) et L. 811-4 (dits du deuxième cercle[146]) du code de la sécurité intérieure, des éléments de toute nature nécessaires à l'exercice des missions des services concernés au titre de la prévention de la criminalité et de la délinquance organisées, pour peu que ces éléments apparaissent dans des procédures ouvertes pour des infractions déterminées (trafic de stupéfiants, traite des êtres humains, lutte contre les filières d'immigration clandestine, trafic d'armes).

En tout état de cause, la décision de transmettre revient à l'autorité judiciaire. Les services de renseignement ne peuvent obtenir communication de ces informations que pour des finalités strictement définies et il leur est interdit de les retransmettre à des services de renseignement étrangers.

1.1.2. Les crimes internationaux de la compétence du procureur de la République national antiterroriste

Les crimes contre l'humanité et les crimes et délits de guerre, ainsi que les infractions qui leur sont connexes, sont poursuivis, instruits et jugés selon les dispositions des articles 628 à 628-10 du code de procédure pénale qui organisent notamment la compétence nationale concurrente du procureur de la République antiterroriste et des juges d'instruction de Paris dans cette matière et précisent les spécificités procédurales qui y sont attachées.

Au titre des **crimes contre l'humanité**, le génocide est le fait, en exécution d'un plan concerté tendant à la destruction totale ou partielle d'un groupe national, ethnique, racial ou religieux, ou d'un groupe déterminé à partir de tout autre critère arbitraire, de commettre ou de faire commettre, à l'encontre de membres de ce groupe, une atteinte volontaire à la vie, une atteinte grave à l'intégrité physique ou psychique, une soumission à des conditions d'existence de nature à entraîner la destruction totale ou partielle du groupe, des mesures visant à entraver les naissances ou un transfert forcé d'enfants[147].

[145] Services spécialisés en matière de sécurité des systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, désignés dans l'arrêté du 17 juillet 2015 déterminant les services de l'Etat mentionnés au second alinéa de l'article L. 2321-2 du code de la défense.

[146] Services visés à l'article R. 811-2 du code de la sécurité intérieure.

[147] Article 211-1 du code pénal.

Depuis la loi n° 2010-930 du 9 août 2010 portant adaptation au statut de la Cour pénale internationale, le code pénal sanctionne également la provocation publique et directe, par tous moyens, à commettre un génocide, avec des peines variables suivant que la provocation aura ou non été suivie d'effets[148].

Le code pénal regroupe les « autres crimes contre l'humanité » aux articles 212-1 à 212-3. Constituent ainsi des crimes contre l'humanité les actes limitativement énumérés tels que les atteintes volontaires à la vie, l'extermination, la réduction en esclavage, la déportation ou le transfert forcé de population, la torture ou le viol commis en exécution d'un plan concerté à l'encontre d'un groupe de population civile, dans le cadre d'une attaque généralisée ou systématique.

À la différence du génocide, les motifs ayant conduit à la sélection du groupe victime ne sont pas déterminants. Il suffit que ces actes concernent la population civile.

Les actes précédemment visés constituent également des crimes contre l'humanité lorsqu'ils sont commis en temps de guerre en exécution d'un plan concerté contre ceux qui combattent le système idéologique au nom duquel sont perpétrés des crimes contre l'humanité. Ce texte permet de faire entrer dans le champ d'application des crimes contre l'humanité des crimes qui pourraient être qualifiés par ailleurs de crimes de guerre, lorsqu'ils sont commis à l'encontre de combattants résistants[149].

Est enfin incriminée la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un génocide ou autre crime contre l'humanité. Il s'agit ici d'incriminer à titre principal l'association de malfaiteurs appliquée aux crimes contre l'humanité.

Les **crimes et délits de guerre** sont prévus et réprimés par les articles 461-1 à 462-11 du code pénal. Il s'agit d'actes :

- Énumérés par ces différentes dispositions et visant les personnes et les biens également mentionnés (par exemple, la population civile ou les installations sanitaires),
- Commis lors d'un conflit international ou non international et en relation avec ce conflit,
- Et violant les lois et coutumes de guerre ou les conventions internationales applicables aux conflits armés (par exemple, l'utilisation de gaz toxique).

Sont détaillées ainsi des atteintes à la vie et à l'intégrité physique, des atteintes à la liberté individuelle, des atteintes aux droits de mineurs, des moyens et méthodes de combat prohibés en vertu du droit international humanitaire et des atteintes aux biens, dans le cadre de conflits armés internationaux ou non.

[148] Article 211-2 du code pénal.
[149] Article 212-2 du code pénal.

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel considère qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public, la recherche des auteurs d'infractions et la prévention du renouvellement des infractions ou encore la sauvegarde des intérêts fondamentaux de la Nation, toutes nécessaires à la protection de droits de valeur constitutionnelle parmi les plus fondamentaux et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés.

À l'occasion de l'examen d'une question prioritaire de constitutionnalité, le Conseil constitutionnel a admis que le secret de l'enquête et de l'instruction est une garantie donnée aux citoyens pour assurer à la fois la préservation de l'ordre public en permettant la recherche des auteurs d'infractions, mais aussi une garantie du respect de la présomption d'innocence et de la protection de la vie privée[150]. Il ne peut subir de restriction que si celle-ci est justifiée par un motif d'intérêt général et proportionnée à celui-ci.

Le secret de l'enquête et de l'instruction a deux finalités : « *d'une part, garantir le bon déroulement de l'enquête et de l'instruction, poursuivant ainsi les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, tous deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle [...], d'autre part, protéger les personnes concernées par une enquête ou une instruction, afin de garantir le droit au respect de la vie privée et de la présomption d'innocence, qui résulte des articles 2 et 9 de la Déclaration de 1789* ».

La transmission d'informations, lorsque celles-ci ont la nature de données à caractère personnel doit donc notamment être appréciée au regard du droit au respect de la vie privée et de la présomption d'innocence.

Par ailleurs, le Conseil constitutionnel estime que, si « *aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées* »[151].

La transmission d'informations nominatives à caractère pénal par l'autorité judiciaire doit être justifiée par des impératifs protégeant d'autres droits ou intérêts de même valeur avec lesquels les droits ou intérêts légitimes des personnes concernées doivent se concilier.

[150] V. Conseil constitutionnel, décision n° 2017-693 QPC du 2 mars 2018.

[151] V. Conseil constitutionnel, décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, cons. 32.

1.3. CADRE CONVENTIONNEL

Le droit à la présomption d'innocence, garantie protégée par le secret de l'enquête, est consacré par l'article 11 de la Déclaration universelle des droits de l'homme et par l'article 14 du Pacte des Nations Unies sur les droits civils et politiques. Le paragraphe 2 de l'article 6 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales le consacre également dans des termes qui sont repris à l'article 48 de la Charte des droits fondamentaux de l'Union européenne.

Le droit au respect de la vie privée est garanti par le paragraphe 2 de l'article 8 de la Convention qui précise dans quelles conditions il peut y avoir ingérence dans la jouissance du droit protégé : une telle ingérence doit être « prévue par la loi », poursuivre un « but légitime » et être « nécessaire dans une société démocratique ». Ce droit figure également à l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Par ailleurs, l'article 627 du code de procédure pénale prévoit que, pour l'application du statut de la Cour pénale internationale signé le 18 juillet 1998 et ratifié le 9 juin 2000, la France participe à la répression des infractions et coopère avec cette juridiction.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le rôle des services de renseignement est d'anticiper, de comprendre et d'informer les autorités de l'Etat d'une menace et de prévenir sa réalisation sur le territoire de la République. A ce titre, ils participent à la lutte contre l'impunité des auteurs de crimes internationaux par la collecte et l'analyse de renseignements relatifs à des individus ou des groupes déterminés, le cas échéant positionnés à l'extérieur du territoire de la République.

Or, les procédures judiciaires peuvent comporter des informations qui, au-delà de leur valeur probatoire permettant la caractérisation de l'infraction poursuivie, révèlent ou documentent l'existence d'une menace distincte qui ne se matérialise pas par la commission d'une infraction. Certains éléments de ces enquêtes pénales peuvent alors se révéler déterminants pour les services de renseignement.

Comme indiqué plus haut, des dispositions législatives permettant des échanges d'informations entre autorité judiciaire et services de renseignement ont été introduites en matière de lutte contre le terrorisme ainsi qu'en matière de criminalité organisée et de lutte contre les cyberattaques.

Une telle disposition n'existe pas pour les procédures d'enquête ou d'instruction portant sur des faits de crimes et délits de guerre et de crimes contre l'humanité, quand bien même elles révèleraient des renseignements ou informations nécessaires à l'exercice des missions des services concernés. /

La situation au Sahel ou au Levant et plus récemment la guerre en Ukraine ont mis en exergue le besoin d'élargir la possibilité pour le procureur de la République antiterroriste ou pour le juge d'instruction de communiquer aux services de renseignement des éléments relatifs aux procédures portant sur les violations les plus graves des normes fondamentales du droit international.

Le rôle de ces services, comme le rythme des enquêtes judiciaires sur les crimes internationaux, ont évolué dans le cadre des nouvelles formes de conflits armés. Les enquêtes pénales se déroulent concomitamment aux évènements susceptibles d'être qualifiés de crimes contre l'humanité ou crimes de guerre, nécessitant une plus grande réactivité et plus d'échanges entre les autorités judiciaires et les services spécialisés de renseignement.

Or, la transmission d'information par l'autorité judiciaire aux services de renseignement est de nature à permettre préventivement d'empêcher notamment la fuite des criminels de guerre ou encore leur entrée sur le territoire de l'Union européenne.

Une personne impliquée dans des crimes de guerre peut également être suivie par un service de renseignement afin de s'assurer de la nature de la menace qu'il représente, à raison de ses contacts, de ses activités, ou de tout autre critère.

De façon plus générale, les services spécialisés doivent pouvoir continuer de collecter et traiter les informations nécessaires à leurs missions préventives d'évaluation de la menace, notamment sur les individus ou groupes divers positionnés à l'extérieur du territoire, dès lors que la légitimité du droit d'en connaître a été validée par la seule autorité judicaire.

Cette transmission d'éléments de procédure peut être essentielle à leur mission de collecte et d'exploitation des renseignements relatifs aux enjeux géopolitiques et stratégiques et à la défense des intérêts fondamentaux de la Nation, telle que l'exécution des engagements européens et internationaux de la France ou la prévention de toute forme d'ingérence étrangère.

Aussi paraît-il nécessaire de prévoir une disposition permettant, par dérogation à l'article 11 du code de procédure pénale, au Parquet national antiterroriste (PNAT) ou aux juges d'instruction saisis de transmettre aux services spécialisés de renseignement visés à l'article L. 811-2 du code de la sécurité intérieure (premier cercle), des éléments figurant dans des procédures ouvertes des chefs de crimes et délits de guerre ou de crimes contre l'humanité.

Cette dérogation à l'article 11 du code de procédure pénale doit être instaurée par une norme de niveau équivalent.

2.2. OBJECTIFS POURSUIVIS

L'objectif est de transposer et d'adapter le mécanisme déjà existant à l'article 706-25-2 du code de procédure pénale, en matière de terrorisme, en l'élargissant aux procédures ouvertes pour crimes et délits de guerre ou crimes contre l'humanité, et de permettre ainsi au parquet anti-terroriste de transmettre aux services de renseignement les informations qu'il y aurait découvert et qu'il estimerait nécessaires à l'accomplissement de leurs missions.

Le Parquet national antiterroriste dispose en effet, au-delà de sa compétence en matière de terrorisme, d'une compétence nationale concurrente, en application de l'article 628-1 du code de procédure pénale, pour les crimes contre l'humanité et les crimes de guerre.

Cette extension permettrait ainsi d'unifier ses prérogatives : les transmissions d'informations issues d'une procédure suivie par le PNAT vers les services de renseignement du premier cercle obéiront pour les principales infractions relevant de sa compétence au même régime[152].

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Conformément à l'article 34 de la Constitution, les dispositions de procédure pénale, en l'espèce s'agissant de dispositions relatives au secret de l'enquête et de l'instruction, relèvent du domaine de la loi. Un vecteur réglementaire ou infra-réglementaire contreviendrait aux règles fixant le domaine d'intervention respectif de la loi et du règlement.

L'intégration de la disposition après l'article 11-2 du code de procédure pénale aurait pu être envisagée. Cependant, au vu de l'architecture retenue dans ce code pour intégrer les dispositifs analogues, cet article trouve plus opportunément sa place au sein du sous-titre II du même code, consacré aux juridictions compétentes pour la poursuite, l'instruction et le jugement des crimes contre l'humanité et des crimes et délits de guerre.

3.2. OPTION RETENUE

Il est prévu de transposer et d'adapter le mécanisme existant à l'article 706-25-2 du code de procédure pénale en matière de terrorisme au contentieux spécifique des crimes contre l'humanité et des crimes et délits de guerre.

Après l'article 628-8 du code de procédure pénale, un nouvel article 628-8-1 est créé au sein du sous-titre II du titre Ier du livre IV du même code.

---

[152] Le Parquet national antiterroriste dispose d'une compétence nationale concurrente également pour les infractions relatives à la prolifération d'armes de destruction massive et leurs vecteurs (articles 706-167 à 706-174 du code de procédure pénale) et pour les crimes de tortures commises par les autorités étatiques et les crimes de disparitions forcées (article 628-10 du code de procédure pénale).

Ce nouvel article permet d'élargir aux enquêtes ouvertes pour crimes contre l'humanité ou crimes et délits de guerre la possibilité pour le procureur de la République antiterroriste ou le juge d'instruction en cas d'information judiciaire de communiquer aux services de renseignement des éléments d'une procédure en cours et ainsi d'unifier le régime applicable au Parquet national antiterroriste pour les principales infractions relevant de sa compétence, compte tenu des possibilités déjà ouvertes en matière de terrorisme.

Pour limiter l'atteinte portée au secret de l'enquête et de l'instruction, à la protection de la vie privée et à la présomption d'innocence, les éléments ainsi transmis ne pourront être obtenus par ces services que pour le seul exercice de leurs missions au titre de la défense des intérêts fondamentaux de la Nation mentionnés aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du code de la sécurité intérieure[153].

Il apparaît ainsi nécessaire de prévoir une possible communication quand des éléments d'une procédure sont en corrélation avec certains domaines d'action des services de renseignement, spécifiquement leurs missions relatives à l'indépendance nationale, l'intégrité du territoire et la défense nationale, aux intérêts majeurs de la politique étrangère, à l'exécution des engagements européens et internationaux de la France et à la prévention de toute forme d'ingérence étrangère, à la prévention du terrorisme, à la prévention de la criminalité organisée ainsi qu'à la prévention de la prolifération des armes de destruction massive.

Par exemple, dans le cadre d'une enquête ouverte pour des faits de crimes contre l'humanité, des actes de procédure peuvent permettre aux services de renseignement de poursuivre une opération de prévention du terrorisme et de lutte contre la prolifération d'armes de destruction massive. Une personne mise en cause pour des crimes de guerre peut tout autant justifier, dans le cadre des dispositions du code de la sécurité intérieure, la collecte ou l'exploitation de renseignements pour son implication dans un réseau transnational de criminalité organisée.

Cette correspondance entre les procédures pour crimes et délits de guerre ou crimes contre l'humanité et les missions mentionnées aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du code de la sécurité intérieure tient compte d'une certaine porosité entre les différents faits criminels et de la diversification de certains individus ou groupes déterminés dans leurs activités.

Par ailleurs, si la procédure fait l'objet d'une information, cette communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction. Ce dernier peut également procéder à cette communication pour les procédures d'information dont il est saisi après avoir recueilli l'avis du procureur de la République antiterroriste.

Les informations communiquées en application de cet article ne pourront faire l'objet d'un échange avec des services de renseignement étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement. Il s'agit d'une adaptation renforcée de la règle de coopération internationale qui impose qu'un service de renseignement destinataire d'informations émanant d'un autre service de renseignement ne peut les retransmettre à un autre

[153] 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; 4° La prévention du terrorisme ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive.

service (service tiers) qu'avec l'accord du service émetteur. En l'espèce, plus strictement, aucune transmission des éléments de procédure communiqués initialement par le Parquet national antiterroriste ou le magistrat instructeur ne peut être autorisée.

Toute personne qui en sera rendue destinataire sera tenue au secret professionnel, dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal (alinéa 4 du nouvel article 628-8-1 du code de procédure pénale).

En outre, pour limiter l'atteinte portée au secret de l'enquête, à l'instar de l'article 706-25-2 du code de procédure pénale, seuls les services de renseignement dits du premier cercle visés à l'article L. 811-2 du code de la sécurité intérieure pourront bénéficier de ces dispositions et tant le procureur de la République antiterroriste que le juge d'instruction conserveront la faculté d'apprécier l'opportunité de transmettre les informations sollicitées. La requête formulée par le service de renseignement sera susceptible d'être rejetée par l'autorité judiciaire si, en droit et en fait, les conditions ne sont pas réunies pour justifier la mise en œuvre de cette procédure dérogatoire à l'article 11 du code de procédure pénale.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La mesure envisagée nécessite la création, après l'article 628-8 du code de procédure pénale, d'un article 628-8-1, au sein du sous-titre II du même code, consacré aux juridictions compétentes pour la poursuite, l'instruction et le jugement des crimes contre l'humanité et des crimes et délits de guerre. Cette disposition sera rédigée dans des termes analogues à ceux de l'article 706-25-2 et adaptée au contentieux des crimes supranationaux.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les modifications législatives ne méconnaissent aucune règle issue du droit international ou du droit de l'Union européenne.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES JUDICIAIRES

Cette mesure pourrait générer une charge supplémentaire pour le Parquet national antiterroriste, qui devrait néanmoins rester limitée. Si en l'état, un peu plus de 160 procédures sont suivies par les juridictions spécialisées pour des crimes internationaux (enquêtes préliminaires ou informations judiciaires), cette disposition ne créera pas d'obligation de transmission à la charge de l'autorité judiciaire mais seulement une faculté lui permettant d'apprécier la nécessité de mettre en œuvre cette dérogation à l'article 11 du code de procédure pénale dans certains dossiers dans lesquels les pièces de procédure sont susceptibles de permettre aux services de renseignement d'assurer leurs missions.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal Officiel* de la République française.

S'agissant d'un texte fixant les modalités de poursuites et les formes de la procédure, il est d'application immédiate aux procédures pénales en cours[154].

5.2.2. Application dans l'espace

Ces dispositions ont vocation à s'appliquer dans les collectivités d'Outre-mer régies par l'article 73 de la Constitution du fait du principe d'identité législative sans qu'il soit requis d'en faire mention expresse.

Dans les collectivités d'Outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie soumises au régime de spécialité législative, une mention expresse d'application est nécessaire afin de rendre ces dispositions applicables[155] via la mise à jour de l'article 804 du code de procédure pénale modifié à cette fin par l'article 36 du présent projet de loi.

---

[154] Article 112-2 du code pénal.

[155] Cf. article 7 de la loi organique n° 2004-192 du 27 février 2004 pour la Polynésie Française ; article 4 de la loi n° 61-814 du 29 juillet 1961 pour les îles Wallis et Futuna ; article 6-2 de la loi n° 99-209 organique du 19 mars 1999 pour la Nouvelle-Calédonie ; article 1-1 de la loi n° 55-1052 du 6 août 1955 pour les Terres australes et antarctiques françaises.

Par ailleurs, aucune adaptation de ces dispositions tenant aux caractéristiques des collectivités n'apparaît nécessaire.

Ces mesures sont donc applicables sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Les présentes dispositions n'appellent aucune mesure réglementaire d'application.

Article 22 : Protéger l'anonymat des anciens agents des services de renseignement ou des anciens membres des forces spéciales ou unités d'intervention spécialisées dans le cadre des procédures judiciaires

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Les agents des services de renseignement et les membres des unités des forces spéciales ou des unités d'intervention spécialisées dans la lutte contre le terrorisme bénéficient de deux dispositifs de protection pénale ou judiciaire de leur anonymat.

1.1.1. La protection pénale renforcée contre la révélation de leur(s) identité(s) ou de leur appartenance au service

Cette protection pénale est assurée par les articles 413-13 et 413-14 du code pénal. La révélation de toute information qui pourrait conduire, directement ou indirectement, à la découverte de l'usage, en application de l'article L. 861-2 du code de la sécurité intérieure, d'une identité d'emprunt ou d'une fausse qualité, de l'identité réelle d'un agent d'un service mentionné à l'article L. 811-2 du même code ou d'un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 dudit code ou de son appartenance à l'un de ces services est punie de cinq ans d'emprisonnement et de 75 000 € d'amende.

Les articles L. 811-2 et L. 811-4 du code de la sécurité intérieure déterminent les services spécialisés de renseignement dits du « premier cercle[156] » et les services dits du « second cercle[157] » concernés par cette protection.

Les alinéas 2 et 3 de l'article 413-13 du code pénal prévoient des peines aggravées en cas de résultat dommageable survenu à la suite de la révélation sur les agents ou leurs proches (atteinte physique ou psychique, mort).

La révélation commise par négligence ou imprudence par une personne dépositaire de l'information dans le cadre professionnel est également réprimée à l'alinéa 4.

[156] Services visés à l'article R. 811-1 du code de la sécurité intérieure : « la direction générale de la sécurité extérieure, la direction du renseignement et de la sécurité de la défense, la direction du renseignement militaire, la direction générale de la sécurité intérieure, le service à compétence nationale dénommé " direction nationale du renseignement et des enquêtes douanières " et le service à compétence nationale dénommé " traitement du renseignement et action contre les circuits financiers clandestins". »

[157] Services visés à l'article R. 811-2 du code de la sécurité intérieure.

L'alinéa 5 confère une protection similaire aux sources ou collaborateurs du service concerné.

Depuis 2016, un dispositif analogue est prévu à l'article 413-14 du code pénal[158], au sein d'une section nouvellement dénommée « Des atteintes à certains services ou unités spécialisés », au bénéfice des membres des unités des forces spéciales désignées par arrêté du ministre de la défense ou des unités d'intervention spécialisées dans la lutte contre le terrorisme désignées par arrêté du ministre de l'intérieur[159].

L'objectif de ces dispositions est de préserver la confidentialité et l'effet de surprise que requièrent les opérations militaires non conventionnelles, mais aussi de consentir aux membres des forces spéciales une protection inspirée de celle dévolue aux agents de renseignement dont ils prolongent l'action et qui sont exposés aux mêmes menaces.

1.1.2. La protection judiciaire de leur anonymat en cas d'audition en qualité de témoin dans le cadre d'une procédure pénale

Au titre IV *bis* du code de procédure pénale intitulé « De la manière dont sont reçues les dépositions des personnels de certains services ou unités spécialisés », l'article 656-1 prévoit que lorsque le témoignage d'un agent d'un service mentionné à l'article L. 811-2 du code de la sécurité intérieure ou d'un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 du même code ou d'une personne mentionnée à l'article 413-14 du code pénal est requis au cours d'une procédure judiciaire sur des faits dont il aurait eu connaissance lors d'une mission intéressant la défense et la sécurité nationale, son identité réelle ne doit jamais apparaître au cours de la procédure judiciaire.

Le cas échéant, son appartenance à l'un de ces services et la réalité de sa mission sont attestées par son autorité hiérarchique. Les questions posées ne doivent avoir ni pour objet ni pour effet de révéler, directement ou indirectement, la véritable identité de cet agent. Les auditions sont reçues dans des conditions permettant la garantie de son anonymat.

S'il est indiqué par l'autorité hiérarchique que l'audition requise, même effectuée dans les conditions d'anonymat indiquées aux premier et troisième alinéas, comporte des risques pour l'agent, ses proches ou son service, cette audition est faite dans un lieu assurant l'anonymat et la confidentialité. Ce lieu est choisi par le chef du service et peut être le lieu de service d'affectation de l'agent.

Si une confrontation doit être réalisée entre une personne mise en examen ou comparaissant devant la juridiction de jugement et un agent mentionné au premier alinéa en raison des éléments de preuve à charge résultant de constatations personnellement effectuées par cet agent, cette confrontation est réalisée dans les conditions prévues par l'article 706-61 du code de

[158] Loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires.

[159] Arrêté du 20 octobre 2016 relatif à la préservation de l'anonymat des membres des unités des forces spéciales et arrêté du 25 juin 2018 relatif à la préservation de l'anonymat des membres des unités d'intervention spécialisées dans la lutte contre le terrorisme.

procédure pénale, soit par l'intermédiaire d'un dispositif technique permettant l'audition à distance du témoin, sa voix étant rendue non identifiable par des procédés techniques appropriés.

Ce cadre procédural n'est naturellement pas applicable aux personnels qui seraient mis en cause dans le cadre d'une enquête pénale, cette disposition ne constituant aucunement une cause d'irresponsabilité pénale.

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel se livre à un contrôle strict des textes limitant la liberté d'expression et de communication. Pour lui, les « *atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées, et proportionnées à l'objectif poursuivi* », critères se déduisant de l'article 11 de la Déclaration de 1789[160].

Concernant le dispositif parallèle d'incrimination de la révélation d'identité des agents spécialisés, la chambre criminelle de la Cour de cassation a été saisie d'une question prioritaire de constitutionnalité en 2013 portant sur l'article 413-13 du code pénal qui, selon le requérant, portait une atteinte disproportionnée à la liberté d'expression garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen, l'objectif à valeur constitutionnelle de recherche des auteurs d'infractions et enfin au droit des personnes à exercer un recours juridictionnel effectif garanti par l'article 16 de cette même Déclaration.

La Cour de cassation y a répondu par la négative, disant n'y avoir lieu de renvoyer la QPC au Conseil constitutionnel, considérant que l'article 413-13, alinéa 1er, du code pénal se contente de créer une limite à la liberté d'information concernant l'identité des agents des services de renseignement, justifiée par la protection des intérêts fondamentaux de la Nation et de la sécurité des intéressés, tant que ceux-ci remplissent leur mission dans le respect des lois, la Cour observant que le texte n'institue aucune immunité pénale au bénéfice des intéressés qui se seraient rendus coupables de crimes ou de délits[161].

Par ailleurs, l'article 16 de la Déclaration des droits de l'homme et du citoyen assure la « garantie des droits », au titre de laquelle sont protégés, en tant que principes constitutionnels, les droits de la défense et le principe du contradictoire qui en est le corollaire. Dans ce cadre, le Conseil constitutionnel juge :

- que le principe du contradictoire et le respect des droits de la défense impliquent en particulier qu'une personne mise en cause devant une juridiction répressive ait été mise en mesure, par elle-même ou par son avocat, de contester les conditions dans lesquelles ont été recueillis les éléments de preuve qui fondent sa mise en cause[162] ;

[160] V. CC, décision n° 2010-3 QPC, *Union des familles en Europe [Associations familiales],* 28 mai 2010, cons. 6.

[161] Crim., QPC, 17 avr. 2013, n° 13-90.009 : https://www.legifrance.gouv.fr/juri/id/JURITEXT000027365440.

[162] V. CC, décision n° 2014-693 DC, *Loi relative à la géolocalisation*, 25 mars 2014.

– qu'il appartient au législateur d'assurer la conciliation entre, d'une part, les droits de la défense et le principe du contradictoire et, d'autre part, l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation[163].

Dans sa décision n° 2019-778 DC du 21 mars 2019, le Conseil constitutionnel a validé les dispositions de l'article 15-4 du code de procédure pénale permettant aux agents de la police nationale ou de la gendarmerie nationale de ne pas être identifiés par leurs noms et prénoms dans certains actes de procédure dans lesquels ils interviennent, après avoir relevé que l'anonymat de ces agents n'est préservé que lorsque la révélation de leur identité serait susceptible de mettre en danger leur vie ou celle de leurs proches. Dans ces conditions, il a jugé que le législateur avait procédé à une conciliation équilibrée entre la prévention des atteintes à l'ordre public et l'exercice des droits et libertés constitutionnellement garantis, au nombre desquels figurent les droits de la défense.

1.3. CADRE CONVENTIONNEL

L'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales garantit le droit au procès équitable, qui implique le respect des droits de la défense et commande en matière pénale de donner à l'accusé une possibilité adéquate et suffisante de contester les témoignages à charge et d'en interroger les auteurs. Toutefois, la Cour européenne des droits de l'homme admet que, pourvu que les droits de la défense soient respectés, il peut être légitime pour des autorités de police de souhaiter préserver l'anonymat d'un agent employé à des activités secrètes, afin non seulement d'assurer sa protection et celle de sa famille, mais aussi de ne pas compromettre la possibilité de l'utiliser dans des opérations futures[164].

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

[163] V. CC, décision n° 2022-987 QPC, M. Saïd Z. [Conditions de recours aux moyens des services de l'État soumis au secret de la défense nationale dans le cadre de certaines procédures pénales], 8 avril 2022, § 12.

[164] V. CEDH, Van Mechelen et autres c. Pays-Bas, 1997, §§ 56-57 ; Batek et autres c. République tchèque, 2017, § 46 ; Van Wesenbeeck c. Belgique, 2017, §§ 100-101.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les dispositions de l'article 656-1 du code de procédure pénale ne précisent pas les conditions d'application dans le temps du régime d'audition comme témoin des agents de renseignement, des membres des unités de forces spéciales ou des unités d'intervention spécialisées dans la lutte contre le terrorisme et plus précisément si ce cadre procédural est applicable au-delà de la fin de l'affectation dans le service désigné.

Le principe d'interprétation stricte de la loi pénale pourrait permettre de considérer que l'absence de référence aux ex-agents ou ex-membres, tant à l'article 656-1 du code de procédure pénale, qu'aux articles auxquels il renvoie dans son alinéa 1er, suffit à les écarter du bénéfice de ce régime dérogatoire applicable uniquement aux fonctions actuelles.

Or, la problématique de l'application dans le temps des dispositions de l'article 656-1 du code de procédure pénale émerge régulièrement dans le cadre des procédures judiciaires. La pratique actuelle repose sur une appréciation différenciée, en fonction des situations présentées, ce qui est source d'insécurité juridique pour l'ensemble des acteurs judiciaires, anciennes administrations d'emplois ou intéressés eux-mêmes.

La question de l'application du texte peut porter par exemple sur le cas d'un ancien agent des forces spéciales retourné à une affectation classique ou sur celui d'un militaire devenu agent d'un service de renseignement amené à déposer au sujet d'une mission antérieure à cette affectation.

Or, la perte de qualité d'agent de renseignement, de membre d'une unité des forces spéciales ou d'interventions spécialisées dans la lutte contre le terrorisme n'entame en rien la nécessité de protéger ces personnels - au même titre que les services spécialisés auxquels ils ont appartenu - *a fortiori* si le départ du service est très récent.

Outre les enjeux de sécurité juridique, il apparaît inadapté de priver les agents dès la cessation des fonctions d'un cadre d'audition spécialement prévu pour les protéger lorsqu'ils témoignent sur des faits dont ils auraient eu connaissance lors d'une mission intéressant la défense et la sécurité nationale.

Quel que soit leur lien organique avec ce service ou leur parcours professionnel, la mission peut se poursuivre, les enjeux opérationnels se maintenir et la sensibilité du contexte s'accroître.

L'identification de ces agents spécialisés dans un cadre judiciaire peut, de surcroît, faciliter, par recoupement, la découverte de l'identité de leurs anciens collègues, toujours en affectation.

2.2. OBJECTIFS POURSUIVIS

Il s'agit de prévoir une modification de l'article 656-1 du code de procédure pénale pour écarter toute incertitude juridique quant à l'application dans le temps de ce cadre juridique. Indépendamment de la répression pénale prévue aux articles 413-13 et 413-14 du code pénal, la protection dans le cadre judiciaire des personnels ayant appartenu à des unités spécialisées reste un enjeu fort y compris lorsque les agents ont quitté leurs fonctions.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

S'agissant d'une disposition législative précisant le cadre d'audition dérogatoire applicable à certains anciens agents spécialisés et prévu lors de l'enquête judiciaire, elle doit par principe trouver sa place au sein du code de procédure pénale.

Il aurait pu être envisagé d'insérer cette modification dans les différentes dispositions générales du code de procédure pénale traitant des auditions de témoins aussi bien dans le cadre de l'enquête menée par le ministère public (articles 62 et 78) qu'au cours de l'information judiciaire (article 102). Elle trouve néanmoins plus opportunément sa place au sein du titre IV *bis* qui organise le régime des dépositions applicable aux personnels de certains services ou unités spécialisées.

Sur le fond du dispositif, il pourrait être envisagé de :

- D'en limiter l'application dans le temps, après la cessation des fonctions ;
- De subordonner expressément son application au constat d'un danger pour la sécurité de la personne concernée ou de ses proches ou pour la bonne exécution des missions de l'ancien service ou unité d'appartenance de l'intéressé.

3.2. OPTION RETENUE

L'article 656-1 du code de procédure pénale est complété par un nouvel alinéa précisant le champ d'application du dispositif rendu explicitement applicable au témoignage des personnes ayant appartenu aux services et unités qu'il mentionne.

Cet ajout garantit une interprétation claire de ces dispositions et sécurise leur application aux agents qui ont quitté ces unités.

L'article 656-1 du code de procédure pénale ainsi modifié permettra aux personnes désignées de se voir appliquer ce régime spécial d'audition en qualité de témoin pour concourir à l'enquête pénale, sans créer de risque particulier pour leur sécurité, celle de leurs proches ou de leur ancien service.

Sur le fond, il ne paraît pas approprié de limiter dans le temps l'application du dispositif après la cessation des fonctions, ce qui serait insuffisamment protecteur pour la sécurité de la personne ou de ses proches, ni de subordonner la protection de l'anonymat au constat préalable du danger par l'autorité administrative sous le contrôle du juge pénal (à l'instar du dispositif de l'article 15-4 du code de procédure pénale). En effet, compte tenu de la nature particulière des missions, secrètes, confiées aux services de renseignement et unités concernés par la disposition, la révélation de l'identité des agents qui y ont concouru, même dans le cadre d'une procédure judiciaire, serait de nature à donner des indications sur leur fonctionnement et leur organisation susceptibles de fragiliser l'efficacité de leurs actions en cours ou à venir.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La nouvelle disposition ajoute un alinéa à l'article 656-1 du code de procédure pénale.

Elle ne remet pas en cause le respect des droits de la défense, garanti par la Constitution. L'article 656-1 assure en effet la possibilité pour la personne mise en cause de contester le témoignage ainsi recueilli, le cas échéant dans le cadre d'une confrontation avec le témoin dans les conditions prévues à l'article 706-61 du code de procédure pénale. Il garantit en outre qu'aucune condamnation ne puisse être prononcée sur le seul fondement des déclarations recueillies d'un témoin anonyme.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les modifications législatives ne nécessitent pas d'articulation avec le droit international et le droit de l'Union européenne.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet

4.4. IMPACTS SUR LES SERVICES JUDICIAIRES

Cette mesure concerne une catégorie très particulière et résiduelle de témoins. L'extension aux anciens agents des services ou unités spécialisés visés à l'alinéa 1er de l'article ne devrait pas avoir d'impact particulier sur les services judiciaires.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Aucune consultation obligatoire n'est identifiée et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal Officiel* de la République française. S'agissant d'un texte fixant les modalités de poursuites et les formes de la procédure, il est d'application immédiate aux procédures pénales en cours[165].

5.2.2. Application dans l'espace

Ces dispositions ont vocation à s'appliquer dans les collectivités d'Outre-mer régies par l'article 73 de la Constitution du fait du principe d'identité législative sans qu'il soit requis d'en faire mention expresse.

Dans les collectivités d'Outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie soumises au régime de spécialité législative, une mention expresse d'application est nécessaire afin de rendre ces dispositions applicables via la mise à jour de l'article 804 du code de procédure pénale modifié à cette fin par l'article 36 du projet de loi.

Par ailleurs, aucune adaptation de ces dispositions tenant aux caractéristiques des collectivités n'apparaît nécessaire.

Ces mesures sont donc applicables sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

La présente disposition n'appelle aucune mesure réglementaire d'application.

[165] Article 112-2 du code pénal.

CHAPITRE III – ECONOMIE DE DEFENSE

Article 23 : Moderniser et adapter le régime des réquisitions en temps de paix et en temps de guerre

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Ainsi que l'a récemment souligné une mission d'information parlementaire, « *le triple contexte de crise climatique et écologique, de raréfaction des ressources et de montée des antagonismes entre puissances – s'exprimant aussi par des menaces hybrides non couvertes par la dissuasion nucléaire –, sur fond de recul de la démocratie et du droit international, laisse peu de doute quant à l'intensité croissante des crises que nous connaîtrons dans les prochaines décennies et quant à leur intrication* »[166].

Face à ce constat, le rapport concluait à la nécessité, pour l'Etat, de s'inscrire dans une « *démarche de résilience* », présentée comme « *la volonté et la capacité de la nation dans toutes ses composantes à se prémunir des principaux risques et menaces auxquels elle est exposée, et, si une catastrophe ou une agression majeure surviennent, à résister à leurs conséquences et à recouvrer rapidement un équilibre qui conforte sa cohésion et ses valeurs fondamentales* ». Une telle posture, destinée à « *laisser aussi peu de place que possible à la surprise stratégique* », suppose dès lors « *que les pouvoirs publics prennent également en compte les situations où leurs capacités propres seraient dépassées* ».

Dans une telle hypothèse, au-delà de ses capacités d'intervention directes ou indirectes, par voie contractuelle, l'Etat peut user de son pouvoir de réquisition, manifestation type des prérogatives exorbitantes dont il bénéficie, à la confluence de la puissance et de l'utilité publiques. Il s'agit, en effet, pour l'autorité administrative, d'imposer unilatéralement, pour des motifs d'intérêt général, le transfert temporaire de l'usage d'un bien, l'accomplissement d'une activité ou l'exécution d'une prestation de service par une personne, lorsque ceux-ci ne peuvent être obtenus au moyen d'une négociation amiable. La réquisition ne peut néanmoins être prononcée qu'à titre subsidiaire, lorsque les moyens dont dispose l'autorité requérante pour répondre aux besoins en cause apparaissent inexistants, inadaptés, indisponibles ou insuffisants.

[166] Alexandre Freschi et Thomas Gassiloud, Mission d'information sur la résilience nationale, Assemblée nationale, 23 février 2022.

Or, il peut être rappelé que le droit des réquisitions ne repose pas sur une procédure unique, mais qu'il est fondé sur une juxtaposition de procédures distinctes, obéissant à des règles de mise en œuvre différentes.

Historiquement, la première réglementation intervenue en la matière remonte à la loi du 3 juillet 1877[167], avec la fixation d'un régime spécifique aux réquisitions militaires, dont l'objet est de « *suppléer à l'insuffisance des moyens ordinaires d'approvisionnement de l'armée* », entendus au sens large, incluant le logement, les biens et denrées nécessaires à leur subsistance ou encore les installations, les équipements et la main d'œuvre nécessaires à la poursuite des activités militaires.

Ce n'est qu'à travers la loi du 11 juillet 1938[168] qu'a été consacrée cette faculté pour l'autorité civile. Initialement conçues pour ne s'appliquer qu'à titre temporaire, à l'approche de la Seconde Guerre mondiale, les dispositions de cette dernière loi ont finalement été prorogées à plusieurs reprises après la fin du conflit[169], jusqu'à leur pérennisation, par les ordonnances n° 59-63 du 6 janvier 1959[170] et n° 59-147 du 7 janvier 1959[171], qui ont consacré la possibilité d'y recourir « *pour les besoins du pays, les services des entreprises et des personnes, ainsi que la propriété ou l'usage de tous les biens* ».

Aujourd'hui codifiées au livre II de la deuxième partie du code de la défense[172], les dispositions issues des lois du 3 juillet 1877 et du 11 juillet 1938 ainsi que des ordonnances des 6 et 7 janvier 1959 constituent ainsi le corpus juridique de droit commun des réquisitions mobilisables par l'Etat, en temps de paix comme en temps de guerre, respectivement qualifiées de « *réquisitions pour les besoins généraux de la Nation* », s'agissant des prérogatives conférées à l'autorité civile, et de « *réquisitions militaires* », pour celles dévolues à l'autorité militaire.

A cet égard, il peut être souligné que si l'article L. 2211-1 du code de la défense énonce que les réquisitions pour les besoins généraux de la Nation ont été conçues afin de mettre en œuvre « *les prestations nécessaires pour assurer les besoins de la défense* » dans les cas mentionnés à l'article L. 1111-2 du même code – renvoyant ainsi à la mobilisation générale, à la mise en garde ou à une « *menace portant notamment sur une partie du territoire, sur un secteur de la vie nationale ou sur une fraction de la population* » –, l'article L. 2211-2 de ce code précise qu' « *Indépendamment des cas prévus à l'article L. 1111-2, le Gouvernement continue de disposer*

[167] Loi du 3 juillet 1877 relative aux réquisitions militaires.

[168] Loi du 11 juillet 1938 sur l'organisation générale de la nation pour le temps de guerre.

[169] Par des prolongations annuelles entre 1946 et 1949, *via* les lois du 10 mai 1946, n° 47-344 du 28 février 1947, n° 48-341 du 28 février 1948 et n° 49-266 du 26 février 1949, puis sans limitation de durée, par la loi n° 50-244 du 28 février 1950 maintenant provisoirement en vigueur au-delà du 1er mars 1950 certaines dispositions législatives et réglementaires du temps de guerre prorogées par la loi du 26 février 1949.

[170] Ordonnance n° 59-63 du 6 janvier 1959 relative aux réquisitions de biens et de services.

[171] Ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense.

[172] A l'occasion de l'ordonnance n° 2004-1374 du 20 décembre 2004 relative à la partie législative du code de la défense.

des pouvoirs qui lui sont conférés » en la matière[173], lui offrant ainsi la possibilité de « *réquisitions à connotation plus civiles* »[174].

Le régime actuel de réquisitions pour les besoins généraux de la Nation comprend ainsi deux volets :

- d'une part, l'article L. 2211-1, relatif aux réquisitions « *pour assurer les besoins de la défense* » (et seulement eux), qui est applicable dans les hypothèses de l'article L. 1111-2 et en cas de déclaration de l'état d'urgence[175] ;

- d'autre part, l'article L. 2211-2, relatif à ce que l'on appelait jusqu'à la codification les réquisitions pour les « *besoins du pays* » (et non seulement de la défense), possible dans tous les cas, au-delà des seules hypothèses de l'article L. 1111-2 (donc y compris en dehors d'une « *menace* » au sens de cet article). Comme l'a indiqué le Conseil d'Etat dans un avis de 1945, « *ni la loi du 11 juillet 1938, ni aucune disposition législative ultérieure n'ont donné une définition de cette dernière expression dont le sens doit dès lors être déterminé d'après l'objet général poursuivi par la loi* ». Toutefois, les besoins du pays (ou de la Nation) peuvent être rapportés aux « *activités essentielles à la vie du pays* », dont le maintien serait « *indispensable pour faire face aux exigences de la défense nationale, en raison soit des prestations qu'elles sont appelées à fournir, soit du trouble grave que leur disparition apporterait à l'ordre public* »[176]. C'est sur ce fondement que des réquisitions de grévistes ont été effectuées de 1948 à 1963. Le Conseil d'Etat a néanmoins exigé qu'il soit démontré, à propos d'une grève d'une régie de transports, que « *les perturbations qui en sont résultées, sur ce trafic aient eu pour effet de porter soit à la continuité du service des transports, soit à la satisfaction des besoins de la population une atteinte suffisamment grave pour justifier légalement la réquisition du personnel de cette régie* »[177].

Ce régime est ainsi à la fois imprécis et très englobant : il vise à remédier à toutes les atteintes aux besoins généraux de la Nation, sans énumérer les différentes hypothèses dans lesquelles celles-ci pourraient subvenir. En principe, les réquisitions pour les besoins de la Nation, comme leur nom l'indique, constituent les réquisitions de droit commun au service des intérêts de la Nation toute entière (ou une partie d'entre elle), par opposition aux réquisitions de police du 4° de l'article L. 2215-1 du code général des collectivités territoriales, nécessairement localisées à

[173] Les dispositions de l'article L. 2211-2 du code de la défense ont ainsi codifié celles de l'article 45 de l'ordonnance n° 59-147 du 7 janvier 1959 susmentionnée, dont l'objet était de préserver la faculté conférée au Gouvernement, par l'article 2 de la loi n° 50-244 du 28 février 1950 susmentionnée, de recourir largement au mécanisme de réquisition issu de la loi du 11 juillet 1938.

[174] Jacques-Henri Stahl, « Juridiction compétente pour indemniser un médecin réquisitionné par un préfet », AJDA, 2006.

[175] Article 10 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence : « *La déclaration de l'état d'urgence s'ajoute aux cas prévus à l'article L. 1111-2 du code de la défense pour la mise à exécution des réquisitions dans les conditions prévues au livre II de la deuxième partie du même code* ».

[176] CE, avis, 31 mai 1945, Revue de droit public, 1947, pp. 22-23.

[177] CE, 24 fév. 1961, Isnardon, n° 40013, A.

l'échelle du département et strictement dédiée à la prévention d'une menace à l'ordre public (ce que les besoins généraux de la Nation englobent sans s'y résumer).

Néanmoins, ainsi qu'il ressort de l'usage de ce régime sous la V^e^ République, les pouvoirs publics n'y ont recours qu'avec une extrême parcimonie, lorsque des intérêts publics sont manifestement menacés. On ne dénombre ainsi que cinq décrets en conseil des ministres portant ouverture du droit de réquisition dans de telles circonstances :

- le décret n° 61-404 du 24 avril 1961 portant ouverture du droit de réquisition, pris sur le fondement du décret n° 61-395 du 22 avril 1961 portant déclaration de l'état d'urgence et du décret n° 61-396 du 22 avril 1961 relatif à l'application de l'état d'urgence dans tous les départements du territoire métropolitain, consécutivement au « putsch des généraux » du 21 avril de cette même année ;
- le décret n° 91-42 du 14 janvier 1991 portant ouverture du droit de réquisition des compagnies aériennes françaises, à titre préventif, pour permettre d'évacuer les ressortissants français en cas de conflit dans le Golfe ;
- le décret n° 91-60 du 17 janvier 1991 portant ouverture du droit de réquisition de l'emploi des personnels des compagnies d'armement maritime françaises, à titre préventif, pour permettre d'évacuer les ressortissants français en cas de conflit dans le Golfe ;
- le décret n° 2004-1190 du 10 novembre 2004 portant ouverture du droit de réquisition des compagnies aériennes françaises, afin de permettre l'évacuation des ressortissants français présents en Côte d'Ivoire après le bombardement d'un camp de la force Licorne à Bouaké par un avion de l'armée ivoirienne, le 6 novembre de cette même année ;
- le décret n° 2022-1020 du 20 juillet 2022 portant ouverture du droit de réquisition des sociétés de location d'hélicoptères en capacité de participer à la lutte contre les feux de forêts, afin de répondre à « *de multiples incendies d'une rare intensité sur l'ensemble du territoire national* ».

Parallèlement à la construction de ce droit commun des réquisitions, se sont également développés plusieurs régimes spéciaux de réquisition civile, au nombre desquels figurent, pour ne citer que les domaines d'intervention les plus significatifs :

- en matière de **logement**, l'ordonnance n° 45-2394 du 11 octobre 1945[178], prise en vue de remédier aux difficultés de logement causées par les destructions de la Seconde Guerre mondiale avant d'être pérennisées et codifiées[179] du fait de la persistance de la crise du logement, confère au préfet la faculté de « *procéder, par voie de réquisition, pour une durée maximum d'un an, renouvelable, à la prise de possession partielle ou totale des locaux à usage d'habitation vacants, inoccupés ou insuffisamment occupés* » pour les attribuer à des « *personnes dépourvues de logement ou logées dans des conditions manifestement*

[178] Ordonnance n° 45-2394 du 11 octobre 1945 instituant des mesures exceptionnelles et temporaires en vue de remédier à la crise du logement.

[179] Cf. articles L. 641-1 à L. 641-14 du code de la construction et de l'habitation.

insuffisantes » ou « *à l'encontre desquelles une décision judiciaire définitive ordonnant leur expulsion est intervenue* », en contrepartie d'une « *indemnité d'occupation* » ;

- en matière de **protection des eaux marines**, les lois n° 61-1262 du 24 novembre 1961[180] et n° 76-599 du 7 juillet 1976[181], respectivement codifiées aux articles L. 5141-2-1 et L. 5242-17 du code des transports et L. 218-72 du code de l'environnement, confèrent à l'autorité administrative compétente de l'Etat la faculté de procéder à la réquisition des personnes et des biens en vue de mettre fin à un danger ou à une entrave prolongée à l'exercice des activités maritimes, littorales ou portuaires induit par la présence d'un engin flottant ou résultant d'une avarie ou d'un accident, renvoyant au régime d'indemnisation prévu par le code de la défense ;

- en matière de **propriété intellectuelle**, les dispositions de la loi n° 68-1 du 2 janvier 1968[182], aujourd'hui codifiées aux articles L. 612-8 à L. 612-10 du code de la propriété intellectuelle, confèrent au ministre de la défense un pouvoir de réquisition lui permettant, pour une durée d'un an renouvelable, d'interdire la divulgation et la libre exploitation d'inventions faisant l'objet de demandes de brevet, dès lors qu'elles intéressent la défense nationale, ouvrant ainsi « *droit à une indemnité au profit du titulaire de la demande de brevet, dans la mesure du préjudice subi* » ;

- en matière de **sauvegarde de l'ordre public**, les dispositions de la loi n° 87-565 du 22 juillet 1987[183], aujourd'hui codifiées au sein du code de la sécurité intérieure[184], ont conféré aux autorités territorialement compétentes de l'Etat, « *en cas d'accident, sinistre ou catastrophe* », la faculté de réquisitionner « *les moyens privés nécessaires aux secours* », avant que l'article 3 de la loi n° 2003-239 du 18 mars 2003[185] ne consacre plus largement le pouvoir de réquisition dont bénéficient les préfets, obéissant à un régime d'indemnisation spécifique. Ces dernières dispositions ont, en effet, inséré un nouveau 4° au sein de l'article L. 2215-1 du code général des collectivités, qui prévoit qu' « *en cas d'urgence, lorsque l'atteinte constatée ou prévisible au bon ordre, à la salubrité, à la tranquillité et à la sécurité publiques l'exige et que les moyens dont dispose le préfet ne permettent plus de poursuivre les objectifs pour lesquels il détient des pouvoirs de police, celui-ci peut, par arrêté motivé, pour toutes les communes du département ou plusieurs ou une seule d'entre elles, réquisitionner tout bien ou service, requérir toute personne nécessaire au fonctionnement de ce service ou à l'usage de ce bien* » ;

- en matière **sanitaire**, l'article 20 de la loi n° 2004-806 du 9 août 2004[186] a introduit, au sein du code de la santé publique, les articles L. 3131-8 et L. 3131-9 permettant aux autorités

[180] Loi n° 61-1262 du 24 novembre 1961 relative à la police des épaves maritimes.

[181] Loi n° 76-599 du 7 juillet 1976 relative à la prévention et à la répression de la pollution marine par les opérations d'immersion effectuées par les navires et aéronefs, et à la lutte contre la pollution marine accidentelle.

[182] Loi du n° 68-1 du 2 janvier 1968 sur les brevets d'invention.

[183] Loi n° 87-565 du 22 juillet 1987 relative à l'organisation de la sécurité civile, à la protection de la forêt contre l'incendie et à la prévention des risques majeurs.

[184] Cf. articles L. 115-1, L. 742-2, L. 742-3 et L. 742-12 à L. 742-15 de ce code.

[185] Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

[186] Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique.

territorialement compétentes de l'Etat, « *Si l'afflux de patients ou de victimes ou la situation sanitaire le justifie* », de « *procéder aux réquisitions nécessaires de tous biens et services, et notamment requérir le service de tout professionnel de santé, quel que soit son mode d'exercice, et de tout établissement de santé ou établissement médico-social* », renvoyant au régime d'indemnisation prévu par le code de la défense ;

– en matière **spatiale**, l'ordonnance n° 2022-232 du 23 février 2022[187] a introduit, au sein du livre II de la deuxième partie du code de la défense, un nouveau titre II *bis* établissant un cadre spécifique relatif aux réquisitions de biens et services spatiaux, permettant au Premier ministre d'obtenir en cas d'urgence, au profit de l'Etat, le transfert de maîtrise d'un objet spatial ou la fourniture de prestations de services fondées sur l'utilisation d'un tel objet, afin de répondre à des besoins liés à la sauvegarde des intérêts de la défense nationale, moyennant un mécanisme d'indemnisation intégrale des préjudices occasionnés à cette occasion.

Enfin, des lois de circonstance ont parfois été adoptées pour permettre l'usage du droit de réquisition à l'occasion d'événements exceptionnels, à l'image :

– des lois n° 67-532 du 4 juillet 1967[188], n° 87-1132 du 31 décembre 1987[189] et n° 2018-202 du 26 mars 2018[190], autorisant la réquisition temporaire de terrains et de bâtiments dans la perspective de l'organisation des **jeux Olympiques** sur le territoire national ;

– de la loi n° 2020-290 du 23 mars 2020[191], qui a ouvert aux préfets la faculté d' « *ordonner la réquisition de toute personne et de tous biens et services nécessaires à la lutte contre la catastrophe sanitaire* » pendant la durée de l'**état d'urgence sanitaire**, renvoyant une fois de plus au régime d'indemnisation prévu par le code de la défense ;

– de la loi n° 2022-1158 du 16 août 2022[192], qui a ouvert au ministre de l'énergie, pour une durée de quatre ans, la faculté de réquisitionner les services chargés de l'exploitation d'installations de **production d'électricité utilisant du gaz naturel**, dans le contexte de menace sur la sécurité des approvisionnement consécutif au conflit ukrainien.

Ainsi qu'il ressort des développements qui précèdent, le droit des réquisitions est le fruit d'un empilement de textes épars, obéissant à des objectifs et à des procédures qui n'apparaissent ni homogènes ni coordonnés et dont la rédaction semble parfois désuète, sujette à interprétation ou, plus largement, inadaptée aux besoins de l'époque.

---

[187] Ordonnance n° 2022-232 du 23 février 2022 relative à la protection des intérêts de la défense nationale dans la conduite des opérations spatiales et l'exploitation des données d'origine spatiale.

[188] Loi n° 67-532 du 4 juillet 1967 autorisant la réquisition temporaire de terrains nécessaires aux aménagements et installations provisoires destinées au déroulement des X^es^ jeux Olympiques d'hiver de Grenoble.

[189] Loi n° 87-1132 du 31 décembre 1987 autorisant, en ce qui concerne la prise de possession des immeubles nécessaires à l'organisation ou au déroulement des XVI^es^ jeux Olympiques d'hiver d'Albertville et de la Savoie, l'application de la procédure d'extrême urgence et la réquisition temporaire.

[190] Loi n° 2018-202 du 26 mars 2018 relative à l'organisation des jeux Olympiques et Paralympiques de 2024.

[191] Loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19.

[192] Loi n° 2022-1158 du 16 août 2022 portant mesures d'urgence pour la protection du pouvoir d'achat.

Or, l'objectif stratégique n°3 de la Revue nationale stratégique 2022 souligne la nécessité de disposer d'outils permettant, en période de crise, de pallier l'insuffisance des moyens dont dispose l'Etat pour répondre pleinement aux exigences de la politique de défense, dont l'objet est « *d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées* », de contribuer « *à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale* », de pourvoir « *au respect des alliances, des traités et des accords internationaux* » et de participer « *dans le cadre des traités européens en vigueur, à la politique européenne de sécurité et de défense commune* »[193].

1.2. CADRE CONSTITUTIONNEL

Le principe même des réquisitions et les modalités générales qui les régissent, qui doivent être définies dans la loi en application de l'article 34 de la Constitution, en ce que sont en cause les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques et en ce qu'elles constituent, de par leur objet même, des sujétions imposées par la défense nationale aux citoyens en leur personne et en leurs biens, est soumis au contrôle du juge constitutionnel.

A l'occasion de son contrôle, le Conseil constitutionnel s'assure que les dispositions législatives procèdent à une « *conciliation qui ne soit pas déséquilibrée* » entre les différentes exigences constitutionnelles en cause.

Par ailleurs, sur les décisions de réquisition, le juge exerce un contrôle concret et entier visant à s'assurer que celles-ci soient nécessaires, adaptées et proportionnées aux objectifs poursuivis[194].

1.2.1. La sauvegarde des intérêts fondamentaux de la Nation est une exigence constitutionnelle susceptible de justifier une atteinte à d'autres principes à valeur constitutionnelle

Il ressort de la jurisprudence du Conseil constitutionnel et du Conseil d'Etat que les « *exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* », au premier rang desquelles figurent l'indépendance nationale et l'intégrité du territoire, qui en sont la finalité, mais également la protection du secret de la défense nationale et la libre disposition de la force armée[195], sont prises en compte par le juge dans son contrôle de proportionnalité en cas d'atteinte à d'autres principes à valeur constitutionnelle.

---

[193] Cf. article L. 1111-1 du code de la défense.

[194] CE, 4 décembre 2017, Commune de Sainte-Croix-en-Plaine, 405598.

[195] Le principe de « *nécessaire libre disposition de la force armée* » découle des articles 20 et 21 de la Constitution, en application desquels « *le Gouvernement décide, sous l'autorité du Président de la République, de l'emploi de la force armée* » (M. Dominique de L., 28 novembre 2014, n° 2014-432 QPC).

Il revient au juge d'assurer une « *conciliation qui ne soit pas déséquilibrée* » entre la sauvegarde des intérêts fondamentaux de la Nation et les autres exigences constitutionnelles[196].

1.2.2. Les atteintes au droit de propriété doivent être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi

Il ressort de la jurisprudence du Conseil constitutionnel que : « *La propriété figure au nombre des droits de l'homme consacrés par les articles 2 et 17 de la Déclaration de 1789. Selon son article 17 : « La propriété étant un droit inviolable et sacré, nul ne peut en être privé, si ce n'est lorsque la nécessité publique, légalement constatée, l'exige évidemment, et sous la condition d'une juste et préalable indemnité ». En l'absence de privation du droit de propriété au sens de cet article, il résulte néanmoins de l'article 2 de la Déclaration de 1789 que les atteintes portées à ce droit doivent être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi* »[197].

Si la réquisition constitue une atteinte au droit de propriété, elle ne constitue aucunement une privation de ce droit au sens de l'article 17 de la Déclaration de 1789. Bien que répondant à un objectif de valeur constitutionnelle, une telle atteinte ne saurait cependant revêtir un caractère de gravité tel qu'elle dénature le sens et la portée du droit de propriété[198].

En l'absence de dépossession, aucun principe à valeur constitutionnelle n'impose que l'indemnisation des atteintes au droit de propriété relève de la compétence du juge judiciaire[199].

1.2.3. Le respect du principe d'égalité devant les charges publiques impose une réparation intégrale des préjudices

Il ressort de la jurisprudence du Conseil constitutionnel que : « *le respect du principe d'égalité devant les charges publiques ne saurait permettre d'exclure du droit à réparation un élément quelconque du préjudice indemnisable résultant de la mise en œuvre de la procédure de réquisition ; qu'il suit de là qu'au cas où l'indemnité prévue à l'article L. 642-15 ne suffirait pas à couvrir l'intégralité du préjudice subi par le titulaire du droit d'usage, l'article L. 642-16 doit*

---

[196] Mme Ekaterina B., épouse D., et autres, 10 novembre 2011, n° 2011-192 QPC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif et du droit à un procès équitable ; Loi relative au renseignement, 23 juillet 2015, n° 2015-713 DC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif, du droit à un procès équitable et du principe du contradictoire ; Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias, 10 novembre 2016, n° 2016-738 DC, à propos de la liberté d'expression et de communication ; La Quadrature du net, 9 juillet 2021, n° 2021-924 QPC, à propos du respect de la vie privée.

[197] M. Jean-Claude G., 17 janvier 2012, n°2011-209 QPC ; M. Raïme A., 2 décembre 2016, n° 2016-600 QPC.

[198] Loi d'orientation relative à la lutte contre les exclusions, 29 juillet 1998, n° 98-403 DC.

[199] Loi modifiant la loi n° 82-652 du 29 juillet 1982 et portant diverses dispositions relatives à la communication audiovisuelle, 13 décembre 1985, n° 85-198 DC.

être interprété comme permettant au juge judiciaire de lui allouer une indemnité complémentaire »[200].

1.2.4. Des restrictions peuvent être apportées à la liberté d'entreprendre dès lors qu'il n'en résulte pas d'atteinte disproportionnée au regard de l'objectif poursuivi

Même si le Conseil constitutionnel rappelle que « *la liberté qui, aux termes de l'article 4 de la Déclaration* [des droits de l'Homme et du citoyen du 26 août 1789]*, consiste à pouvoir faire tout ce qui ne nuit pas à autrui, ne saurait elle-même être préservée si des restrictions arbitraires ou abusives étaient apportées à la liberté d'entreprendre* »[201], il considère que cette dernière « *n'est toutefois ni générale ni absolue* »[202] et « *qu'il est loisible au législateur d'apporter à cette liberté des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi* »[203].

1.2.5. Des restrictions peuvent être apportées à la liberté contractuelle dès lors qu'il n'en résulte pas d'atteinte disproportionnée au regard de l'objectif poursuivi

Le Conseil constitutionnel considère, selon une jurisprudence constante, qu'il « *est loisible au législateur d'apporter à la liberté contractuelle, qui découle de l'article 4 de la Déclaration de 1789, des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi. Par ailleurs, le législateur ne saurait porter aux contrats légalement conclus une atteinte qui ne soit justifiée par un motif d'intérêt général suffisant sans méconnaître les exigences résultant des articles 4 et 16 de la Déclaration de 1789* »[204].

1.2.6. Le juge veille à assurer une conciliation entre l'exercice du droit de grève et l'exigence constitutionnelle tenant à la continuité du service public

Selon le septième alinéa du Préambule de la Constitution de 1946 : « *Le droit de grève s'exerce dans le cadre des lois qui le réglementent* ». Le Conseil constitutionnel en déduit que : « *En édictant cette disposition, les constituants ont entendu marquer que le droit de grève est un principe de valeur constitutionnelle mais qu'il a des limites et ont habilité le législateur à tracer*

---

[200] Loi modifiant la loi n° 82-652 du 29 juillet 1982 et portant diverses dispositions relatives à la communication audiovisuelle, 13 décembre 1985, n° 85-198 DC.

[201] Loi de nationalisation, 16 janvier 1982, n° 81-132 DC.

[202] Loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques, 20 janvier 1993, n° 92-316 DC.

[203] Société Chaud Colatine, 21 janvier 2011, n° 2010-89 QPC.

[204] Loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, 8 décembre 2016, n° 2016-741 DC.

celles-ci en opérant la conciliation nécessaire entre la défense des intérêts professionnels, dont la grève est un moyen, et la sauvegarde de l'intérêt général auquel la grève peut être de nature à porter atteinte. En ce qui concerne les services publics, la reconnaissance du droit de grève ne saurait avoir pour effet de faire obstacle au pouvoir du législateur d'apporter à ce droit les limitations nécessaires en vue d'assurer la continuité du service public qui, tout comme le droit de grève, a le caractère d'un principe de valeur constitutionnelle »[205].

L'exercice du droit de réquisition peut contribuer à assurer le principe de continuité de service public[206].

1.3. CADRE CONVENTIONNEL

Si la jurisprudence de la Cour européenne des droits de l'homme (CEDH) et celle de la Cour de justice de l'Union européenne (CJUE) confirme les grands principes de la jurisprudence détaillée au sein de l'item 1.2 *supra*, le régime des réquisitions est susceptible ou non d'impacter certains autres principes conventionnels.

1.3.1. Une réquisition de services ou de personnes ne saurait être assimilée à du travail forcé ou obligatoire

Si l'article 4 de la Convention européenne de sauvegarde des droits et de l'Homme et des libertés fondamentales et l'article 8 du Pacte international relatif aux droits civils et politiques interdisent le travail forcé ou obligatoire, ces conventions prévoient que n'est pas considéré comme du travail forcé ou obligatoire : *« tout service requis dans le cas de crises ou de calamités qui menacent la vie ou le bien-être de la communauté* » (article 4.3.c de la Convention européenne de sauvegarde des droits et de l'Homme et des libertés fondamentales) ou : « *Tout service exigé dans les cas de force majeure ou de sinistres qui menacent la vie ou le bien-être de la communauté* » (article 8.3.c.iii du Pacte international relatif aux droits civils et politiques).

1.3.2. Les réquisitions ne sont pas soumises au respect des principes de la commande publique

Le recours à la réquisition, en ce qu'il fait intervenir des opérateurs économiques pour répondre à un besoin de l'Etat sur la base d'un « *prix commercial normal* », présente certains points communs avec la commande publique.

[205] Loi de transformation de la fonction publique, 1er août 2019, n° 2019-790 DC.

[206] Loi relative aux aéroports, 14 avril 2005, n° 2005-513 DC.

Toutefois, la réquisition n'est pas un contrat dès lors qu'il manque le consentement du prestataire. En l'absence de cet élément lié à la volonté de l'opérateur économique, la réquisition n'entre pas dans le cadre des directives sur les marchés publics[207].

1.3.3. Les règles relatives au bon fonctionnement du marché intérieur de l'UE ne font pas obstacle à l'exercice du droit de réquisition

De telles mesures seraient, en effet, susceptibles de porter atteinte à l'interdiction des restrictions quantitatives à l'importation ou à l'exportation entre les Etats membres, respectivement prévues aux articles 34 et 35 du Traité sur le fonctionnement de l'Union européenne (TFUE). Toutefois, l'article 36 autorise notamment les Etats membres à adopter des dispositions législatives, réglementaires et administratives instituant de telles restrictions lorsqu'elles sont justifiées par des raisons d'ordre public, de sécurité publique et de santé publique.

1.4. ÉLEMENTS DE DROIT COMPARE

Tous les Etats se trouvent confrontés à la difficulté de concilier les droits des personnes privés avec la nécessité, face à certaines situations critiques, de mettre en œuvre des mesures de contrainte pour obtenir, de leur part, la fourniture d'un bien ou l'exécution d'une prestation de service, lorsqu'elles ne peuvent être obtenues ni par l'action directe des pouvoirs publics ni par voie contractuelle. Parmi les dispositifs les plus anciens, l'on peut notamment citer les régimes institués aux Etats-Unis et au Royaume-Uni, qui confèrent aux pouvoirs publics un large périmètre d'intervention, tout en assurant une stricte garantie des droits fondamentaux des personnes concernées.

En premier lieu, le V[e] amendement de la Constitution des Etats-Unis, promulgué le 15 décembre 1791, énonce que « *nulle propriété privée ne pourra être réquisitionnée dans l'intérêt public sans une juste indemnité* ».

Si ces dispositions ont, dans un premier temps, été considérées comme ne s'appliquant qu'à la réquisition de biens immobiliers, la jurisprudence de la Cour suprême en a progressivement étendu le périmètre d'application afin de garantir le droit à indemnisation des propriétaires[208]. Elles couvrent aujourd'hui tous types de biens, tangibles comme intangibles, y compris les servitudes, les droits contractuels ou encore les secrets commerciaux, ainsi que les services des entreprises. En outre, la jurisprudence retient une acception particulièrement large de « *l'intérêt public* », même si son interprétation diffère selon les juridictions, certaines considérant que le

[207] Notamment la directive n° 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE qui définit, en son article 2, les marchés publics comme étant « d*es contrats à titre onéreux conclus par écrit entre un ou plusieurs opérateurs économiques et un ou plusieurs pouvoirs adjudicateurs et ayant pour objet l'exécution de travaux, la fourniture de produits ou la prestation de services* ».

[208] *Pumpelly v. Green Bay & Mississippi Canal Co.* (1871).

V^e amendement a vocation à s'appliquer dès que la réquisition procure un bénéfice à la collectivité, y compris lorsque l'Etat y a recours pour faciliter un intérêt privé[209].

Même si, la plupart du temps, la mise en œuvre de ces réquisitions se concrétise par une expropriation, par exemple pour construire une route, une base militaire ou un parc, elle peut également se traduire par une simple limitation temporaire du droit de propriété, étant précisé que, le cas échéant, les débats juridictionnels se concentrent sur la durée au-delà de laquelle est ouvert le droit à indemnisation et sur le montant de cette dernière. Tel fut, par exemple, le cas pendant la Seconde Guerre mondiale, au cours de laquelle ont été pratiquées des saisies d'entrepôts et d'usines[210], ou encore à l'occasion de la réquisition d'une mine de charbon pour une durée d'un mois et demi[211]. Dans tous les cas, le propriétaire n'est indemnisé que pendant la durée au cours de laquelle il était complétement privé de son bien.

La réquisition doit donner lieu à une « *juste compensation* » de l'utilisation du bien en cause par l'Etat[212]. En pratique, la Cour suprême précise qu'elle est due même si elle n'affecte que faiblement l'intérêt économique du propriétaire et qu'elle doit être établie par rapport aux prix du marché[213]. En revanche, aucune indemnisation n'est exigée de la part de l'Etat lorsque la réquisition est pratiquée en vue d'une destruction dudit bien en cas de péril imminent, par exemple à l'occasion d'opérations de retraite réalisées par les armées face à l'ennemi[214] ou encore pour empêcher la propagation d'une maladie ou de toute autre menace pour la santé ou la sécurité publiques[215].

En second lieu, au Royaume-Uni, l'*Emergency Powers Act* autorise depuis 1920 le gouvernement, lorsqu'il proclame « *l'état d'urgence* », à prendre les mesures nécessaires pour garantir les « *besoins essentiels de la communauté* », lorsque l'approvisionnement et la distribution de nourriture, d'eau, de combustible et d'électricité ou les moyens de transport sont menacés. Ce texte, modifié en 1964, a été abrogé par le *Civil Contingences Act* de 2004, qui fixe le régime actuellement applicable en matière de préparation et de réponse aux situations d'urgence, au cours desquelles il autorise notamment l'édiction d'une législation spéciale temporaire, dite « *règlements d'urgence* », sans examen parlementaire préalable. L'urgence y est ainsi définie comme renvoyant aux événements et aux situations qui menacent de porter gravement atteinte au bien-être humain, à l'environnement ou à la sécurité du Royaume-Uni ainsi qu'à la guerre et au terrorisme.

L'article 21 de la loi de 2004 précise les conditions de recours à ces dispositifs exceptionnels : d'une part, le fait qu'une urgence s'est produite, se produit ou est sur le point de se produire et, d'autre part, le fait qu'il est nécessaire de prendre des dispositions afin de prévenir, contrôler

[209] *Kelo v. City of New London* (2005).

[210] *Kimball Laundry Co. v. United States* (1949) ; *United States v. Petty Motor Co.* (1946) ; *United States v. General Motors Corp.* (1945).

[211] *United States v. Peewee Coal Co.* (1951).

[212] *Kohl v. United States* (1875).

[213] *Loretto v. Teleprompter Manhattan CATV Corp.* (1982).

[214] *United States v. Pacific R. Co.* (1887) et *United States v. Caltex Inc.* (1952).

[215] *First English Evangelical Lutheran Church v. County of Los Angeles* (1987).

ou atténuer un aspect ou un effet de cette urgence, tandis que l'article 20 énonce que de telles mesures peuvent être prises par un décret du Roi ou, si l'urgence l'impose, par un acte du Premier ministre, d'un secrétaire d'Etat ou d'un commissaire du Trésor de Sa Majesté. Il apparaît, en outre, que « *Les règlements d'urgence ne peuvent être utilisés que dans des conditions spécifiques et ils deviennent caducs après sept jours, à moins que les deux chambres du Parlement n'adoptent une résolution les approuvant. Si l'approbation parlementaire est accordée, les règlements d'urgence deviennent automatiquement caducs au plus tard 30 jours après leur adoption. D'autres règlements peuvent être adoptés pour une nouvelle période de 30 jours, mais doivent être approuvés par chaque chambre dans un délai de 7 jours, avec une disposition de rappel obligatoire si l'une des deux chambres est en vacances. Ils peuvent être amendés ou rejetés à tout moment et constituent donc tout au plus une solution législative temporaire* »[216].

Lorsque les règlements d'urgence sont mis en œuvre, le §1 de l'article 22 de la loi de 2004 précise qu'ils « *peuvent prévoir toute disposition dont la personne qui les établit est convaincue qu'elle est appropriée pour prévenir, contrôler ou atténuer un aspect ou un effet de la situation d'urgence à l'égard de laquelle les règlements sont établis* », tandis que le §3 ajoute qu'ils « *peuvent prendre des dispositions de toute nature qui pourraient être prises par une loi du Parlement ou par l'exercice de la prérogative royale ; en particulier, les règlements peuvent :* [...] *b) prévoir ou permettre la réquisition ou la confiscation de biens (avec ou sans compensation)* ».

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Ainsi que le rappelle le rapport de la mission d'information parlementaire cité en préambule de l'item 1.1, « *les risques susceptibles d'éprouver la résilience d'une nation sont plus diversifiés que ceux auxquels s'exposent un écosystème ou un individu. Du fait de la complexité des sociétés contemporaines, due à la diversité et à l'intensité des activités et des échanges au sein de chacune d'entre elles autant qu'aux rapports d'interdépendance qui les lient les unes aux autres, les sources de vulnérabilité sont nombreuses et se recoupent en partie : les risques géopolitiques, pouvant revêtir la forme de conflits de haute intensité entre États, se superposent à des fragilités économiques, que celles-ci soient l'effet d'une conjoncture particulière ou de la longue durée ; l'impact de phénomènes tels que le dérèglement climatique comme de risques environnementaux plus circonscrits dans l'espace et dans le temps, s'analyse aussi bien en termes écologiques que politiques, sociaux ou économiques ; la fragmentation du corps politique, la défiance dont font l'objet les institutions et la difficulté à définir un ensemble de*

[216] *Civil Contingencies Act Post-Implementation Review*, 2022.

principes constituant une vision du monde capable de réunir les membres d'une nation par-delà leurs différences, sont autant de vulnérabilités propres aux sociétés démocratiques »[217].

Les parlementaires auteurs de ce rapport en concluent que ce panorama des évènements d'ampleur susceptibles d'affecter la vie de la Nation « *doit nous amener à nous demander en permanence quel est le bon niveau d'assurance pour le pays, afin de déterminer ensuite quel est le bon niveau de réponse, en fonction du niveau de couverture souhaité – étant entendu que la garantie collective ultime reste celle que nous offrent nos armées, dont la remontée en puissance doit être résolument poursuivie* ». Au-delà d'un devoir d'anticipation des risques et de prévention de leur réalisation, ces constats impliquent pour l'Etat de s'assurer que les moyens dont ils disposent lui permettront d'intervenir efficacement le moment venu.

Or, il apparaît que, depuis la fin de la guerre froide, notre modèle d'armée s'est progressivement décentré de sa mission originelle de défense du territoire. En effet, structuré autour de la dissuasion nucléaire et sur le recours à des forces expéditionnaires, il doit désormais être adapté pour faire face à la dégradation du contexte stratégique sur tout le spectre de la conflictualité contemporaine. Depuis trois décennies, la France maintient un niveau d'engagement extérieur substantiel, avec en moyenne 8 000 militaires projetés en permanence[218]. L'ampleur de cet engagement a nécessairement une incidence sur les capacités susceptibles d'être mobilisées par les armées en faveur de la défense du territoire, étant précisé que ces interventions extérieures provoquent une usure accélérée des équipements militaires, dans un contexte marqué par les difficultés d'approvisionnement et de régénération des stocks. Ainsi que le souligne d'ailleurs un représentant du ministère des armées dans le rapport susmentionné, « *dans une logique d'optimisation et pour respecter les contrats opérationnels qui figurent dans le Livre blanc, le fonctionnement des armées s'appuie sur une logique de flux.* […] *En l'absence de référence à un contrat, le ministère est moins résilient qu'à l'époque de la guerre froide où il disposait de stocks importants – masques, tenues NRBC* ».

Dans un tel contexte, il est nécessaire pour les pouvoirs publics de développer leur capacité à répondre aux crises et à toute autre situation critique susceptible d'affecter le territoire national. Or, à cet égard, le rapport susmentionné précise que « *la résilience de la nation sera d'autant plus forte que le citoyen sera considéré comme un élément de la réponse.* […] *De même, au niveau des entreprises et de l'administration des collectivités et de l'Etat, la résilience doit devenir une exigence au même titre que l'efficacité et l'efficience, avec toutes les procédures préventives que cela implique* ». Le recours potentiel à la réquisition de moyens privés pour compléter ceux dont dispose l'administration apparaît ainsi comme un volet essentiel dans la construction d'une stratégie nationale globale de prévention et de gestion des risques.

---

[217] Alexandre Freschi et Thomas Gassiloud, Mission d'information sur la résilience nationale, Assemblée nationale, 23 février 2022.

[218] Dans un contexte de multiplication des opérations extérieures, notamment au Sahel et au Moyen-Orient (telles « *Chammal* » et « *Daman* ») et des interventions militaires menées conformément aux engagements internationaux de la France, notamment pour la protection des espaces maritimes (telles « *Atalante* », « *Irini* », « *Agénor* » ou encore « *Corymbe* ») ou en vue du renforcement du flanc Est de l'Organisation du traité de l'Atlantique Nord (telles « *Aigle* » et « *Linx* »).

La modernisation du droit applicable en la matière constituerait alors, pour l'Etat, la garantie qu'il dispose d'un vecteur d'action efficace, répondant à des conditions de mise en œuvre claires et adaptées aux évolutions du contexte stratégique.

Compte tenu des sujétions qui s'attachent à l'application d'un régime de réquisition pour les personnes privées, une telle refonte du droit en vigueur ne peut être prévue, en vertu de l'article 34 de la Constitution, que dans le cadre d'un dispositif législatif, assorti de toutes les garanties applicables au titre de la jurisprudence constitutionnelle et européenne, tant au regard de l'exécution des réquisitions que du point de vue de l'indemnisation des prestations effectivement réalisées et des dommages subis à cette occasion.

2.2. OBJECTIFS POURSUIVIS

Ainsi qu'il ressort de la rubrique 1.1 *supra*, le régime des réquisitions défini par le code de la défense est historiquement fondé sur deux régimes distincts : d'une part, celui des réquisitions militaires, dont l'objet principal est d'assurer l'approvisionnement des forces armées et formations rattachées, et, d'autre part, celui des réquisitions pour les besoins généraux de la Nation, destiné à obtenir les prestations nécessaires aux besoins de la Nation pour répondre à des situations critiques.

Or, ces dispositions apparaissent aujourd'hui largement obsolètes, complexes à mettre en œuvre et fondées sur des critères dont la portée est parfois incertaine. Ces carences nuisent à l'efficacité générale des dispositifs en cause et obèrent les capacités des autorités militaires à les mettre en œuvre dans des situations d'urgence.

Ces carences structurelles ont notamment justifié la création récente d'un nouveau régime de réquisition de biens et services spatiaux, fondé sur des critères d'utilisation revus, sur une procédure de mise en œuvre allégée et sur un principe de réparation intégrale des dépenses engagées par les opérateurs spatiaux concernés et des dommages survenus à cette occasion.

2.2.1. La nécessité d'une clarification des cas de recours possibles au régime des réquisitions et de leur adaptation au contexte actuel

En premier lieu, les cas d'ouverture du droit à réquisition ne paraissent plus adaptés aux évolutions du contexte stratégique, notamment au regard des besoins de la défense nationale et des missions dévolues aux forces armées et formations rattachées.

En effet, les réquisitions miliaires ne peuvent être utilisées, pour les besoins de l'armée de terre et de la gendarmerie, qu' « *en cas de mobilisation partielle ou générale* […] *ou de rassemblement des troupes* » (article L. 2221-2 du code de la défense), ce qui apparaît particulièrement restrictif. Indépendamment de ces circonstances exceptionnelles, elles peuvent, certes, être utilisées « *en tout temps et en tout lieu* » pour répondre aux besoins de la marine et de l'armée de l'air et de l'espace (article L. 2221-3 du même code) mais, « *hors le cas de mobilisation* », il ne peut être fait réquisition que des prestations d'approvisionnement

énumérées aux 1° à 6° de l'article L. 2222-1 (logement, vivres, chauffage, moyens de transport et leurs accessoires, matériaux, outils et machines nécessaires à l'exécution des travaux militaires), à l'exclusion par exemple des nécessités liées au maintien en condition opérationnelle des équipements militaires ou de l'approvisionnement des forces en armes, munitions ou matériels de guerre. En tout état de cause, il apparaît que les réquisitions militaires revêtent un caractère subsidiaire par rapport aux réquisitions pour les besoins généraux de la Nation (article L. 2221-1 du code de la défense).

De même, lorsqu'elle est destinée à répondre aux « *besoins de la défense* », la mise en œuvre des réquisitions pour les besoins généraux de la Nation est subordonnée à la mise en œuvre de la mobilisation générale ou de la mise en garde ou à l'existence d'une menace portant notamment sur une partie du territoire, sur un secteur de la vie nationale ou sur une fraction de la population (article L. 2211-1, qui renvoie aux cas énumérés à l'article L. 1111-2). Si d'autres dispositions permettent, en principe, d'élargir l'utilisation potentielle de ce type de mesure « *indépendamment des cas prévus à l'article L. 1111-2* » (article L. 2211-2), cette faculté n'est assortie d'aucune précision ni condition, induisant de fortes interrogations quant à la constitutionnalité d'un tel recours à la réquisition.

Compte tenu de ce dernier risque juridique, l'ouverture du droit de réquisition semble cantonnée à des situations d'une exceptionnelle gravité, restreignant de ce fait considérablement sa portée et, au-delà, son utilité opérationnelle.

A cet égard, il paraît, en outre, indispensable de prendre davantage en compte l'anticipation des menaces et des crises, en dotant l'Etat de capacités d'intervention en amont de leur survenance. La guerre en Ukraine et, dans une certaine mesure, la crise sanitaire, ont ainsi démontré que les réponses apportées à des évènements d'une telle ampleur s'avèrent généralement beaucoup plus onéreuses que celles qui auraient pu être mises en œuvre en amont, afin d'en prévenir ou d'en limiter les effets. Cela est d'autant plus vrai en matière militaire, où la réquisition de certaines matières ou de certains composants nécessaires à la fabrication ou à l'entretien des matériels de guerre apparaît sensiblement moins efficace lorsque des opérations militaires sont engagées compte tenu des délais de production nécessaires au renouvellement des stocks, qui plus est dans un secteur extrêmement concurrentiel et marqué par des situations de pénuries mondiales. Dans cette perspective, il peut s'avérer nécessaire de réquisitionner tout ou partie d'une chaîne de production, sans qu'une menace directe et immédiate pesant sur le territoire national ne soit nécessairement caractérisée.

Parallèlement, il importe de doter la puissance publique d'un droit de réquisition lorsqu'elle est confrontée à un besoin urgent de sauvegarder les intérêts de la défense nationale. A titre d'exemple, dans l'hypothèse où un avion de chasse s'abîmerait en mer, l'armée peut avoir besoin de recourir, dans les meilleurs délais, aux moyens de sociétés spécialisées dans le secteur des activités en eaux profondes pour récupérer l'appareil avant l'intervention de puissances étrangères, préservant ainsi des informations protégées qui lui confèrent un avantage militaire tactique.

A l'aune de ces développements, il paraît nécessaire de clarifier les cas d'ouverture du droit à réquisition en déterminant de manière exhaustive la typologie des situations dans lesquelles l'Etat pourrait y recourir, apportant par la même occasion des garanties de sécurité juridique aux pouvoirs publics comme aux personnes privées potentiellement concernées.

2.2.2. La nécessité d'une démarche globale de simplification des dispositions en vigueur

En deuxième lieu, les modalités d'exercice des réquisitions prévues par le code de la défense apparaissent particulièrement complexes, étant précisé qu'elles sont régies par près d'une centaine d'articles législatifs et plus de cent quatre-vingt articles réglementaires. A titre de comparaison, le cadre juridique applicable aux réquisitions préfectorales, qui apparaît pourtant parfaitement opérationnel, est fondé sur un article législatif unique, prévu à l'article L. 2215-1 du code général des collectivités territoriales. Ce constat témoigne de la nécessité de simplifier drastiquement les règles en vigueur afin de les rendre pleinement applicables et opérationnelles pour l'autorité administrative.

Certaines dispositions apparaissent, de surcroît, anachroniques et doivent en ce sens être modifiées ou supprimées, à l'instar de celles portant sur « *les personnels féminins* » (article L. 2212-2), sur « *les communautés religieuses cloîtrées* » (article L. 2223-4) ou encore celles précisant que « *les habitants ne sont jamais délogés de la chambre ou du lit où ils ont l'habitude de coucher* » (article L. 2223-5). Dans le même ordre d'idées, il ne paraît aujourd'hui plus nécessaire de conserver dans la loi des subdivisions aussi développées que celles relatives aux réquisitions se rapportant au « *logement et [au] cantonnement* » (articles L. 2223-1 à L. 2223-1), aux « *véhicules* » (articles L. 2223-7 à L. 2223-11), aux « *chemins de fer* » (articles L. 2223-12 à L. 2223-16), « *aux voies navigables* » (article L. 2223-17), aux « *établissements industriels* » (articles L. 2222-2 et L. 2223-18) ou encore aux « *marchandises déposées dans les entrepôts de douane et dans les magasins généraux, ou en cours de transport par voie ferré*e » (article L. 2223-19), d'autant qu'en dépit de ces longs développements, il apparaît paradoxalement que les garanties apportées aux personnes requises dans ces situations ne sont pas nécessairement adaptées aux exigences constitutionnelles actuelles.

Enfin, la construction même de la partie législative du code de la défense consacrée aux réquisitions comporte un certain nombre d'incohérences auxquelles il convient de remédier. Parmi les plus notables, il peut être souligné que figurent dans un chapitre consacré aux réquisitions de biens et services pour les besoins généraux de la Nation des dispositions consacrées aux transports maritimes présentant un caractère d'intérêt national (articles L. 2213-5 à L. 2213-8), dont les conditions de mise en œuvre sont définies à l'amiable entre les armateurs et l'administration, et à la constitution d'une flotte à caractère stratégique (article L. 2213-9), « *permettant d'assurer en temps de crise la sécurité des approvisionnements de toute nature, des moyens de communications, des services et des travaux maritimes indispensables ainsi que de compléter les moyens des forces armées* », alors que les dispositifs en cause ont, en principe, vocation à être utilisés hors réquisition.

2.2.3. La nécessité d'une refonte du régime d'indemnisation en vigueur

En troisième lieu, il apparaît que le régime d'indemnisation des réquisitions et des dommages qui en résultent, tel qu'il est défini par le code de la défense, est particulièrement inadapté, eu égard à la complexité des mécanismes de détermination du montant des indemnités, à l'inadéquation des règles procédurales en vigueur avec la structuration actuelle de l'administration ainsi qu'au caractère désuet des modes de règlement des différends qu'il institue entre l'Etat et les administrés.

Afin d'illustrer cette complexité, il peut être souligné que l'indemnisation des prestations requises distingue la situation des réquisitions d'immeubles, d'exploitations, selon qu'elles sont ou non agricoles (article L. 2234-2), des biens meubles (article L. 2234-4), des véhicules automobiles (article L. 2234-6), des personnes (article L. 2234-7) ainsi que des logements de troupes (articles L. 2234-8 et L. 2234-9). Nonobstant ces règles particulières, il est précisé, d'une part, que « *chaque fois que les circonstances le permettent, des tarifs ou des barèmes d'indemnisation, établis dans le cadre de la législation sur les prix, sont définis par arrêtés conjoints du ministre de la défense, du ministre de l'économie et des finances et du ministre responsable de la ressource, après consultation obligatoire ou sur proposition d'un comité consultatif* […]*, qui s'adjoint, à cette occasion, des représentants des organismes professionnels* » (article L. 2234-5) et, d'autre part, que « *des indemnités complémentaires sont allouées éventuellement, sur justifications, pour compenser des préjudices non indemnisés* » (article L. 2234-3). De même, s'agissant de la réparation des préjudices subis par les personnes requises, des règles spécifiques sont prévues pour régir les « *conséquences des travaux exécutés par l'Etat sur des immeubles, des navires ou des aéronefs réquisitionnés* » (articles L. 2234-11 à L. 2234-16).

Au-delà du risque d'inconstitutionnalité d'un tel régime de réparation forfaitaire (cf. item 1.2.3), la procédure de règlement des indemnités dues au titre des réquisitions apparaît excessivement lourde, dans la mesure où « *Dans chaque département siège une commission d'évaluation des réquisitions composée en nombre égal de représentants des administrations publiques et de représentants des groupements économiques, professionnels, industriels, commerciaux ou agricoles* » (article L. 2234-20), qui se prononce sur la fixation des tarifs ou des barèmes d'indemnisation susmentionnés (article L. 2234-5) ou lorsque la personne requise conteste le montant de l'indemnisation (article L. 2234-21). En outre, il apparaît que « *des commissions spéciales d'évaluation peuvent être instituées pour certaines catégories de biens, à l'initiative du ministre responsable* » (article L. 2234-20).

La simplification des dispositions en cause, peu aisées à mettre en œuvre en cas de crise, permettra de renforcer l'efficacité du régime des réquisitions fixé par le code de la défense. Au-delà, il peut être souligné que les modifications en cause produiront des effets équivalents sur de multiples autres régimes juridiques qui renvoient à ce dispositif d'indemnisation.

2.2.4. La nécessité de compléter les dispositifs connexes aux réquisitions

En quatrième et dernier lieu, le code de la défense aménage des dispositifs connexes à celui des réquisitions, qui méritent d'être développés, afin de leur conférer leur pleine efficacité, mais également renforcés, pour répondre aux exigences constitutionnelles actuelles.

Ainsi, l'article L. 2232-1 prévoit que « *Le Gouvernement peut procéder dès le temps de paix* […] *à tout recensement de personnes, matériels, véhicules, matières ou objets, produits, denrées alimentaires, outillage, immeubles, installations ou entreprises susceptibles d'être requis à la mobilisation ou dans les cas prévus à l'article L. 1111-2 et à tous essais qu'il juge indispensables* ». Cependant, il n'existe pas, à ce jour, de possibilité de planifier des exercices de crises.

Or, ainsi que le souligne le rapport de la mission d'information parlementaire évoqué au sein de l'item 1.1 *supra*, il importe de développer en France une culture du risque, présentée par le portail « *Géorisques* » du ministère de la transition écologique comme devant « *permettre d'acquérir des règles de conduite et des réflexes, mais aussi de débattre collectivement des pratiques, des positionnements et des enjeux* ». Il s'agit ainsi d'« *améliorer l'efficacité de la prévention et de la protection* », en « *faisant émerger toute une série de comportements adaptés lorsqu'un événement majeur survient* ». Cette exigence se traduit à travers la recommandation n° 1 formulée par ledit rapport, qui préconise de « *développer la culture du risque auprès de la population française par des politiques de sensibilisation et d'exercices pratiques à intervalles réguliers* ».

Au-delà de ces considérations, assortir la possibilité de recenser et de tester, en amont, les personnes, biens et services susceptibles d'être réquisitionnés de celle de les mobiliser dans le cadre d'exercices confèrerait ainsi à l'Etat une vision exhaustive des ressources mobilisables en fonction des menaces. Par ailleurs, la mise en œuvre d'une telle faculté lui permettrait d'engager un dialogue avec les personnes potentiellement concernées, facilitant par la même occasion la recherche de solutions amiables, alternatives à la mise en œuvre des réquisitions, une fois la crise survenue. De même, l'appréhension des conditions pratiques de mise en œuvre de ces mesures permettrait, pour l'Etat, de mieux circonscrire ses besoins et, pour les entreprises concernées, de préparer, le cas échéant, des modèles alternatifs permettant la poursuite de leur activité ou, tout au moins, de réduire l'impact des réquisitions sur leur modèle économique.

Enfin, il apparaît nécessaire d'assortir les dispositions législatives applicables au recensement ainsi que celles permettant de prescrire le blocage des biens mobiliers en vue de procéder à leur réquisition (article L. 2233-1) de conditions maximales de durée, afin de garantir que leur mise en œuvre n'aura qu'un impact limité sur les droits des personnes concernées. Il convient, en outre, de souligner l'importance d'assurer la pleine effectivité de ce dernier dispositif, qui permet d'empêcher que les biens susceptibles d'être réquisitionnés ne soient préalablement vendus ou exportés afin, d'une part, de conférer à l'autorité administrative le temps nécessaire pour définir et mettre en œuvre un plan de réquisition et, d'autre part, de préserver les capacités internes de réponse aux besoins de la Nation.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

En préambule, il peut être souligné qu'il n'est pas apparu opportun de développer de nouveaux mécanismes contractuels pour répondre aux difficultés et aux objectifs respectivement présentés aux items 2.1 et 2.2. En effet, toutes les réquisitions obéissent au principe de subsidiarité : il ne peut en être fait usage, d'une part, que lorsque les moyens dont dispose l'Etat sont inexistants, inadaptés, indisponibles ou insuffisants et, d'autre part, après qu'un accord amiable ait été recherché avec la personne concernée, sauf lorsque l'urgence de la situation ne le permet pas.

Dès lors, deux grandes options ont été envisagées :

- soit conserver l'architecture générale du code de la défense, en ne procédant qu'aux ajustements nécessaires pour répondre efficacement aux besoins de la défense nationale ;
- soit procéder à une refonte totale des dispositions en vigueur, rompant ainsi avec un corpus juridique dont la rédaction s'inscrit dans la droite ligne des dispositions des lois du 3 juillet 1877 et du 11 juillet 1938, s'agissant respectivement des réquisitions militaires et des réquisitions pour les besoins généraux de la Nation.

Or, c'est précisément la question de la conservation de cette distinction, sur laquelle repose, depuis l'origine, le droit français des réquisitions, qui a permis de faire un choix entre les deux options susmentionnées. En effet, après une démarche de recensement des besoins de la défense réalisée au sein du ministère des armées, il est apparu que les réquisitions militaires étaient aujourd'hui devenues manifestement inadaptées au cadre d'emploi des forces armées et formations rattachées sur le territoire national, étant rappelé que l'article L. 1321-1 du code de la défense énonce qu'en principe « *aucune force armée ne peut agir sur le territoire de la République pour les besoins de la défense et de la sécurité civiles sans une réquisition légale* ». *A contrario*, nonobstant sa complexité et ses lacunes, le dispositif des réquisitions pour les besoins généraux de la Nation, beaucoup plus large dans son objet, semblait offrir, dans ses grands principes de mise en œuvre, un cadre juridique approprié.

Dès lors que l'option retenue était de supprimer les réquisitions militaires, une réforme d'ampleur semblait donc s'imposer puisqu'il était *a minima* nécessaire d'abroger le titre II du livre II de la deuxième partie du code de la défense et quelques articles connexes (article, L. 2234-8 et L. 2236-3 à L. 2236-5), soit 37 articles législatifs. En outre, il ne paraissait plus cohérent de conserver un titre I consacré aux réquisitions pour les besoins généraux de la Nation et un titre III relatif aux « *dispositions communes à l'ensemble des réquisitions* ». Eu égard à la nécessité de clarifier les cas de recours possibles au régime des réquisitions pour les besoins généraux de la Nation, de supprimer certaines dispositions anachroniques, de remédier aux incohérences de la construction de certaines subdivisions du titre I, de rendre plus opérationnel le mécanisme d'indemnisation et d'assortir les dispositions en vigueur de garanties conformes

aux exigences constitutionnelles, une simple renumérotation des règles en vigueur, moyennant quelques ajustements, apparaissait ainsi largement insuffisante.

Afin de respecter les objectifs de simplification et de lisibilité du droit, l'option d'une refonte totale du régime des réquisitions a ainsi été retenue.

3.2. OPTION RETENUE

3.2.1. S'agissant des dispositifs connexes aux réquisitions

Les dispositions concernant les transports maritimes présentant un caractère d'intérêt national et la constitution d'une flotte à caractère stratégique, prévues aux articles L. 2213-5 à L. 2213-9 du code de la défense, sont conservées à droit constant et intégrées dans la première partie du code de la défense, au sein du chapitre consacré au contrôle naval de la navigation maritime. Seul l'article L. 2213-8 relatif à la réquisition de cette flotte n'a pas été conservé, son utilité disparaissant en ce qu'il n'apparaît plus opportun de distinguer le régime selon le type de biens.

Par ailleurs, comme le relève l'item 2.2.4 *supra*, le mécanisme du recensement et des essais prévu à l'actuel article L. 2232-1 est repris et complété, afin d'être conforme aux exigences de l'article 34 de la Constitution. Le Premier ministre peut ordonner le recensement des personnes, biens et services susceptibles d'être requis que les ministres intéressés peuvent soumettre à tous essais ou exercices, sous certaines conditions et limites : ils doivent tenir compte des nécessités de fonctionnement des entreprises concernées et de la continuité du service public et ne peuvent excéder cinq jours par an.

La programmation des essais et exercices est portée à la connaissance des personnes concernées et, le cas échéant, de leur employeur au plus tard quinze jours avant leur exécution et la réalisation de ces derniers ouvrent droit à indemnisation.

Comme le relève l'item 2.2.4 *supra*, le mécanisme du blocage des biens mobiliers, actuellement prévu à l'article L. 2233-1, est également conservé et assorti de garanties au regard des exigences de l'article 34 de la Constitution et des droits et libertés en cause. Les garanties de durée et d'indemnisation qui sont prévues en partie réglementaire sont rehaussées au niveau législatif. Le blocage est limité à quinze jours, renouvelable une fois, ce délai devant être suivi soit d'une réquisition, soit d'une levée. Il obéit, par ailleurs, aux mêmes conditions que les réquisitions en ce qui concerne les garanties apportées aux personnes. Ce dernier donne lieu à indemnisation.

3.2.2. S'agissant des cas d'usage des réquisitions

La dichotomie entre les réquisitions pour les besoins de la Nation et les réquisitions militaires est remplacée par la dichotomie entre les réquisitions visant à répondre à :

– une menace actuelle ou prévisible sur les activités essentielles à la vie de la Nation, la protection de la population, l'intégrité du territoire, la permanence des institutions de la République ou justifiant la mise en œuvre des engagements internationaux de l'Etat en matière de défense.

  Ce cas d'usage, qui s'inspire des notions retenues à l'article L. 1111-1 relatif à la stratégie de sécurité nationale et à la politique de défense, en ce qu'il concerne la continuité de l'État, la permanence des institutions, l'intégrité du territoire et le respect des traités, relève des attributions dévolues par l'article 5 de la Constitution au Président de la République[219]. Un décret en Conseil des ministres sera alors nécessaire pour ouvrir le recours à ce type de réquisition.

  Le Président de la République pourra également habiliter l'autorité administrative ou militaire qu'il désigne à procéder à ces mesures.

– une urgence, lorsque la sauvegarde des intérêts de la défense nationale le justifie. Ces critères sont inspirés des dispositions concernant les réquisitions préfectorales et les réquisitions spatiales[220]. Ce cas d'usage relève des attributions dévolues par la Constitution au Premier ministre qui est responsable de la Défense Nationale (article 21). Un décret du Premier ministre sera alors nécessaire pour ouvrir le recours à ce type de réquisition.

  Cette hypothèse de réquisition peut intervenir si les conditions précitées sont réunies et si les circonstances n'appellent pas une réponse du Président de la République.

Dans les deux hypothèses, les réquisitions peuvent concerner toute personne, physique ou morale, ainsi que tous biens et services nécessaires pour parer à la menace ou à l'urgence. Il est en effet proposé, pour des motifs de simplification et d'intelligibilité de la norme, de renoncer aux nombreux régimes qui concernent tel type de bien ou tel type de services.

En outre, l'activation de ces deux types de réquisitions ne fera pas obstacle au déclenchement du rappel ou du maintien à l'activité des personnes soumises à l'obligation de disponibilité au titre de la réserve opérationnelle militaire en cas de circonstances exceptionnelles, dont les conditions de mises en œuvre sont également modernisées par le présent projet de loi.

3.2.3. S'agissant des conditions de fond des réquisitions

Chaque type de réquisition obéit à un régime identique : les mesures prescrites doivent être strictement proportionnées aux objectifs poursuivis et adaptées aux circonstances de temps et de lieu. Une réquisition ne peut être ordonnée qu'à défaut de tout autre moyen adéquat pour répondre au besoin et ne peut durer plus longtemps que ce qui est nécessaire.

Chaque décision de réquisition devra préciser son objet et ses modalités d'application. En matière de réquisitions de personnes, les aptitudes physiques et psychiques, ainsi que les

[219] M. Dominique L, 28 novembre 2014, n° 2014-432 QPC, considérant 9.

[220] Cf. article L. 2224-1 du code de la défense.

compétences professionnelles et techniques seront prises en compte et permettront de ne réquisitionner que les personnes nécessaires et pouvant répondre à l'objectif poursuivi. Cette mesure permettra de renforcer l'application du principe de proportionnalité des réquisitions et assurera également une protection supplémentaire de publics potentiellement fragiles (personnes en situation de handicap, femmes enceintes, *etc.*).

3.2.4. S'agissant du champ d'application territorial du dispositif

Le champ d'application territorial du dispositif est défini :

- toute personne physique sur le territoire national pourra être réquisitionnée et, ce, quelle que soit sa nationalité ;
- de même, tout ressortissant français, quel que soit son lieu de résidence, pourra également faire l'objet de ces mesures. En effet, les situations imposant de recourir aux réquisitions ne peuvent jamais être totalement prédéfinies à l'avance et certains ressortissants français disposant de compétences particulières pourraient être utiles aux armées en cas d'assistance à des pays alliés ;
- ne pourront en revanche être réquisitionnées que les personnes morales dont le siège est situé en France ;
- enfin, il est apparu nécessaire de rédiger une disposition spécifique pour les navires. La nationalité du pavillon du navire se distingue en effet de la nationalité de son armateur. La Convention sur le droit de la mer du 10 décembre 1982 de Montego Bay prévoit l'application de la loi de l'Etat du pavillon, où que le navire se trouve. Afin de respecter cette convention internationale et d'éviter des situations potentiellement sensibles, il a été estimé préférable de mentionner expressément cette restriction.

3.2.5. S'agissant des modalités d'indemnisation

L'indemnisation des réquisitions (ainsi que du blocage), dont les modalités sont prévues au futur article L. 2212-8 du code de la défense, reprendra les grands principes du régime fixé pour les réquisitions préfectorales. Seront rétribués les frais matériels, directs et certains résultant de l'application des mesures prescrites, et uniquement ces derniers. En effet, l'indemnisation de réquisition ne peut être source d'enrichissement sans cause pour la personne réquisitionnée. Si la réparation doit être intégrale, elle ne peut être supérieure à la réalité des préjudices, conformément à l'exigence constitutionnelle de bon usage des deniers publics[221]. Le montant de la rétribution sera établi sur la base du prix normal et licite de la prestation.

Pour les dommages qui ne seraient pas couverts par la rétribution (exemple de dommages causés aux biens de la personne faisant l'objet de la réquisition), un alinéa prévoit la réparation intégrale desdits dommages sauf fait personnel de la personne requise. Enfin, le cas de

[221] Loi portant réforme de la représentation devant les cours d'appel, 20 janvier 2011, décision n° 2010-624 DC.

dommage résultant de faits du tiers est également prévu, l'Etat étant dans ce cas subrogé dans les droits de la victime.

Il appartiendra à la juridiction administrative au regard de ses attributions découlant de la Constitution de connaître des recours introduits par les administrés en la matière.

Afin d'assurer le respect du bon usage des deniers publics, la personne requise sera tenue de fournir à l'autorité administrative ou militaire, si celle-ci en fait la demande, tous documents ou éléments d'information permettant d'évaluer le montant de l'indemnisation qui lui est due. Les agents publics assurant ces missions seront tenus au secret professionnel.

3.2.6. S'agissant de l'exécution des réquisitions

Au regard des enjeux en cause, le dispositif reprend ce qui existe actuellement dans le code de la défense[222] et dans le code général des collectivités territoriales, pour les réquisitions préfectorales, en prévoyant la possibilité pour l'Etat de faire exécuter d'office les mesures prescrites par la décision de réquisition.

En outre, le principe de la sanction pénale en cas d'inexécution volontaire par la personne requise d'une mesure de réquisition légalement ordonnée est maintenu.

Toutefois, afin de prévoir des peines suffisamment dissuasives au regard des enjeux en cause, d'une part, et, d'autre part, de disposer des prérogatives d'enquête adaptées, le quantum de la sanction pénale (actuellement d'un an d'emprisonnement et d'une amende de 4 500 euros en temps de paix) est aligné sur le quantum existant pour les réquisitions spatiales[223], soit une peine de cinq ans d'emprisonnement et de 500 000 euros d'amende.

Enfin, le fait pour un agent public de procéder à des réquisitions illégales sera lui aussi sanctionné pénalement qu'il soit militaire[224] ou civil[225]. Cette mesure reprend les dispositions actuelles du code de la défense.

3.2.7. S'agissant des mesures de coordination des dispositifs

Le présent article comprend enfin des dispositions d'adaptation, dans différentes parties du code de la défense, d'une part, et dans d'autres codes et textes législatifs, d'autre part, afin notamment de procéder à une actualisation des renvois existants actuellement. Ces actualisations ne

[222] Article L. 2221-10 du code de la défense.

[223] Article L. 2236-2-1 du code de la défense.

[224] Article L. 323-22 du code de justice militaire : « Le fait pour tout militaire d'exercer une réquisition sans avoir qualité pour le faire est puni, si cette réquisition est faite sans violence, d'un emprisonnement de cinq ans. Si cette réquisition est exercée avec violence, il est puni de dix ans d'emprisonnement. »

[225] Cinq ans d'emprisonnement et une amende de 500 000 euros en application des dispositions combinées de l'article 432-10 du code pénal et de l'actuel article L. 2236-6 du code de la défense.

s'accompagnent d'aucune modification du fond des articles impactés, à l'exception des articles consacrés à l'adaptation outre-mer de ces modifications.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

Les simplifications apportées au régime des réquisitions défini par le code de la défense bénéficieront directement aux nombreux autres dispositifs qui renvoient à son mécanisme d'indemnisation, renforçant, par voie de conséquence, leur utilité opérationnelle. Tel est ainsi le cas pour :

- les réquisitions des services chargés de l'exploitation d'installations de production d'électricité utilisant du gaz naturel, réalisées par le ministre de l'énergie sur le fondement des dispositions du 2° de l'article L. 143-6-1 du code de l'énergie ;
- les réquisitions des personnes et des biens, réalisées par l'autorité administrative compétente de l'Etat en vue de mettre fin à un danger grave d'atteinte au littoral ou aux intérêts connexes français résultant d'une avarie ou d'un accident survenu en mer, sur le fondement des dispositions du V de l'article L. 218-72 du code de l'environnement ;
- les réquisitions de professionnels de santé, d'établissements de santé ou d'établissements médico-sociaux, réalisées par les autorités territorialement compétentes de l'Etat sur le fondement des dispositions des articles L. 3131-8 et L. 3131-9 du code de la santé publique ;
- les réquisitions d'armateurs, de capitaines, de maîtres ou de patrons de navires, marins, ouvriers-dockers, pilotes, lamaneurs et remorqueurs, réalisées par l'autorité investie du pouvoir de police portuaire ou par l'autorité portuaire afin de fournir leur service et les moyens correspondants, sur le fondement des dispositions de l'article L. 5331-9 du code des transports ;
- la diffusion par tous moyens audiovisuels, sans autorisation préalable de son auteur ou de ses ayants droit, d'une œuvre littéraire, scientifique ou artistique non inédite, réalisée par le ministre chargé de la communication sur le fondement des dispositions de l'article L. 1146-1 du code de la défense ;
- l'indemnisation des dommages causés par les exercices de tirs, marches, manœuvres ou opérations d'ensemble que comporte l'instruction des troupes, effectuée sur le fondement des dispositions de l'article L. 2161-2 du code de la défense.

Par ailleurs, les présentes dispositions nécessiteront, à titre de coordination, un certain nombre d'actualisation de références, tant dans le code de la défense (articles L. 1323-1 et L. 2113-2 ainsi que la sixième partie de ce code) que dans le code des assurances (articles L. 160-6 et L. 160-7), dans le code de l'énergie (article L. 143-3), dans le code de justice militaire (article L. 323-22), dans le code général des impôts (article 1048), dans le code des pensions militaires d'invalidité

et des victimes de guerre (article L. 522-5), dans le livre des procédures fiscales (article L. 130) et dans le code des transports (articles L. 5241-1 et L. 5434-1).

En tout état de cause, il convient de souligner qu'indépendamment de la simplification des processus d'indemnisation évoquée *supra*, la présente refonte du régime de réquisition prévu par le code de la défense n'a pas vocation – et n'aura pas davantage pour effet – de remettre en cause les conditions de mise en œuvre des autres dispositifs de réquisition.

En particulier, demeurent inchangées, dans les limites de leur compétence territoriale, les prérogatives conférées aux préfets sur le fondement des dispositions du 4° de l'article L. 2215-1 du code général des collectivités territoriales, dont la portée a été précisée par la jurisprudence comme s'appliquant aux « *mesures nécessaires, imposées par l'urgence et proportionnées aux nécessités de l'ordre public* »[226]. Ainsi, lorsqu'il s'agira d'assurer la protection de la population à l'échelle d'un département, le régime prévu par le code général des collectivités territoriales aura vocation à s'appliquer. Si l'ampleur territoriale de la menace excède les limites d'un département, le code de la défense sera susceptible de s'appliquer à l'instar de la récente réquisition des sociétés de location d'hélicoptères, destinée à lutter contre les feux de forêt de grande ampleur, justifiée par la nécessité d'œuvrer « *de façon coordonnée sur l'ensemble du territoire national* » contre « *une menace importante pour l'ordre public* »[227]. En fonction des circonstances, la solution consistant à adopter plusieurs arrêtés sur le fondement du CGCT dans plusieurs départements restera naturellement ouverte.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Compte tenu des conditions restrictives d'ouverture du droit à réquisition prévu par le code de la défense, dont l'usage demeure par principe exceptionnel ainsi qu'en témoigne l'énumération exhaustive de son utilisation depuis 1958 figurant au sein de l'item 1.1 *supra*, la présente mesure n'aura *a priori* pas d'impact macroéconomique significatif.

4.2.2. Impacts sur les entreprises

Les entreprises réquisitionnées devront exercer leurs activités économiques au profit de l'Etat. Si toutes les actions menées dans le cadre de la réquisition seront indemnisées selon le prix normal de la prestation réalisée et si les dommages éventuels infligés à l'entreprise seront, en principe, intégralement couverts, les sommes qui leur seront ainsi versées à titre de compensation n'auront ni pour objet ni pour effet de pourvoir à un éventuel manque à gagner. En cas de pénalités contractuelles dues par l'entreprise réquisitionnée à l'un de ses cocontractants pour retard ou inexécution du contrat, du fait de la réquisition, le montant de ces

[226] CE, Juge des référés, 27 octobre 2010, n° 343966.

[227] Notice du décret n° 2022-1020 du 20 juillet 2022 portant ouverture du droit de réquisition des sociétés de location d'hélicoptères en capacité de participer à la lutte contre les feux de forêts.

pénalités pourra être supporté par l'Etat. En revanche, étant donné qu'il est impossible d'estimer avec précision la perte d'un avantage compétitif pour une entreprise dans de telles circonstances, celui-ci ne pourra être pris en compte.

Au demeurant, il convient de rappeler que, si une réquisition peut engendrer des coûts significatifs pour une entreprise, ce dispositif n'a vocation à être mis en œuvre qu'à titre exceptionnel et qu'il apparaît, dans la grande majorité des cas, possible de procéder par voie d'accord amiable.

Enfin, les impacts économiques et sociétaux de telles mesures pour les entreprises pourront être atténués par la capacité conférée à l'Etat de recenser au préalable les entreprises susceptibles d'être sollicitées et d'organiser de les associer à des exercices de crises. Ainsi, le périmètre des réquisitions éventuelles pourra être identifié et affiné avant toute application réelle, ce qui permettra de circonscrire les effets de la mesure au strict nécessaire, pour pénaliser au minimum l'activité des entreprises concernées.

4.2.3. Impacts budgétaires

Le coût de la réquisition et les dommages qu'elle aura éventuellement occasionnés, tant sur la personne ou le bien réquisitionné que sur les tiers, seront, en principe, intégralement assumés par l'Etat, à l'exclusion des dommages directement causés par la personne réquisitionnée. Dès lors, toute réquisition aura nécessairement un impact budgétaire. Néanmoins, en raison même du caractère exceptionnel de la réquisition, ce dernier demeure impossible à quantifier.

En revanche, le souci d'apporter une juste indemnisation aux personnes réquisitionnées, tout en assurant la meilleure gestion possible des deniers de l'Etat justifie la création d'un dispositif d'enquête, permettant aux agents habilités de l'Etat de procéder à des contrôles sur pièces et sur place auprès des intéressés. Ce dispositif, qui n'a pas vocation à être utilisé de façon systématique, pourra notamment trouver à s'appliquer lorsque l'estimation du coût de la réquisition par la personne réquisitionnée sera considérée comme excessive par l'administration requérante.

En tout état de cause, le coût financier de la réquisition constituera l'un des paramètres que l'Etat devra prendre en compte avant de décider d'user de ce pouvoir et conditionnera, le cas échéant, le périmètre des mesures effectivement mises en œuvre.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales, comme toutes personnes morales, sont susceptibles d'être mises à contribution et de voir leurs moyens réquisitionnés. Conformément au principe de libre administration des collectivités territoriales, les sujétions qui leur sont imposées en la matière sont fixées par la loi, à l'article L. 1111-7 du code général des collectivités territoriales, qui prévoit que « *les collectivités territoriales exercent leurs compétences propres dans le respect des sujétions imposées par la défense nationale* » et, à ce titre, que « *l'Etat dispose en tant que*

de besoin des services des communes, des départements, des régions, de leurs groupements et de leurs établissements publics . Dès lors, il ne semble pas nécessaire de reprendre ces dispositions dans le code de la défense.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'application du droit des réquisitions demeure facultative pour l'autorité administrative et ne peut intervenir qu'à titre subsidiaire, lorsqu'aucune autre solution n'apparaît envisageable et qu'il n'est pas possible d'obtenir un accord amiable. Elle ne saurait, en ce sens, être considérée comme représentant une charge pérenne pour les services compétents.

Au demeurant, un certain nombre de dispositions sont destinées à faciliter la mise en œuvre du dispositif par l'autorité administrative, à savoir :

- la faculté de recenser, en amont, les personnes, biens et services susceptibles d'être réquisitionnés (article L. 2211-1), qui permet de définir *a priori* le périmètre des mesures à mettre en œuvre en cas de survenance d'une situation critique et d'obtenir, à cette fin, de précieuses informations ;
- la faculté d'organiser des essais ou exercices (article L. 2211-1), qui permet tout à la fois d'établir un dialogue avec les personnes concernées, d'obtenir en amont les informations nécessaires sur les personnes, bien ou services en cause et de se préparer à la mise en œuvre pratique du dispositif, le moment venu ;
- la faculté de prescrire une mesure de blocage (articles L. 2211-2 à L. 2211-4), qui permet notamment à l'administration de disposer d'un délai de 15 à 30 jours pour définir et mettre en œuvre un plan organisé de réquisition, lorsque cela s'avère nécessaire.

Par ailleurs, des agents habilités par l'autorité administrative pourront, le cas échéant, effectuer des contrôles sur pièces et sur place pour s'assurer de la juste indemnisation des réquisitions opérées. Ce contrôle, qui sera mis en œuvre si les circonstances le justifient, ne paraît pas de nature à faire porter une charge supplémentaire démesurée à l'administration.

Enfin, la présente mesure simplifie sensiblement les procédures applicables en la matière, notamment en supprimant les commissions d'évaluation des réquisitions, les tarifs et barèmes d'indemnisation ou encore les procédures différenciées de mise en œuvre et d'indemnisation des réquisitions, qui alourdissaient jusqu'alors considérablement la tâche de l'administration.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur les personnes en situation de handicap

Les mesures envisagées ne comportent pas de dispositions spécifiques applicables aux personnes en situation de handicap. Cependant, le nouvel article L. 2212-6 du code de la défense précisera expressément que « *les personnes sont réquisitionnées en fonction de leurs aptitudes*

physiques et psychiques et de leurs compétences professionnelles ou techniques ». Ainsi, les réquisitions de personnes seront-elles individualisées et prendront en compte les caractéristiques personnelles des personnes concernées.

4.5.2. Impacts sur l'égalité entre les femmes et les hommes

Cet article n'emporte aucun impact sur l'égalité entre les femmes et les hommes. Bien que les dispositions en vigueur de l'article L. 2212-2 du code de la défense, qui comportent des dispositions spécifiquement consacrées à la réquisition de « *personnels féminins* » ne seront pas reprises, le nouvel article L. 2212-6, mentionné à l'item 4.5.1, permettra de tenir compte de la situation individuelle de chaque personne potentiellement concernée, par exemple s'agissant des femmes enceintes. Dans l'esprit de la réforme, les femmes et les hommes apparaissent en ce sens sur un strict pied d'égalité.

4.5.3. Impacts sur la jeunesse

Le présent article ne comporte aucune disposition impactant spécifiquement ce public.

4.5.4. Impacts sur les professions réglementées

Les dispositions envisagées n'entraînent aucun impact spécifique sur les professions réglementées.

4.6. IMPACTS SUR LES PARTICULIERS

Les particuliers pourront être faire l'objet de réquisitions, soit directement, soit à travers des mesures concernant leurs biens, soit en tant que salariés d'une entreprise réquisitionnée. Chaque mesure sera néanmoins assortie des garanties requises au titre des exigences constitutionnelles et conventionnelles évoquées au sein des items 1.2 et 1.3, tant sur les conditions de mise en œuvre de la réquisition elle-même que sur l'indemnisation apportée.

4.7. IMPACTS ENVIRONNEMENTAUX

Aucun impact environnemental spécifique n'a été identifié pour cette mesure.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les collectivités relevant de l'article 74 de la Constitution et la Nouvelle-Calédonie ont été saisies les 24 février 2023 (Saint-Barthélémy, Saint-Martin, Saint-Pierre-et-Miquelon, Polynésie Française), 27 février 2023 (Polynésie Française) et 28 février 2023 (Nouvelle-Calédonie).

Le Conseil supérieur des tribunaux administratifs et des cours administratives d'appel a été saisi le 24 février 2023 sur le fondement de l'article L. 232-3 du code de justice administrative et a rendu un avis favorable à l'unanimité le 23 mars 2023.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ainsi qu'il est précisé ci-dessous, au sein de l'item 5.2.3 *infra*, les présentes dispositions législatives nécessitent l'adoption d'un décret en Conseil d'Etat pour produire leur plein effet.

Ces mesures n'entreront en vigueur qu'à compter de la publication du décret d'application de cette mesure et au plus tard douze mois à compter de la publication de la présente loi.

5.2.2. Application dans l'espace

Conformément aux dispositions de l'article L. 1 du code de la défense, en tant qu'il s'agit d'une mesure liée à la politique de défense nationale, la présente mesure s'appliquera de plein droit sur l'ensemble du territoire de la République, y compris à l'ensemble des collectivités d'outre-mer, sans qu'aucune mention expresse d'application ne soit, en principe, requise.

Cependant, l'organisation administrative particulière de certaines collectivités et leur éloignement physique de la métropole, nécessitent l'adoption de modalités particulières de réquisition en cas de rupture des communications. Pour ce faire, le droit de réquisition, en ce cas particulier, sera attribué au haut fonctionnaire de défense et de sécurité territorialement compétent, à l'instar des pouvoirs de défense non militaire qui lui sont dévolus au titre de l'article L. 1311-1 du code de la défense, à charge pour lui d'en rendre compte dès que possible aux autorités compétentes.

Si les réquisitions pourront concerner toute personne physique présente sur le territoire national, y compris les ressortissants étrangers et les personnes morales dont le siège est situé en France, elles pourront également être appliquées à toute personne physique de nationalité française ne résidant pas sur le territoire national.

Enfin, comme cela a été explicité au sein de l'item 3.2 *supra*, la réquisition de navire s'effectuera en fonction de la nationalité de son pavillon, quelle que soit celle de l'armateur.

5.2.3. Textes d'application

Le livre II de la deuxième partie de la partie réglementaire du code de la défense devra être modifié par décret en Conseil d'Etat afin notamment :

- d'aligner ses subdivisions sur celles retenues dans la loi, conformément au principe de l'homothétie des parties législatives et réglementaires d'un code, en renumérotant en conséquence les articles dont le maintien apparaît nécessaire ;
- de tirer les conséquences de la suppression des réquisitions militaires, de la simplification globale des modalités d'exercice des réquisitions et de la refonte du régime d'indemnisation, en abrogeant les articles ainsi devenus sans objet ;
- de fixer les conditions de mise en œuvre pratique du recensement, des essais et exercices, du blocage et des deux nouvelles hypothèses de recours aux réquisitions, respectivement fondés sur l'urgence et sur la menace.

Article 24 : Organiser la possibilité de constituer des stocks stratégiques des matières ou composants d'intérêt stratégique pour les armées ainsi que la priorisation de la livraison de biens et services au bénéfice des armées

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Forte d'une dizaine de grands groupes et de près de 4 000 petites et moyennes entreprises et entreprises de taille intermédiaire – dont 500 identifiées comme stratégiques – qui génèrent près de 200 000 emplois directs ou indirects, la base industrielle et technologique de défense (BITD) constitue l'un des atouts majeurs de la France, lui permettant d'être l'une des rares nations à produire, de manière autonome, des équipements militaires aussi structurants que des avions de chasse ou des sous-marins nucléaires. Parmi les points forts de cet écosystème, l'on peut notamment citer la qualité du dialogue entre l'Etat et les entreprises concernées, la dualité de bon nombre d'entre elles, permettant de faire bénéficier le segment militaire des investissements dans le secteur civil (comme l'illustre l'avion de transport A400M), ainsi que leur succès à l'exportation.

Cependant, l'évolution récente de la situation internationale, marquée par une guerre de haute intensité sur le continent européen comme par les risques de pénurie de matières premières, rend plus que jamais nécessaire de sécuriser et de fluidifier l'approvisionnement en matériels et en munitions des forces armées françaises par les entreprises de la BITD. En effet, structuré autour de la dissuasion nucléaire et sur le recours à des forces expéditionnaires, notre modèle d'armée doit être adapté pour faire face à la dégradation du contexte stratégique sur tout le spectre de la conflictualité contemporaine, à l'aune du triptyque « *compétition-contestation-affrontement* » développé dans l'Actualisation stratégique de 2021. Ce dernier repose sur le constat d'une hausse sensible du budget militaire des grandes puissances depuis le début des années 2010, qui a fait de la compétition entre Etats le déterminant principal de leurs politiques de défense. Cette mondialisation de la compétition apparaît propice à la contestation, correspondant à la situation où un compétiteur profite d'une opportunité pour imposer un fait accompli, y compris en employant la force militaire, et à l'extension des champs de confrontation, multipliant, par voie de conséquence les risques d'affrontements militaires directs entre grandes puissances.

Depuis la fin de la guerre froide, dans un contexte de déflation du budget alloué à la défense[228] au titre des « *dividendes de la paix* », l'accent a été mis, s'agissant de l'équipement des forces armées, sur l'optimisation de la performance et sur la contrainte du coût. Cependant, le retour

[228] Au début des années 1980, le budget de la défense, hors pensions, représentait 3 % du PIB, contre 2 % aujourd'hui. En euros constants, il est, en outre, passé de 39 milliards d'euros en 1990 à 31,4 milliards d'euros en 2014, soit une diminution de 20 %.

de l'hypothèse d'un engagement majeur appelle un changement de paradigme, la capacité à réduire les délais de production et à augmenter la cadence des livraisons n'étant plus des variables d'ajustement, mais constituant à nouveau des enjeux cruciaux d'approvisionnement.

Or, au nombre des enseignements de la guerre en Ukraine, il apparaît que la structuration de l'outil national de production n'est plus adaptée à la situation actuelle de « *contestation* », au titre de laquelle nos forces armées ont besoin de reconstituer rapidement leurs stocks consécutivement aux livraisons réalisées au profit des forces ukrainiennes, ni *a fortiori* à une éventuelle situation d'« *affrontement* », au titre de laquelle elles seraient confrontées au niveau d'attrition, de consommation et d'érosion des matériels constaté dans les récents conflits.

Nonobstant la difficulté d'obtenir des chiffres précis s'agissant de la guerre en Ukraine, les pertes matérielles subies de part et d'autre comme le niveau de consommation de munitions témoignent de la réalité du risque de pénurie pour les belligérants. A ce titre, la récente mission d'information de l'Assemblée nationale sur la préparation à la haute intensité relevait que « *les taux d'attrition subis par l'armée israélienne lors de la guerre de Kippour (1973) ou l'armée argentine pendant la guerre des Malouines (1982)* [ont été] *respectivement de 4 % et 8 %* »[229].

Ces constats ont notamment été corroborés par de récents exercices de haute intensité menés par les armées, qui ont confirmé le nombre potentiellement élevé des destructions de matériels. Ainsi, l'exercice *Polaris 21*, réalisé en 2021, s'est soldé par la destruction de sept à huit bâtiments de premier rang sur la vingtaine mobilisée, dont deux frégates dans les quinze premières minutes. De même, les exercices *Volfa* menés par l'armée de l'air et de l'espace font ressortir des hauts niveaux d'attrition des aéronefs et de consommation de munitions.

A cet égard, la livraison d'équipements militaires à l'Ukraine a permis de mettre en lumière la relative faiblesse de nos stocks pour certains équipements ou munitions, s'agissant notamment des canons *Caesar* ou dans le domaine de la défense sol-air, mais également l'incapacité de notre BITD, sans évolution de son modèle actuel, à produire rapidement ces matériels en vue de reconstituer les stocks de nos forces armées et d'assurer la poursuite des livraisons aux forces ukrainiennes. A cette fin, le ministre des armées a proposé, le 22 février 2023, un plan d'action pour la production des munitions, axé sur la relocalisation des stocks et des lieux de production[230] ainsi que sur l'accélération de la cadence[231] et sur l'augmentation de la production[232] des munitions.

---

[229] Patricia Mirallès et Jean-Louis Thiérot, Mission d'information sur la préparation à la haute intensité, Assemblée nationale, 17 février 2022.

[230] Le ministre a notamment annoncé la décision prise par la société *Eurenco*, leader européen des explosifs, des propulseurs et des combustibles militaires, de relocaliser sa chaîne de production de poudre pour les gros calibres au premier semestre 2025, avec pour objectif de produire 1 200 tonnes de poudre par an, soit 500 000 charges modulaires, dans la ville de Bergerac.

[231] Tout particulièrement s'agissant des canons *Caesar*, des obus de 155 mm ainsi que des missiles *Mistral*, essentiels à la défense sol-airs, pour lesquels le ministre a précisé : « *Nous produisions 20 Mistral par mois en 2022. Ce chiffre est passé à 30 en 2023 et montera à 40 en 2024* ».

[232] L'accent est mis sur les partenariats européens, à l'image de la société MBDA à laquelle le Royaume-Uni, l'Italie et la France ont donné un mandat collectif pour réduire la production des missiles *Aster* de 40 à 18 mois.

Au vu de ces constats, le Président de la République a insisté sur la nécessité d'entrer dans une « *économie de guerre* », à l'occasion de son discours aux armées du 13 juillet 2022, soulignant que « *Pour répondre à ce besoin que la Nation va avoir de continuer à s'équiper, parfois d'aider certains de nos amis ou alliés à s'équiper eux-mêmes, nous devons structurer une économie française et européenne dans laquelle les modèles, les rythmes, les standards doivent être envisagés selon, si je puis dire, un solfège différent*. […] *nous allons devoir investir parfois plus vite, plus fort et les industriels devront répondre à ces besoins.* […] *La très grande sophistication et la personnalisation de nos systèmes qui font notre force* […] *sont parfois causes de délais de développement et de production considérables* […]. *Reconstituer plus vite et plus fort certains stocks, savoir produire davantage des matériels qui sont adaptés à ce retour de la guerre de haute intensité sur notre sol, réinterroger certains choix d'innovation pour remettre en quelque sorte en équilibre, en tension, des objectifs qui peuvent rentrer en concurrence : l'innovation la plus extrême et les délais, la capacité à les produire en masse le plus vite possible. C'est pourquoi nous devons à chaque instant garder l'avantage technologique et tactique, tout en sécurisant les chaînes de sous-traitance et les approvisionnements en matières premières et maintenir les compétences nécessaires* ».

Ces orientations conduisent notamment à adapter l'économie générale des contrats relatifs aux matériels de guerre et, plus largement, des marchés de défense et de sécurité, dont le cadre législatif et réglementaire ne comporte actuellement aucune disposition spécifiquement dédiée à la sécurité des approvisionnements des forces armées. A cette fin, la Revue nationale stratégique de 2022 précise notamment qu'« *en complément d'acquisitions, sur les prochaines années, des équipements les plus critiques nécessaires pour faire face à un conflit de haute intensité ou susceptibles d'attrition rapide, un plan de préparation à l'économie de guerre est en cours d'élaboration afin d'adapter de manière progressive et modulable la BITD aux différents contextes géopolitiques* ». Au-delà de ces considérations, le contexte stratégique actuel souligne la nécessité de disposer d'outils juridiques nouveaux permettant, en période de crise, de pallier l'insuffisance des dispositifs contractuels pour mobiliser les ressources d'intérêt stratégique pour les armées et réduire les délais de livraison des matériels de guerre, dans un contexte concurrentiel.

1.2. CADRE CONSTITUTIONNEL

1.2.1. La sauvegarde des intérêts fondamentaux de la Nation est une exigence constitutionnelle susceptible de justifier une atteinte à d'autres principes à valeur constitutionnelle.

Il ressort de la jurisprudence du Conseil constitutionnel et du Conseil d'Etat que les « *exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* », au premier rang desquelles figurent l'indépendance nationale et l'intégrité du territoire, qui en sont la finalité, mais également la protection du secret de la défense nationale et la libre disposition de la force armée, sont prises en compte par le juge dans son contrôle de proportionnalité en cas d'atteinte à d'autres principes à valeur constitutionnelle.

Il revient au juge d'assurer une « *conciliation qui ne soit pas déséquilibrée* » entre la sauvegarde des intérêts fondamentaux de la Nation et les autres exigences constitutionnelles[233].

En tant qu'elle est fondée sur la mise en œuvre du principe de « *nécessaire libre disposition de la force armée* » découlant des articles 20 et 21 de la Constitution, en application desquels « *le Gouvernement décide, sous l'autorité du Président de la République, de l'emploi de la force armée* »[234], toute mesure destinée à garantir l'approvisionnement en matériel des armées peut ainsi porter atteinte à l'exercice de certains droits et libertés reconnus aux partenaires de l'administration.

1.2.2. Des restrictions peuvent être apportées à la liberté d'entreprendre dès lors qu'il n'en résulte pas d'atteinte disproportionnée au regard de l'objectif poursuivi.

Même si le Conseil constitutionnel rappelle que « *la liberté qui, aux termes de l'article 4 de la Déclaration* [des droits de l'Homme et du citoyen du 26 août 1789]*, consiste à pouvoir faire tout ce qui ne nuit pas à autrui, ne saurait elle-même être préservée si des restrictions arbitraires ou abusives étaient apportées à la liberté d'entreprendre* »[235], il considère que cette dernière « *n'est toutefois ni générale ni absolue* »[236] et « *qu'il est loisible au législateur d'apporter à cette liberté des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi* »[237].

A titre d'exemple, afin de reconnaître le caractère proportionné des dispositions de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence permettant à l'autorité administrative, dans le cadre de l'état d'urgence, d'ordonner la fermeture provisoire des salles de spectacle, débits de boissons et lieux de réunion de toute nature, le juge constitutionnel a constaté que le législateur avait encadré les conditions de mise en œuvre du dispositif, qu'il avait expressément prévu que les mesures en cause devaient être justifiées et proportionnées aux raisons les ayant motivé, que « *le juge administratif est chargé de s'assurer que chacune de ces mesures est adaptée, nécessaire et proportionnée à la finalité qu'elle poursuit* » et que la loi en définissait les conditions d'application dans le temps[238].

---

[233] Mme Ekaterina B., épouse D., et autres, 10 novembre 2011, n° 2011-192 QPC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif et du droit à un procès équitable ; Loi relative au renseignement, 23 juillet 2015, n° 2015-713 DC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif, du droit à un procès équitable et du principe du contradictoire ; Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias, 10 novembre 2016, n° 2016-738 DC, à propos de la liberté d'expression et de communication ; La Quadrature du net, 9 juillet 2021, n° 2021-924 QPC, à propos du respect de la vie privée.

[234] M. Dominique de L., 28 novembre 2014, n° 2014-432 QPC.

[235] Loi de nationalisation, 16 janvier 1982, n° 81-132 DC.

[236] Loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques, 20 janvier 1993, n° 92-316 DC.

[237] Société Chaud Colatine, 21 janvier 2011, n° 2010-89 QPC.

[238] Ligue des droits de l'homme, 19 février 2016, n° 2016-535 QPC.

L'instauration de mesures destinées à garantir l'approvisionnement des forces armées suppose, dès lors, que les obligations corrélatives imposées aux professionnels de l'armement soient pleinement justifiées au regard des objectifs poursuivis par la loi et qu'elles apparaissent proportionnées par rapport aux catégories d'entreprises concernées et à leur activité réelle.

1.2.3. Les dérogations à la liberté contractuelle doivent être justifiées par des motifs d'intérêt général.

Le Conseil constitutionnel considère, selon une jurisprudence constante, qu'il « *est loisible au législateur d'apporter à la liberté contractuelle, qui découle de l'article 4 de la Déclaration de 1789, des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi. Par ailleurs, le législateur ne saurait porter aux contrats légalement conclus une atteinte qui ne soit justifiée par un motif d'intérêt général suffisant sans méconnaître les exigences résultant des articles 4 et 16 de la Déclaration de 1789* »[239].

En l'espèce, s'agissant de l'existence d'un tel motif d'intérêt général, le juge constitutionnel a notamment retenu qu'en conférant au Haut conseil de stabilité financière la faculté de limiter temporairement le paiement des valeurs de rachat d'un contrat d'assurance-vie, « *le législateur a entendu permettre la prévention de risques représentant une menace grave et caractérisée soit pour la stabilité du système financier, soit pour la situation financière de l'ensemble ou d'un sous-ensemble significatif des organismes du secteur de l'assurance* » et que, « *ce faisant, le législateur a poursuivi un but d'intérêt général* ».

Il en ressort que le législateur est notamment fondé à reporter temporairement les effets de contrats afin de prévenir la survenance de risques représentant une menace grave et caractérisée soit pour la continuité d'un secteur d'activités donné, soit pour la situation particulière d'un sous-ensemble significatif d'entités de ce secteur. La garantie de l'approvisionnement des forces armées paraît, en ce sens, constituer un motif d'intérêt général suffisant pour justifier une atteinte à la liberté contractuelle.

1.2.4. Des limitations peuvent être apportées à l'exercice du droit de propriété, sous réserve d'être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi.

Alors que l'article 2 de la Déclaration de 1789 consacre la propriété au nombre des « *droits naturels et imprescriptibles de l'homme* », l'article 17 de ce même texte proclame que « *la propriété étant un droit inviolable et sacré, nul ne peut en être privé si ce n'est lorsque la nécessité publique, légalement constatée, l'exige évidemment, et sous la condition d'une juste et préalable indemnité* ».

[239] Loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, 8 décembre 2016, n° 2016-741 DC.

Or, à l'occasion de l'examen d'une disposition prévoyant que le propriétaire d'un mur séparatif peut être tenu de le rendre mitoyen en tout ou partie à la demande du propriétaire du fonds qui le joint, le Conseil constitutionnel a jugé qu'elle n'entrait pas dans le champ d'application de l'article 17 de la Déclaration de 1789 dans la mesure où le « *maître du mur* […]*, dans les limites de l'usage en commun fixées par les articles 653 et suivants du code civil, continue à exercer sur son bien tous les attributs du droit de propriété* »[240].

Selon un raisonnement similaire, il a retenu qu'une disposition permettant à l'autorité administrative de subordonner la délivrance d'un permis de construire ou l'absence d'opposition à une déclaration de travaux à l'institution d'une servitude interdisant ou limitant l'usage, en période hivernale, des chalets d'alpage ou des bâtiments d'estive non desservis par des voies et réseaux « *n'entraîne pas une privation de propriété au sens de l'article 17 de la Déclaration de 1789 mais une limitation à l'exercice du droit de propriété* »[241]. Il en va de même de servitudes tendant à l'établissement à demeure de canalisations souterraines ou de supports pour conducteurs aériens sur des terrains privés non bâtis non clôturés[242].

Il en est ainsi notamment de dispositions autorisant les agents des impôts à procéder à des tests de contrôle des procédures de traitement automatisé de la comptabilité d'une entreprise « *sans prévoir une indemnisation pour privation temporaire de jouissance du matériel de l'entreprise* », étant précisé qu' « *aucune règle constitutionnelle n'impose l'indemnisation des sujétions subies par une entreprise du fait du contrôle fiscal* »[243].

En outre, à l'instar de sa jurisprudence susmentionnée relative aux atteintes à la liberté d'entreprendre et à la liberté contractuelle, le Conseil constitutionnel considère qu'« *en l'absence de privation du droit de propriété, il résulte néanmoins de l'article 2 de la Déclaration de 1789 que les limites apportées à son exercice doivent être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi* »[244].

S'agissant de l'appréciation de la proportionnalité d'une telle mesure, le juge constitutionnel a, par exemple, jugé que cette condition était satisfaite dès lors que le législateur avait circonscrit son périmètre d'application, que la décision correspondante était « *placée sous le contrôle du juge administratif* » et que « *Le propriétaire du bien objet de la servitude dispose de la faculté, au regard des changements de circonstances, d'en demander l'abrogation à l'autorité administrative à tout moment* »[245].

Il paraît dès lors possible d'imposer aux entreprises contribuant à l'approvisionnement des forces armées des limitations à l'exercice du droit de propriété qu'elles détiennent sur les biens nécessaires à l'exercice de cette activité, sans pour autant les assortir d'un mécanisme

[240] M. Pierre B., 12 novembre 2010, n° 2010-60 QPC.

[241] Société civile Groupement foncier rural Namin et Co, 10 mai 2016, n° 2016-540 QPC.

[242] Association Avenir Haute Durance et autres, 2 février 2016, n° 2015-518 QPC.

[243] Loi de finances pour 1982, 30 décembre 1981, n° 81-133 DC.

[244] Mme Barbara D. et autres, 8 avril 2011, n° 2011-118 QPC.

[245] *Cf.* décision n° 2016-540 QPC susmentionnée.

d'indemnisation, sous réserve qu'elles soient justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi.

1.2.5. Des obligations peuvent être mises à la charge d'opérateurs privés sans créer de rupture d'égalité devant les charges publiques, sous réserve d'être rattachables aux activités desdits opérateurs.

Selon l'article 13 de la Déclaration de 1789 « *Pour l'entretien de la force publique, et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens, en raison de leurs facultés* ». Le Conseil constitutionnel considère que si cet article « *n'interdit pas de faire supporter, pour un motif d'intérêt général, à certaines catégories de personnes des charges particulières, il ne doit pas en résulter de rupture caractérisée de l'égalité devant les charges publiques* »[246].

En pratique, le juge constitutionnel vérifie si, à travers la différence de traitement ainsi instituée, le législateur « *n'a pas reporté sur des personnes privées des dépenses qui, par leur nature, incomberaient à l'Etat* ». Tel fut le cas pour les dispositions de l'article L. 34-11 du code des postes et des communications électroniques soumettant à autorisation préalable l'exploitation de certains équipements de réseaux radioélectriques mobiles (5G) pour vérifier l'absence de risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale : si la mise en œuvre de ces dispositions est susceptible d'entraîner des charges pour les opérateurs, il n'en résulte pas de rupture caractérisée de l'égalité devant les charges publiques, la sécurisation des réseaux de communication mobile étant « *directement liée aux activités des opérateurs qui utilisent et exploitent ces réseaux afin d'offrir au public des services de communications électroniques* »[247].

De manière plus souple, le Conseil constitutionnel a considéré que des dispositions imposant aux fabricants et importateurs de produits du tabac, d'une part, d'imprimer ou d'apposer sur les unités de conditionnement de ces produits un dispositif de sécurité infalsifiable et, d'autre part, de fournir gratuitement les équipements nécessaires à la détection de ces éléments aux agents des administrations chargées de les contrôler, « *le législateur a entendu garantir l'authenticité des produits du tabac mis sur le marché pour lutter contre leur commerce illicite* », étant précisé que « *la lutte contre le commerce illicite des produits du tabac n'est pas sans lien avec les activités des entreprises qui les fabriquent ou les importent, qui ont au demeurant un intérêt à la mise en œuvre de la mission de contrôle, par l'Etat, des dispositifs de sécurité apposés sur les unités de conditionnement de ces produits* »[248].

A contrario, il a été jugé que « *s'il est loisible au législateur, dans le respect des libertés constitutionnellement garanties, d'imposer aux opérateurs de réseaux de télécommunications*

[246] Loi portant diverses dispositions d'adaptation au droit communautaire dans le domaine des transports, 10 janvier 2001, n° 2000-440 DC.

[247] Société Bouygues télécom et autre, 5 février 2021, n° 2020-882 QPC.

[248] Société nationale d'exploitation industrielle des tabacs et allumettes, 24 janvier 2020, n° 2019-821 QPC.

de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population, est étranger à l'exploitation des réseaux de télécommunications » et « *que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs* »[249].

En conséquence, ne sauraient être mises à la charge des entreprises concourant à l'approvisionnement des forces armées, sans compensation des dépenses induites, que des obligations susceptibles d'être directement rattachées à leurs activités et qui n'auraient, par leur nature, pas nécessairement vocation à relever de la compétence de l'Etat.

1.2.6. L'application du principe de responsabilité ne fait pas obstacle à l'instauration de conditions particulières de mise en œuvre de cette responsabilité

Le Conseil constitutionnel considère, selon une jurisprudence constante, qu'« *il résulte de la liberté proclamée par l'article 4 de la Déclaration de 1789 qu'en principe, tout fait quelconque de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer. La faculté d'agir en responsabilité met en œuvre cette exigence constitutionnelle. Toutefois, cette dernière ne fait pas obstacle à ce que le législateur aménage, pour un motif d'intérêt général, les conditions dans lesquelles la responsabilité peut être engagée. Il peut ainsi, pour un tel motif, apporter à ce principe des exclusions ou des limitations à condition qu'il n'en résulte une atteinte disproportionnée ni aux droits des victimes d'actes fautifs ni au droit à un recours juridictionnel effectif qui découle de l'article 16 de la Déclaration de 1789* »[250].

En ce sens, le législateur apparaît fondé à assortir la faculté, pour des entreprises, de solliciter l'indemnisation des préjudices causés par les décisions de l'administration d'une procédure permettant de vérifier la réalité et l'étendue des préjudices allégués.

A cet égard, le Conseil constitutionnel a notamment jugé que des dispositions conférant à l'autorité préfectorale la faculté de diligenter une enquête administrative préalablement à l'exercice d'un droit de propriété par des particuliers ne méconnaissait pas les droits et libertés que ces derniers tiennent de la Constitution dès lors que « *ni par leur objet, ni par leur libellé, le dispositions* [en cause] *n'excluent la mise en jeu de la responsabilité de la puissance publique au cas où une décision légalement prise sur leur fondement causerait un préjudice indemnisable* »[251].

---

[249] Loi de finances rectificative pour 2000, 28 décembre 2000, n° 2000-441 DC.

[250] 2010-2 QPC, 11 juin 2010, cons. 11 ; 2010-8 QPC, 18 juin 2010, cons. 10 ; 2011-116 QPC, 8 avril 2011, cons. 4 ; 2011-127 QPC, 6 mai 2011, cons. 7 ; 2011-167 QPC, 23 septembre 2011, cons. 4 ; 2014-415 QPC, 26 septembre 2014, cons. 5.

[251] Loi complémentaire à la loi n° 88-1202 du 30 décembre 1988 relative à l'adaptation de l'exploitation agricole à son environnement économique et social, 22 janvier 1990, n° 89-267 DC.

Ce faisant, tout mécanisme de vérification préalable mis en œuvre par l'administration apparaît fondé dès lors qu'il demeure soumis au contrôle du juge.

1.2.7. Tout manquement à des mesures ordonnées par l'autorité administrative, diligentées dans le cadre de prérogatives de puissance publique, est susceptible de donner lieu à des sanctions administratives.

Il ressort de la jurisprudence constitutionnelle que « *le principe de la séparation des pouvoirs, non plus qu'aucun principe ou règle de valeur constitutionnelle ne fait obstacle à ce qu'une autorité administrative, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction dès lors, d'une part, que la sanction susceptible d'être infligée est exclusive de toute privation de liberté et, d'autre part, que l'exercice du pouvoir de sanction est assorti par la loi de mesures destinées à sauvegarder les droits et libertés constitutionnellement garantis* »[252].

Au titre de ces droits et libertés constitutionnellement garantis, il est possible de distinguer des exigences procédurales comme des exigences de fond.

1.2.7.1. *Les droits de la défense doivent être pris en compte préalablement au prononcé de sanctions et s'imposent sans que le législateur n'ait à en rappeler l'existence.*

Le respect des droits de la défense, initialement consacré comme principe général du droit[253], puis comme principe fondamental reconnu par les lois de la République[254], constitue à présent une exigence à valeur constitutionnelle rattachée à l'article 16 de la Déclaration des droits de l'Homme et du citoyen de 1789[255].

Ce principe ne concerne pas seulement les peines prononcées par le juge pénal, mais s'applique à toute sanction ayant le caractère d'une punition, y compris si le législateur a laissé le soin de la prononcer à une autorité de nature non judiciaire[256]. Il implique « *qu'aucune sanction ayant le caractère d'une punition ne puisse être infligée à une personne sans que celle-ci ait été mise à même de présenter ses observations sur les faits qui lui sont reprochés* » et « *s'impose aux autorités disposant d'un pouvoir de sanction sans qu'il soit besoin pour le législateur d'en rappeler l'existence* »[257].

[252] Loi relative à la sécurité et à la transparence du marché financier, 28 juillet 1999, n° 89-260 DC.

[253] CE, 5 mai 1944, Dame Veuve Trompier-Gravier, Rec. p. 133.

[254] Loi relative au développement de la prévention des accidents du travail, 2 décembre 1976, n° 76-70 DC.

[255] Loi pour l'égalité des chances, 30 mars 2006, n° 2006-535 DC.

[256] Loi relative à la liberté de communication, 17 janvier 1989, n° 88-248 DC.

[257] M. Stéphane R. et autres, 24 octobre 2014, n° 2014-423 QPC.

1.2.7.2. *L'impartialité objective et l'indépendance des tribunaux ne sont pas opposables aux sanctions prises par une autorité soumise au pouvoir hiérarchique du ministre.*

La portée de ces principes a été singulièrement étendue sous l'influence de l'article 6§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH)[258], qui implique d'aller au-delà de l'impartialité subjective tenant à l'homme et à son comportement, mais de bien veiller à l'impartialité objective tenant aux fonctions exercées qui sont de nature, indépendamment de ses convictions personnelles, à faire douter de l'indépendance de celui qui les tient[259].

Néanmoins, le respect de ces principes s'impose lorsque la sanction est prononcée par une autorité administrative non soumise au pouvoir hiérarchique du ministre[260].

Le respect de l'impartialité objective et de l'indépendance ne s'impose pas aux autorités administratives placées sous la responsabilité d'un ministre en ce qu'elles ne sauraient être assimilées à un « tribunal » au sens de l'article 6§1 (voir, en ce sens, CE, 27 mars 2000, n°187703 à propos des pénalités fiscales ; CE, 21 décembre 2018, n°424520, à propos des sanctions prononcées par l'ANAH).

1.2.7.3. *Le principe de légalité des délits et des peines, qui s'applique aux sanctions administratives, implique de préciser les obligations auxquelles est soumise une personne.*

En matière de sanctions administratives, le Conseil constitutionnel juge « *qu'appliquée en dehors du droit pénal, l'exigence d'une définition des infractions sanctionnées se trouve satisfaite, en matière administrative, par la référence aux obligations auxquelles le titulaire d'une autorisation administrative est soumis en vertu des lois et règlements* »[261].

Dans sa décision n° 255136 du 7 juillet 2004, le Conseil d'Etat a précisé que « *lorsqu'il est appliqué aux sanctions administratives, le principe de légalité des délits et des peines ne fait pas obstacle à ce que les infractions soient définies par référence aux obligations auxquelles est soumise une personne en raison de l'activité qu'elle exerce, de la profession à laquelle elle appartient ou de l'institution dont elle relève ; il implique, en revanche, que les sanctions soient prévues et énumérées par un texte* ».

[258] L'article 6§1 de la CESDH pose le principe d'impartialité et d'indépendance des tribunaux en ces termes : « *Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle* ».

[259] CE, 4 juillet 2003, n° 234353.

[260] Société Numéricâble SAS et autre, 5 juillet 2013, n° 2013-331 QPC ; Société Barnes et autre, 9 mars 2017, n° 2016-616/617 QPC.

[261] Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, 17 janvier 1989, n° 88-248 DC.

1.2.7.4. *Les sanctions sont soumises aux principes d'individualisation et de proportionnalité des peines.*

Aux termes de l'article 8 de la Déclaration de 1789, « *La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée* ». Or, il ressort de la jurisprudence constitutionnelle que « *les principes énoncés par l'article 8 de la Déclaration de 1789 ne concernent pas seulement les peines prononcées par les juridictions pénales mais s'étendent à toute sanction ayant le caractère d'une punition* », étant précisé que « *si la nécessité des peines attachées aux infractions relève du pouvoir d'appréciation du législateur, il incombe au Conseil constitutionnel de s'assurer, en matière disciplinaire, de l'absence d'inadéquation manifeste entre les peines disciplinaires encourues et les obligations dont elles tendent à réprimer la méconnaissance* »[262].

A titre d'exemple, le Conseil constitutionnel a reconnu la constitutionnalité d'un dispositif conférant à l'autorité administrative, « *sous le contrôle du juge, le soin de fixer le montant de la sanction pécuniaire, dans la limite du maximum déterminé par les dispositions contestées, et de proportionner cette sanction à la gravité des faits reprochés, à l'importance du dommage causé à l'économie, à la situation de l'entreprise sanctionnée ou du groupe auquel elle appartient et à l'éventuelle réitération de pratiques prohibées* »[263].

1.3. CADRE CONVENTIONNEL

Si la jurisprudence de la Cour européenne des droits de l'homme (CEDH) et celle de la Cour de justice de l'Union européenne (CJUE) confirme les grands principes de la jurisprudence constitutionnelle détaillée au 1.2 *supra*, il peut être souligné que toute mesure imposée aux entreprises assurant l'approvisionnement des forces armées pourrait avoir un impact sur certains droits et libertés protégés par le droit de l'Union européenne, notamment sur les règles relatives au bon fonctionnement du marché intérieur.

De telles mesures seraient, en effet, susceptibles de porter atteinte à l'interdiction des restrictions quantitatives à l'importation ou à l'exportation entre les Etats membres, respectivement prévues aux articles 34 et 35 du Traité sur le fonctionnement de l'Union européenne (TFUE) ainsi qu'à l'interdiction des restrictions à la liberté d'établissement, prévues à l'article 49 de ce texte.

Toutefois, les articles 36 et 52 du TFUE autorisent notamment les Etats membres à adopter des dispositions législatives, réglementaires et administratives instituant de telles restrictions lorsqu'elles sont justifiées par des raisons d'ordre public, de sécurité publique et de santé publique.

[262] M. Michel G., 25 novembre 2011, n° 2011-199 QPC.

[263] Société Grands Moulins de Strasbourg SA et autre, 14 octobre 2015, n° 2015-489 QPC.

En outre, il apparaît que la sécurité publique peut être invoquée tant pour des raisons de sécurité intérieure que de sécurité extérieure. C'est à chaque Etat membre qu'il revient de démontrer que les mesures qu'il impose sont justifiées. Dans l'arrêt n° 72/83 du 10 juillet 1984, *Campus Oil,* la CJUE a ainsi validé une mesure nationale dérogeant à l'article 34 du TFUE pour des raisons de sécurité publique, qui imposait aux importateurs de pétrole de s'approvisionner, à concurrence de 35 % de leurs besoins, auprès d'une compagnie pétrolière nationale, en respectant des prix fixés par le gouvernement.

Plus particulièrement, le *b* du paragraphe 1 de l'article 346 du TFUE autorise tout Etat membre à « *prendre les mesures qu'il estime nécessaires à la protection des intérêts essentiels de sa sécurité et qui se rapportent à la production ou au commerce* » des produits figurant sur une liste fixée par le Conseil[264], mentionnée au paragraphe 2 du même article. Ainsi que le précise le considérant 10 de la directive 2009/81/CE du Parlement européen et du Conseil du 13 juillet 2009[265], « *cette liste ne comprend que les équipements qui sont conçus, développés et produits à des fins spécifiquement militaires* », étant souligné qu'elle « *est générique et est à interpréter au sens large à la lumière du caractère évolutif des technologies, des politiques d'acquisition et des besoins militaires conduisant au développement de nouveaux types d'équipements* ».

1.4. ÉLEMENTS DE DROIT COMPARE

Le droit américain prévoit, *via* le dispositif « *Defense Priorities and Allocations System Program* » (DPAS), un mécanisme de priorisation des contrats et commandes notamment applicable à la défense nationale, à l'énergie et à la sécurité intérieure. Ce dispositif, dont la mise en œuvre n'est pas limitée aux crises et aux conflits armés, peut également être utilisé pour venir en aide à un autre Etat. Son objectif principal est de garantir, en temps voulu, la disponibilité des ressources industrielles pour répondre aux exigences de la défense nationale et de la préparation aux situations d'urgence.

Le DPAS fait l'objet du paragraphe 700.1 du titre 15 du « *Code of Federal Regulations* » et découle du « *Defense Production Act* » de 1950 (Sec. 101). L'habilitation donnée par le Congrès d'y recourir pour une durée limitée a été renouvelée plus de 50 fois depuis 1950.

Sur le fondement de cette habilitation, le Président des Etats-Unis peut exiger l'acceptation et l'exécution préférentielles des contrats ou des commandes ainsi que l'allocation des matériaux, des services et des installations nécessaires à leur mise en œuvre, afin de soutenir certains programmes concernant la défense nationale ou l'énergie. Le Département du Commerce bénéficie, par le biais d'un décret présidentiel (*The National Defense Resources Preparedness*

[264] Liste fixée par la décision n° 255/58 du Conseil du 15 avril 1958, qui n'a été publiée au Journal officiel des Communautés européennes que le 27 septembre 2001, à l'occasion de la réponse apportée à la question écrite E-1324/01 posée par le député européen Bart Staes.

[265] Directive 2009/81/CE du Parlement européen et du Conseil du 13 juillet 2009 relative à la coordination des procédures de passation de certains marchés de travaux, de fournitures et de services par des pouvoirs adjudicateurs ou entités adjudicatrices dans les domaines de la défense et de la sécurité.

Executive Order, E.O. 13603), d'une délégation pour mettre en œuvre les décisions correspondantes. A cet égard, il lui appartient notamment d'autoriser le Département de la Défense à prioriser les contrats ou commandes concernées.

Il existe deux niveaux de priorisation : d'une part, les contrats « DO », qui sont prioritaires sur les contrats « de droit commun », et, d'autre part, les contrats « DX », qui sont prioritaires sur les contrats « DO ». D'un point de vue formel, tous ces actes comprennent le degré de priorisation, une date de livraison requise, une signature et une déclaration signalant l'applicabilité des procédures DPAS.

Les entreprises américaines concernées par ces contrats et commandes priorisés sont légalement tenues de leur accorder un traitement prioritaire et de respecter, le cas échéant, le calendrier imposé par l'administration. Il existe un nombre très limité de cas où le rejet d'une commande priorisée est possible : soit lorsque la commande est impossible à exécuter à la date demandée (dans ce cas, la commande doit être rejetée, mais une date de livraison ultérieure doit nécessairement être proposée), soit lorsque la commande ou le service demandé n'est pas ou n'est plus fourni par l'entreprise sollicitée.

Ces priorisations sont fréquemment utilisées par le Département de la Défense américain, étant précisé que le département du Commerce estime qu'environ 300 000 de ces contrats sont conclus chaque année.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les conséquences de la guerre en Ukraine et la désorganisation des chaînes logistiques consécutive à la crise sanitaire provoquent actuellement des difficultés d'approvisionnement de certains composants ou matières premières d'intérêt stratégique. A cet égard, parmi les documents relatifs à la loi de finances pour 2023, le projet annuel de performance relatif au programme 146 présente notamment « *la pénurie mondiale de composants et l'allongement de la durée d'approvisionnement de la chaîne de production* » comme les causes du retard de certains programmes d'armement majeurs. De telles difficultés seraient nécessairement démultipliées dans l'hypothèse d'un engagement majeur de la France contre un compétiteur stratégique, obérant ainsi la capacité de la BITD à monter en puissance pour répondre aux besoins en équipements des forces armées. Il apparaît en ce sens nécessaire de s'assurer que la législation nationale confère à ces dernières des garanties suffisantes en termes de sécurisation de leurs approvisionnements.

La Revue nationale stratégique de 2022 traduit cette nécessité en proposant que des « *stocks communs de composants ou de matières premières* [soient] *mis en place à l'initiative et sous la responsabilité de l'industrie pour soutenir les activités industrielles militaires, en cas de conflit* », ajoutant que, « *pour assurer la capacité de ses missions régaliennes, l'Etat doit pouvoir, selon l'évolution de la conflictualité, imposer des priorités* ». En effet, depuis la fin de

la guerre froide, l'industrie de défense fonctionne selon une logique de flux, permettant aux entreprises concernées d'optimiser leurs marges. Or, un tel mode de fonctionnement obère les capacités de résilience et de réactivité de l'outil national de production et n'apparaît, dès lors, pas compatible avec les exigences portées par une « *économie de guerre* », c'est-à-dire une économie articulant ses politiques et ses choix autour du soutien de l'effort de défense afin de permettre à l'industrie française de soutenir cet effort de guerre dans la durée, en cas de nécessité pour les forces armées ou au profit d'un partenaire. Dans un tel contexte, il convient désormais de passer à une logique de stocks, dont le bon dimensionnement dépend des cadences de production des industriels. A cet égard, si l'existence d'un stock initial est toujours nécessaire pour les premières phases d'un conflit, l'un des enjeux stratégiques pour la suite de celui-ci est la capacité des industriels à assurer la reconstitution dudit stock le plus rapidement possible.

Indépendamment du cadre de la relation contractuelle, la législation en vigueur ne comporte aucun dispositif permettant, d'une part, d'imposer aux entreprises de la BITD la constitution de stocks de matières ou de composants d'intérêt stratégique et, d'autre part, de leur ordonner l'exécution prioritaire des commandes passées par l'Etat dans le cadre d'un marché de défense et de sécurité. Sur ce dernier point, il peut être souligné que le pouvoir de modification unilatérale des contrats dont bénéficient les personnes publiques au titre du code de la commande publique et des principes dégagés par la jurisprudence administrative, en vertu des règles générales applicables aux contrats administratifs, ne sont pas nécessairement adaptés à l'objectif d'accélération des délais d'acquisition de la prestation ou du matériel commandé dans la mesure où cette faculté ne trouve pas à s'appliquer, d'une part, si ladite accélération apparaît de nature à bouleverser l'économie générale du contrat et, d'autre part, dans certaines des hypothèses envisagées (*cf.* situations mentionnées ci-dessous, au sein du §2 de l'item 2.2, renvoyant, d'une part, aux contrats conclus par des organisations internationales ou par des Etats partenaires et, d'autre part, aux prestations réalisées par des sous-traitants d'un co-contractant de l'Etat).

Compte tenu des sujétions qui résulteraient de l'instauration de telles mesures à la charge des industriels, celles-ci ne pourraient, en outre, être prévues que dans le cadre d'un dispositif législatif, assorti de toutes les garanties requises au titre de la jurisprudence constitutionnelle et européenne.

2.2. OBJECTIFS POURSUIVIS

Afin de répondre aux difficultés identifiées au paragraphe qui précède, la présente mesure est destinée à sécuriser l'approvisionnement des forces armées :

- d'une part, à titre préventif, en garantissant la disponibilité des ressources nécessaires à la fabrication des équipements militaires ;
- d'autre part, en accélérant la livraison des matériels de guerre déjà commandés, lorsque les circonstances l'exigent.

Pour répondre à ce double objectif, deux dispositifs complémentaires sont ainsi envisagés :

1/ Tout d'abord, l'Etat doit avoir la faculté d'exiger, de la part de certaines entreprises occupant un rôle déterminant dans l'approvisionnement des forces armées, qu'elles disposent de stocks adéquats afin de leur permettre d'honorer les commandes passées auprès d'elles conformément aux délais d'exécution contractuellement définis, d'augmenter leur réactivité et de préparer les futures commandes, y compris dans un contexte de pénurie. Or, même si le ministère des armées s'emploie à obtenir de la part des entreprises de la BITD qu'elles constituent de tels stocks de manière volontaire et coordonnée, dans un cadre contractuel, il apparaît nécessaire de disposer de mesures adaptées destinées à garantir la satisfaction de l'ensemble des besoins de la défense nationale, en conférant à l'autorité administrative le soin de déterminer la nature et le volume desdits stocks.

A cet égard, il convient de distinguer deux types de stocks, qui répondent à des objets distincts et qui n'impliquent pas les mêmes exigences de mise en œuvre.

En premier lieu, la nécessité de conserver des stocks peut porter sur des matières premières ou sur des composants critiques génériques, généralement nécessaires à l'ensemble des industries de défense d'un même secteur, tels que le titane ou d'autres métaux critiques. Ce faisant, il paraît notamment envisageable pour les entreprises concernées de mutualiser la constitution de tels stocks.

En second lieu, la constitution de stocks peut s'avérer nécessaire pour des composants de base ou des produits semi-finis spécifiques à certains équipements militaires, dont la disponibilité immédiate apparaît susceptible de permettre à l'industriel d'augmenter sa cadence de production de façon significative. Tel est par exemple le cas des tubes de canons *Caesar*, qui représentent une faible proportion du coût total de production, mais une part importante dans le délai global de production de ce système d'armes. L'on peut également citer les miroirs entrant dans la fabrication des systèmes optroniques.

2/ Par ailleurs, dans un secteur de l'armement qui apparaît de plus en plus concurrentiel, la disponibilité des matières ou des composants d'intérêt stratégique ne constitue pas, à elle seule, une garantie suffisante pour l'approvisionnement des forces armées. En effet, au-delà du calendrier des commandes fixé par voie contractuelle, l'Etat doit être en mesure, lorsque les circonstances l'exigent :

- de contraindre tout industriel avec lequel il a conclu un marché de défense et de sécurité à exécuter ce marché par priorité sur tout autre engagement contractuel le liant à un tiers ;
- et, le cas échéant, d'ordonner un délai de livraison raccourci par rapport au calendrier initialement prévu au contrat.

Au-delà des seuls besoins des forces armées françaises, il doit, en outre, pouvoir mobiliser cette faculté de priorisation pour honorer ses engagements internationaux, pour assurer la poursuite de coopérations internationales en matière militaire ainsi que pour exécuter les contrats conclus par des organisations internationales auxquelles il est partie ou par des Etats partenaires.

A cet égard, il peut être souligné que 30 à 70 % du processus de production des équipements militaires, selon les programmes d'armement considérés, est effectué par des sous-traitants, qui occupent une place capitale dans le processus de production, notamment en amont de la chaîne de fabrication, le maître d'œuvre assurant souvent un rôle d'intégrateur. A titre d'exemple, sur les deux ans de fabrication des radars qui équipent le *Rafale*, la première année de production est entièrement effectuée chez les sous-traitants de *Thales*. Pour augmenter la cadence de production, il convient donc d'étendre le périmètre d'application de la faculté de priorisation ouverte à l'Etat à l'ensemble de la chaîne de production qu'il est nécessaire de mobiliser, en incluant les sous-contractants de tout niveau dont la participation est indispensable à l'exécution des contrats en cause.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Il a été envisagé de simplement recourir à des mécanismes contractuels pour garantir les conditions d'approvisionnement des forces armées en matériel militaire, étant rappelé que l'administration dispose toujours de la faculté de recourir au régime des réquisitions lorsqu'une mesure de contrainte s'avère nécessaire. Cependant, il est apparu qu'une telle option ne permettrait pas de répondre de manière satisfaisante à l'ensemble des problématiques en cause et qu'il serait préférable d'aménager un dispositif intermédiaire.

En premier lieu, même si le ministère des armées s'emploie à obtenir, de la part des industriels de la BITD avec lesquels il est contractuellement lié, qu'ils constituent, de manière volontaire et coordonnée, des stocks de matières et de composants nécessaires à l'équipement des forces armées, il peut, en pratique, s'avérer difficile d'obtenir des engagements fermes en la matière, surtout dans un contexte de hausse des prix.

En outre, alors que le volume et la nature du stock à constituer peuvent évoluer en fonction de facteurs conjoncturels, les conditions de révision d'une clause contractuelle prévue à cette fin ne sont pas nécessairement compatibles avec la nécessité de l'adapter rapidement à de nouveaux besoins, sachant que, le cas échéant, une telle évolution du contrat peut être assortie d'une lourde contrepartie financière. Or, ce surcoût assumé par l'Etat apparaît d'autant moins approprié que la constitution d'un tel stock, qui s'apparente à un fonds de roulement, est directement liée aux activités des professionnels du secteur et qu'elle contribue nécessairement à la satisfaction de leurs propres intérêts.

En deuxième lieu, toute mesure tendant à la priorisation des commandes passées par l'Etat ou par ses alliés stratégiques apparaît difficilement conciliable avec l'obtention préalable du consentement des industriels du secteur, particulièrement pour les entreprises duales dont la clientèle est, par définition, plus diversifiée. En effet, toute clause instituant un mécanisme de livraison prioritaire pourrait être perçue comme un handicap dans un secteur très concurrentiel.

De plus, la simple voie contractuelle apparaît insuffisante pour sécuriser l'ensemble de la chaîne de production des équipements militaires, qui comprend non seulement l'industriel titulaire du marché, mais également ses sous-traitants, qui n'ont pas nécessairement de lien avec l'Etat.

En troisième et dernier lieu, qu'il s'agisse de la constitution de stocks ou de la priorisation des commandes, la problématique de sécurisation des approvisionnements des forces armées s'inscrit dans une démarche d'anticipation des difficultés qui ne correspond pas nécessairement aux critères de mise en œuvre du régime des réquisitions de défense, tel que modifié par le présent projet de loi, qui ne peuvent être mobilisé qu'en cas de menace actuelle ou prévisible ou en cas d'urgence. Il paraît dès lors nécessaire de disposer d'un dispositif plus souple, permettant d'intervenir en amont, lorsque la voie contractuelle s'avère inadaptée.

3.2. OPTION RETENUE

Afin de répondre aux objectifs définis au sein de l'item 2.2 *supra*, la présente mesure dote l'Etat de deux nouveaux outils susceptibles d'être appliqués unilatéralement afin de compléter les dispositifs qu'il peut mettre en place par voie contractuelle, lesquels n'offrent pas toutes les garanties suffisantes pour prévenir le défaut d'approvisionnement des forces armées en matériels militaires.

En premier lieu, il est prévu de conférer à l'autorité administrative la faculté d'ordonner aux industriels de la BITD la constitution d'un stock minimal de matières ou de composants d'intérêt stratégique, à l'instar de divers mécanismes d'ores et déjà applicables en droit interne.

A cet égard, il peut être rappelé que les articles L. 642-2 et suivants du code de l'énergie imposent à tout opérateur pétrolier agréé réalisant, en France métropolitaine, une opération entraînant l'exigibilité des taxes intérieures de consommation ou, dans un département d'outre-mer, mettant à la consommation certains produits pétroliers ou qui procède à l'avitaillement des aéronefs, de contribuer à la constitution de « *stocks stratégiques* » pétroliers, définis proportionnellement aux quantités faisant l'objet des opérations en cause, de telle sorte que la France dispose, en permanence, d'un quart des quantités importées ou introduites l'année civile précédente. De même, l'article L. 5121-29 du code de la santé publique impose à tout titulaire d'autorisation de mise sur le marché et à toute entreprise pharmaceutique exploitant un médicament de constituer un « *stock de sécurité* » pour les médicaments destinés au marché français, dans une limite qui ne peut excéder quatre mois de couverture des besoins en médicament, calculés sur la base du volume des ventes de la spécialité au cours des douze derniers mois glissants de stock pour tous les médicaments. Il peut, en outre, être souligné qu'aucun de ces deux dispositifs n'est assorti d'un mécanisme d'indemnisation par l'Etat des stocks ainsi constitués par les opérateurs privés concernés.

L'obligation instituée par la présente mesure ne peut néanmoins être imposée qu'aux entreprises titulaires d'une autorisation de fabrication et de commerce de matériels de guerre, d'armes, de munitions ou de leurs éléments des catégories A et B, délivrée sur le fondement de l'article L. 2332-1 du code de la défense. En effet, compte tenu des besoins en équipements militaires

des forces armées, il ne semble pas nécessaire d'étendre cette possibilité à l'ensemble des entreprises du secteur.

Concrètement, cette obligation pourra leur être imposée par arrêté du ministre des armées, indépendamment de tout contrat en cours, dans l'objectif d'augmenter leur réactivité et de préparer les futures commandes émanant des forces armées, tout en comprimant autant que possible les délais entre ces commandes et la livraison effective des matériels en cause. Si le dispositif prévoit que les stocks pourront être mutualisés par convention passée entre les différentes entreprises concernées, ces dernières ne pourront, en revanche, les utiliser sans autorisation de l'autorité administrative. Elles ne pourront pas plus prétendre à l'indemnisation des coûts de constitution et d'immobilisation desdits stocks, dès lors que ceux-ci concourent à la réalisation de leur activité professionnelle, à l'instar du régime applicable pour les stocks stratégiques d'hydrocarbures ou de médicaments.

En contrepartie des sujétions ainsi imposées aux industriels, ce mécanisme est assorti de garanties importantes :

- la valeur maximale du stock prescrit sera plafonnée par voie réglementaire, afin que la constitution et l'entretien du stock restent des charges modérées pour les entreprises ;
- la valeur maximale et le volume du stock prescrit devront être proportionnés et prendre en compte, au cas par cas, la situation particulière de l'entreprise (compte tenu de son volume d'activité, de la nature des matériels vendus et de l'état des commandes en cours), le degré de tension constaté pour l'approvisionnement des matériels et composants concernés ainsi que les besoins prévisibles des forces armées.

Cette dernière exigence de proportionnalité impliquera, en outre, de la part de l'Etat, une révision périodique des sujétions ainsi imposées par voie d'arrêté. A cet égard, compte tenu des délais de production des équipements militaires, il ne paraît toutefois pas nécessaire de s'inscrire dans une logique de court terme, étant précisé qu'une actualisation intervenant environ tous les deux ans devrait permettre aux entreprises concernées de s'organiser pour constituer et gérer ce stock.

La constitution d'un tel stock s'accompagne également de l'obligation, pour l'entreprise, de communiquer au ministère de la défense les éléments strictement nécessaires au contrôle du respect de cette obligation, dont la violation est assortie de sanctions. En cas de manquement, l'autorité administrative dispose ainsi de la faculté, après une mise en demeure non suivie d'effet, de lui infliger une sanction pécuniaire dont le montant ne peut excéder le double de la valeur des stocks non constitué, dans la limite de 5 % du chiffre d'affaires annuel constaté au cours des deux exercices précédents. Il s'agit, en effet, de garantir que l'entreprise s'acquittera de ses obligations en la matière, sans pour autant mettre en péril son équilibre financier. Cependant, en cas de récidive, elle peut se voir retirer l'autorisation de fabrication et de commerce dont elle est titulaire, à l'instar de ce que prévoit l'article L. 2332-11 du code de la défense, pour « *tout individu ayant commis un manquement aux dispositions* » de ce code relatives à la fabrication et au commerce d'armes et de matériels de guerre ou aux dispositions réglementaires y afférentes.

En second lieu, sur le modèle de la législation américaine présentée au sein de la rubrique 1.4, il est prévu de conférer à l'autorité administrative, pour l'exécution d'un marché de défense ou de sécurité qu'elle a passé avec un industriel de la BITD, la faculté, par arrêté, de :

- contraindre l'industriel concerné à exécuter les obligations qui découlent de ce marché par priorité sur tout autre engagement contractuel le liant à un tiers ;
- et, le cas échéant, fixer unilatéralement un délai de livraison réduit par rapport aux stipulations contractuelles.

Limité au seul périmètre de la défense nationale, le champ d'application de ce dispositif est néanmoins plus large que celui prévu s'agissant de l'obligation de constituer des stocks d'intérêt stratégique dès lors qu'il est susceptible de s'appliquer à l'ensemble des titulaires d'un marché de défense et de sécurité mentionnés à l'article L. 1113-1 du code de la commande publique ainsi qu'aux sous-contractants de tout niveau dont la participation est indispensable à l'exécution de tels marchés. En effet, ces derniers peuvent porter sur des matériels lourds ou complexes, dont la production dépend d'une pluralité d'acteurs.

Ce dispositif concourt à la réduction des délais de livraison des matériels de guerre et vise à garantir la continuité des missions des forces armées, à honorer les engagements internationaux de la France et à rendre prioritaire l'exécution des contrats d'armement passés par une entreprise française avec une organisation internationale ou un Etat tiers.

Afin de respecter les exigences constitutionnelles, il est, en outre, expressément prévu que les mesures ainsi prescrites devront être proportionnées aux objectifs poursuivis et appropriées aux circonstances de temps et de lieu.

En contrepartie, l'Etat sera tenu de compenser intégralement le préjudice matériel résultant de manière directe et certaine des mesures de priorisation. Ainsi, notamment, l'effet potentiel de retard induit sur la livraison des mêmes matériels aux autres clients de l'entreprise concernée sera neutralisé, pour l'entreprise, par la garantie que l'ensemble des pénalités de retard que lui infligeraient ses autres partenaires contractuels ou que les éventuelles condamnations qui pourraient être prononcées à son encontre en cas de mise en cause de sa responsabilité contractuelle seront prises en charge par l'Etat. A seule fin d'évaluer les préjudices subis dans de telles situations, les entreprises devront fournir à l'autorité administrative, si celle-ci en fait la demande, tous documents ou éléments d'information de nature à justifier le montant de l'indemnisation due.

A l'instar du dispositif prévu s'agissant de l'obligation de constitution d'un stock d'intérêt stratégique, l'industriel sera passible, en cas de manquement à l'obligation d'exécution prioritaire et après une mise en demeure demeurée sans effet, d'une sanction pécuniaire dont le montant ne pourra excéder le double de la valeur des prestations ordonnées, dans la limite de 5 % de son chiffre d'affaires annuel moyen constaté au cours des deux exercices précédents.

Ces mesures sont regroupées au sein d'un nouveau chapitre, l'architecture actuelle du code de la défense ne permettant pas l'intégration des dispositions correspondantes au sein d'une subdivision de ce code existante.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

A l'aune des choix explicités au sein de l'item 3.2, la présente mesure crée, au sein du titre III du livre III de la première partie du code de la défense, consacré à la défense économique, un nouveau chapitre relatif « *à la sécurité des approvisionnements des forces armées et des formations rattachées* ». Il comprend trois articles :

- l'article L. 1339-1 nouveau introduit la faculté, pour l'autorité administrative, d'ordonner aux entreprises titulaires d'une autorisation de fabrication et de commerce de matériels de guerre, d'armes, de munitions et de leurs éléments des catégories A et B la constitution d'un stock minimal de matières ou composants d'intérêt stratégique ;
- l'article L. 1339-2 nouveau confère à l'autorité administrative la faculté, d'une part, d'ordonner aux entreprises titulaires d'un marché de défense ou de sécurité ainsi qu'à leurs sous-contractants de réaliser tout ou partie des prestations faisant l'objet du marché par priorité sur tout autre engagement contractuel et, d'autre part, de préciser le délai dans lequel la réalisation des prestations est attendue, en dérogeant le cas échéant aux stipulations contractuelles ;
- l'article L. 1339-3 nouveau renvoie à un décret en Conseil d'Etat le soin de préciser les modalités d'application de ce chapitre.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ des dérogations aux règles du marché intérieur consenties par le TFUE, rappelées au sein de la rubrique 1.3 *supra*.

A cet égard, il convient également de souligner qu'est actuellement en cours d'élaboration un règlement européen portant sur la création d'un instrument d'urgence du marché intérieur (SMEI), destiné à garantir une solution structurelle et concrète pour la sauvegarde de la libre circulation des personnes, des biens et des services en cas de crises futures.

L'architecture de gestion de crise proposée dans ce cadre comprend un mécanisme de veille pour le marché unique, la détermination de différents niveaux de risque et la coordination d'une réponse graduée selon trois phases : prévention des urgences, situation d'alerte et situation d'urgence.

Lorsqu'une situation d'alerte est décrétée, la proposition de règlement prévoit que les Etats membres, en lien avec la Commission, concentrent leur veille sur des chaînes d'approvisionnement de biens qualifiés d'importance stratégique et qu'ils constituent des réserves stratégiques desdits biens.

Lorsqu'une situation d'urgence est déclenchée, la proposition de règlement établit une liste de restrictions proscrites et prévoit la mise en place d'un contrôle rapide et renforcé des restrictions décidées par les États membres. A cette occasion, la Commission disposerait, en outre, de la faculté :

- d'émettre des demandes d'informations ciblées auprès des opérateurs économiques, susceptibles de revêtir une forme contraignante assortie d'un pouvoir de sanction ;
- de demander aux opérateurs économiques d'accepter des commandes prioritaires pour des produits jugés utiles en situation de crise, dont la liste serait fixée par un acte d'exécution.

En tout état de cause, ce projet de texte prévoit la possibilité pour les Etats membres de préserver les intérêts essentiels de leur sécurité. Ces travaux européens en cours ne font ainsi pas obstacle à ce que la France se dote de mécanismes de droit interne susceptibles de garantir la continuité l'approvisionnement de ses forces armées.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Les dispositions de la mesure permettant d'imposer la constitution de stocks n'a, au premier ordre, pas d'impact macroéconomique : une fois la constitution initiale des stocks, qui amènera à une sur-commande temporaire sur les marchés, les flux de commandes pour maintenir ces stocks découleront des flux de production et reviendront donc dans des flux habituels auprès des fournisseurs, ne créant pas de déséquilibre durable par rapport aux autres acteurs économiques pouvant dépendre des mêmes fournisseurs. Il est à noter que la constitution initiale représente un flux limité par rapport aux volumes commandés pour les activités civiles : l'impact potentiel est donc jugé non-significatif et temporaire.

Les dispositions de la mesure de priorisation peuvent par principe avoir des conséquences macroéconomiques sur les activités hors défense qui se verraient ralenties du fait de la priorisation accordée à l'exécution des prestations au profit des marchés de défense. Les tailles limitées des séries d'équipements militaires, par comparaison aux séries et volumes produits pour les activités industrielles civiles, permettent néanmoins de considérer que cet impact restera limité.

4.2.2. Impacts sur les entreprises

Les dispositions de constitution de stocks peuvent avoir un impact économique sur les entreprises, du fait de l'immobilisation financière qui en découle. Cette demande se justifie néanmoins au titre des arguments développés préalablement dans cette étude d'impact, par le caractère stratégique des activités menées au profit de l'Etat, qui nécessite que les industriels concernés prennent des précautions adaptées aux enjeux, à l'instar des dispositions existantes pour les stocks pétroliers et dans le secteur de la santé.

Alors que la constitution de stocks s'accompagne de l'obligation, pour les entreprises concernées, de communiquer au ministère de la défense les éléments strictement nécessaires au contrôle du respect des mesures ainsi prononcées, il peut être souligné que les titulaires d'une autorisation de fabrication et de commerce d'armes ou de matériels de guerre sont d'ores et déjà tenus, sur le fondement du second alinéa de l'article L. 2332-5 du code de la défense, d'établir un registre exhaustif des matériels mis en fabrication, réparation, transformation, achetés, vendus, loués, conservés, stockés ou détruits[266]. La compilation des informations portant sur les stocks constitués au titre du nouvel article L. 1339-1 du code de la défense ne constituera, en ce sens, qu'un corolaire de la tenue de ce registre. Dans la mesure où les agents habilités à contrôler le respect de la législation sur l'armement disposent déjà de la faculté de solliciter la fourniture de tous renseignements verbaux ou écrits et de tous comptes rendus nécessaires à la réalisation de ce contrôle[267], cette nouvelle obligation s'inscrira dans la continuité de celles qui incombent aujourd'hui aux entreprises concernées.

Par ailleurs, le texte n'est pas prescriptif sur la nature des solutions et les industriels peuvent définir entre eux les conditions dans lesquelles ils entendent, le cas échéant, mutualiser les stocks de références communes. Les dispositions de la mesure de priorisation n'ont pas de conséquence financière pour les entreprises du fait du mécanisme prévu de compensation. Les impacts économiques potentiels, liés à l'insatisfaction des clients qui verraient leurs fournitures retardées, semble acceptables compte tenu du niveau législatif du dispositif, dont les entreprises pourront se prévaloir pour justifier le caractère subi du décalage. L'existence d'un dispositif similaire dans la législation américaine est également un élément pédagogique utile pour les entreprises vers leur base de clientèle. Le caractère législatif du dispositif permet également aux entreprises d'inclure progressivement des clauses adaptées dans leurs contrats avec leurs clients.

4.2.3. Impacts budgétaires

Ainsi que le permet la jurisprudence constitutionnelle rappelée *supra* au sein de la rubrique 1.2.4, l'obligation faite aux entreprises contribuant à l'approvisionnement des forces armées de constituer des stocks de composants ou de matières premières d'intérêt stratégique n'ouvrira

[266] Cf. articles R. 2332-17 à R. 2332-20 du code de la défense et R. 313-40 et R. 313-41 du code de la sécurité intérieure.

[267] Cf. quatrième alinéa de l'article L. 2339-1 du code de la défense et cinquième alinéa de l'article L. 317-1 du code de la sécurité intérieure.

pas droit à l'indemnisation des préjudices relatifs aux coûts de constitution et de l'entretien desdits stocks. Cette mesure n'aura, en ce sens, pas d'impact sur les finances publiques.

A contrario, l'obligation, pour l'Etat, de compenser intégralement le préjudice matériel résultant de manière directe et certaine des mesures de priorisation prononcées sur le fondement de l'article L. 1339-2 nouveau du code de la défense emportera, le cas échéant, un impact budgétaire. Néanmoins, en raison même du caractère conjoncturel du recours à une telle mesure, ce dernier demeure impossible à quantifier.

Le souci d'apporter une juste indemnisation aux entreprises concernées, tout en assurant la meilleure gestion possible des deniers de l'Etat justifie, en outre, l'obligation pour l'industriel de fournir à l'administration, si celle-ci en fait la demande, tous documents ou éléments d'information de nature à justifier le montant de l'indemnisation due. Ce dispositif, qui n'a pas vocation à être utilisé de façon systématique, pourra notamment trouver à s'appliquer lorsque l'indemnisation sollicitée sera considérée comme excessive par l'administration.

En tout état de cause, le coût financier de cette priorisation constituera l'un des paramètres que l'Etat devra prendre en compte avant de décider d'user de ce pouvoir et conditionnera, le cas échéant, le périmètre des mesures effectivement mises en œuvre.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La mise en œuvre des deux dispositifs introduits aux articles L. 1339-1 et L. 1339-2 nouveaux du code de la défense demeure facultative pour l'autorité administrative. Ceux-ci ne sauraient, en ce sens, être considérés comme représentant une charge pérenne pour les services compétents au sein du ministère des armées.

En outre, si l'autorité administrative décide d'y recourir, il peut être souligné que ces services disposent d'ores et déjà d'un certain nombre d'informations susceptibles d'en faciliter l'application, acquises à l'occasion de l'instruction des demandes d'autorisation de fabrication et de commerce ou de la passation des marchés de défense et de sécurité dont sont titulaires les entreprises concernées. Ce lien préexistant entre les destinataires des mesures correspondantes est ainsi de nature à faciliter la tâche de l'administration.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les représentants des industriels concernés ont été consultés dans le cadre de groupes de travail dédiés, s'agissant des réflexions « économie de guerre ». Les objectifs du dispositif ont ainsi pu être partagés avec le Conseil des industries de défense française (CIDEF), les principaux maitres d'œuvre industriels, les groupements interprofessionnels des secteurs de défense et certains groupements représentants les PME. Les modalités détaillées de mise en œuvre de la réforme n'ont cependant pas été communiquées aux intéressés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ainsi qu'il est précisé *infra* au sein de l'item 5.2.3, les présentes dispositions législatives nécessitent l'adoption d'un décret en Conseil d'Etat pour produire leur plein effet.

Ces mesures n'entreront en vigueur qu'à compter de la publication dudit décret d'application et, au plus tard, dans un délai de douze mois à compter de la publication de la présente loi.

5.2.2. Application dans l'espace

Conformément aux dispositions de l'article L. 1 du code de la défense, s'agissant d'une mesure liée à la politique de défense nationale, la présente disposition s'appliquera de plein droit sur l'ensemble du territoire de la République, y compris à l'ensemble des collectivités d'outre-mer, sans qu'aucune mention expresse d'application ne soit requise.

5.2.3. Textes d'application

Il ressort du deuxième alinéa du I de l'article L. 1339-1 nouveau du code de la défense qu'il appartient au pouvoir réglementaire de fixer la proportion maximale que peut représenter l'obligation de constitution de stocks d'intérêt stratégique imposée à une entreprise par rapport au chiffre d'affaires résultant de ses ventes de matériels au cours des deux exercices précédents. A cet égard, il est précisé que cette valeur maximale peut être différenciée selon la nature des matières et composants considérés.

Par ailleurs, il ressort du premier alinéa du I des articles L. 1339-1 et L. 1339-2 nouveaux de ce code que la mise en œuvre des obligations de constitution de stocks d'intérêt stratégique et de priorisation des commandes est ordonnée par voie d'arrêté.

Enfin, ainsi que le précise l'article L. 1339-3 nouveau du même code, les modalités d'application de ces deux dispositifs doivent être précisées par décret en Conseil d'Etat. Les dispositions correspondantes, qui seront également codifiées au sein du chapitre IX du titre III du livre III de la première partie du code de la défense, devront notamment définir les autorités compétentes :

- d'une part, pour ordonner la mise en œuvre des mesures correspondantes ;
- d'autre part, l'autorité compétente pour prononcer des sanctions administratives en cas de manquement aux obligations correspondantes.

Article 25 : Faire évoluer le régime des enquêtes de coûts dans les marchés publics

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Lorsque l'Etat et ses établissements publics concluent des marchés publics, ils ont la possibilité, dans certains cas identifiés, de diligenter, auprès des soumissionnaires, titulaires, entreprises liées et sous-contractants les plus importants, des enquêtes afin de déterminer les coûts de revient (réels ou estimés) des prestations objet de ces marchés. Ce contrôle, qui porte sur les renseignements permettant d'établir le coût de revient, est destiné à améliorer la connaissance par l'administration des coûts industriels afin de permettre, pour des prestations « analogues » et en l'absence de concurrence, une négociation rationnelle des prix. Ce système permet d'éviter une hausse injustifiée des prix négociés avec les entreprises en situation de monopole, incite les entreprises concernées à maitriser leurs coûts et contribue à garantir le bon usage des deniers publics (convenance du prix négocié).

Le code de la commande publique (CCP) prévoit et encadre cette pratique aux articles L. 2196-4 à L. 2196-6 pour les marchés dits « classiques » et L. 2396-3 et L. 2396-4 pour les marchés de défense ou de sécurité (MDS). En revanche, rien n'est prévu pour les « autres marchés » du livre V de la deuxième partie du code.

Lesdites enquêtes ne peuvent concerner que « *les marchés pour lesquels la spécialité des techniques, le petit nombre de candidats possédant la compétence requise, des motifs de secret ou des raisons d'urgence impérieuse ou de crise ne permettent pas de faire appel à la concurrence ou de la faire jouer efficacement* » et ceux dont les prestations sont complexes et de plus de cinq ans tel que le mentionne l'article L. 2196-4 du code de la commande publique (article L. 2396-3 pour les MDS).

Dans le cadre de telles enquêtes, les entreprises concernées fournissent à l'acheteur, à sa demande, « *tous renseignements sur les éléments techniques et comptables du coût de revient des prestations qui font l'objet du marché* » (article L. 2196-5 du CCP). De plus, les titulaires des marchés comme leurs sous-traitants ont l'obligation de « *permettre et faciliter la vérification éventuelle, sur pièces ou sur place, de l'exactitude de* [ces] *renseignements* » ; dans ce cadre, ils peuvent être « *tenus de présenter leurs bilans, comptes de résultat ainsi que leur comptabilité analytique et tous documents de nature à permettre l'établissement des coûts de revient* » (article L. 2196-6 du CCP).

Concrètement, dans cette situation, la concurrence ne s'exerce pas efficacement et ne peut donc pas jouer entièrement son rôle de modérateur des prix. Pour pallier les inconvénients de cette situation, l'administration effectue un contrôle *a posteriori* (après attribution du marché et achèvement des prestations) des coûts réellement supportés par le titulaire ainsi que par ses

sous-contractants les plus importants et réutilise les éléments ainsi collectés dans le cadre de la négociation des nouveaux marchés comportant des prestations analogues (il s'agit le plus souvent de nouvelles tranches de fabrication d'un produit - qui a pu subir des évolutions limitées-, de la poursuite de la maintenance d'un même produit, de la réalisation de prestations de services semblables, *etc.*). Ce dispositif est particulièrement efficace pour les prestations récurrentes (telle que la maintenance).

L'administration peut aussi réaliser un contrôle des éléments ayant servi à l'élaboration du devis du soumissionnaire. Ce contrôle est effectué lors de la procédure de passation des marchés après la remise des offres par les soumissionnaires et en amont ou en parallèle de la négociation. Dans ce cas, il s'agit d'un contrôle *a priori* (articles L. 2196-5 du CCP et L. 2396-3 pour les MDS). Il est alors possible d'enquêter sur les conditions de construction de l'offre et sur les références sur lesquelles le soumissionnaire s'est appuyé.

1.2. CADRE CONSTITUTIONNEL

Les dispositions relatives aux enquêtes de coût concourent à satisfaire l'exigence constitutionnelle de bon usage des deniers publics, qui découle de l'article 14 de la Déclaration des droits de l'homme et du citoyen[268].

Par ailleurs, le droit de communication des renseignements dont dispose l'administration auprès des entreprises concernées est de nature à porter atteinte à la liberté d'entreprendre. Saisi du droit de communication reconnu aux agents de l'Autorité de la concurrence, portant sur les livres, factures et autres documents professionnels appartenant à une entreprise ou un commerçant faisant l'objet d'une enquête, le Conseil constitutionnel l'a jugé conforme à la Constitution[269]. Répondant plus particulièrement au grief tiré de la méconnaissance du droit au respect de la vie privée et du secret des correspondances, le Conseil constitutionnel, pour l'écarter, s'est notamment attaché à la nature particulière des documents dont la communication est demandée, documents professionnels ou de travail, et sur le fait que les dispositions en cause ne permettent pas d'exiger la communication de documents protégés par le droit au respect de la vie privée ou le secret professionnel.

1.3. CADRE CONVENTIONNEL

Les dispositions relatives au contrôle des coûts de revient relèvent strictement du droit national. Le droit de l'Union européenne n'impose pas d'y recourir et, a contrario, ne l'interdit pas non plus.

[268] Conseil constitutionnel, décision n° 2019-781 DC, 16 mai 2019, § 55 et 56, *Loi relative à la croissance et à la transformation des entreprises.*

[269] Conseil constitutionnel, décision n° 2016-552 QPC du 8 juillet 2016.

1.4. ÉLEMENTS DE DROIT COMPARE

La plupart des grands Etats dans le monde disposant d'une industrie d'armement ont, contrairement à la France qui fait ainsi exception, un texte normatif qui détaille la méthode de construction des éléments de coûts pour la négociation des marchés d'armement sans mise en concurrence ou la prise en compte directe dans les marchés en dépenses contrôlées.

Ainsi, depuis 1953, il existe dans le droit allemand un texte relatif aux principes de détermination des prix sur la base du prix de revient (« Leitsätze für Preisermittlung auf Grund von Selbstkosten »).

En 2014, le Royaume-Uni s'est doté d'une législation sur le contrôle des coûts admissibles pour la passation des contrats de défense (« Allowable Costs guidance »). Le ministère de la défense et ses sous-traitants doivent examiner conjointement, lors de la passation d'un contrat, si les coûts afférents sont admissibles dans les contrats de défense éligibles.

En Espagne, une ordonnance du 15 octobre 1998 édicte les règles établissant les critères à utiliser pour le calcul des coûts de certains marchés de fournitures, de conseil et d'assistance et des services qui sont passés par le ministère de la défense en procédure négociée.

Enfin, en 2012, le Canada a adopté un texte sur les « Principes des coûts contractuels » destiné à détailler l'ensemble des coûts à prendre en considération dans la conclusion de contrats.

Des dispositifs similaires existent également en Italie et en Australie.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le contrôle de la véracité des informations justifiant le montant du prix proposé par une entreprise est fondamental pour les acheteurs publics lorsqu'ils ne peuvent s'appuyer sur d'autres éléments pour apprécier la convenance du prix. Le code de la commande publique leur offre cette prérogative.

Néanmoins, en l'état du droit, il n'existe aucune disposition permettant de définir la constitution et les modalités de calcul des coûts de revient des marchés publics (charges incorporables aux coûts et règles d'incorporation), ce qui conduit à des contentieux lors de la réalisation des contrôles, de la présentation et de l'exploitation de leurs résultats.

Avant leur abrogation en 1999 à la suite de décisions du Conseil d'Etat[270], des arrêtés portant approbation de cahiers des clauses comptables applicables à la détermination des coûts de revient précisaient les charges non incorporables aux coûts[271] et les modalités de calculs des

[270] Conseil d'Etat, 17 décembre 1999, Conseil des industries de défense française, n° 191514 et n° 191515.

[271] tels que les dividendes, l'impôt sur les sociétés, les amortissements des frais d'établissement, les indemnités de licenciement.

taux horaires et de frais. Depuis lors, l'administration et les entreprises de la base industrielle et technologique de défense ne sont pas parvenus à s'entendre sur la détermination des coûts de revient, ce qui est source de difficultés lors des négociations des contrats et de contentieux.

Par conséquent, afin de clarifier le mode de calcul des éléments comptables nécessaires à la valorisation des éléments techniques du coût de revient dans les marchés, tant auprès des industriels que des instances de l'Union européenne, il est proposé d'insérer une accroche dans la partie législative du code de la commande publique, en l'occurrence dans l'article L. 2196-7, permettant l'élaboration de modes de calcul, à valeur de référentiel, par voie règlementaire.

Cette nouvelle disposition est valable tant pour les marchés publics du livre I que pour les marchés de défense ou de sécurité relevant du livre III du CCP ou ceux relevant du livre V du même code. L'article L. 2396-3 sera modifié à cet effet, dans le livre relatif aux MDS.

Pour mémoire, les marchés relevant du livre V, intitulé « autres marchés publics », échappent au droit de l'Union européenne (en particulier aux règles de publicité et de mise en concurrence) et comprennent notamment certains marchés de défense et de sécurité, mentionnés à l'article L. 2515-1. Ainsi, certains contrats répondant à la définition d'un marché de défense ou de sécurité peuvent ne pas être soumis à l'essentiel des dispositions du code. C'est le cas :

- des marchés portant sur des armes, munitions ou matériel de guerre lorsque, au sens de l'article 346 du Traité sur le fonctionnement de l'Union européenne, la protection des intérêts essentiels de sécurité de l'État l'exige, notamment pour des achats qui nécessitent une confidentialité extrêmement élevée ou une grande rapidité d'acquisition (3° de l'article L. 2515-1) ;
- des marchés pour lesquels l'application de la deuxième partie du code obligerait à une divulgation d'informations contraire aux intérêts essentiels de sécurité de l'État, notamment pour des travaux, fournitures ou services particulièrement sensibles, qui nécessitent une confidentialité extrêmement élevée, tels que certains achats destinés à la protection des frontières ou à la lutte contre le terrorisme ou la criminalité organisée, des achats liés au cryptage ou destinés spécifiquement à des activités secrètes ou à d'autres activités tout aussi sensibles menées par les forces de sécurité intérieure ou par les forces armées (4° de l'article L. 2515-1) ;
- des marchés conclus selon des règles de passation particulières prévues par un accord international ou un arrangement administratif conclu entre au moins un État membre de l'Union européenne et au moins un État tiers (6° de l'article L. 2515-1) ;
- des marchés destinés aux activités de renseignement, y compris les activités de contre-espionnage, de contre-terrorisme et de lutte contre la criminalité organisée (7° de l'article L. 2515-1) ;
- des marchés passés pour des besoins opérationnels hors du territoire de l'Union européenne et que les besoins opérationnels exigent qu'ils soient conclus avec des opérateurs économiques locaux implantés dans la zone des opérations (9° de l'article L. 2515-1) ;

Les marchés de défense ou de sécurité du livre III, *a contrario,* sont des marchés qui répondent à la définition des MDS issue de l'article L. 1113-1 du CCP mais dont l'objet ne relève pas de la liste précitée.

- La duplication du dispositif de contrôle des coûts de revient aux « autres marchés de défense ou de sécurité » du livre V du CCP.

Le dispositif de contrôle des coûts de revient doit également être rendu expressément applicable aux marchés relevant du livre V du code de la commande publique. En effet, compte tenu de l'absence de mise en concurrence de ces marchés, les soumissionnaires et titulaires de cette catégorie de marchés publics devraient, tout particulièrement, être soumis aux mêmes obligations de communication des renseignements relatifs aux éléments techniques et comptables du coût de revient de facilitation des vérifications sur pièces et sur place. Les titulaires peuvent faire l'objet d'une enquête au titre de l'article 54 de la loi n° 63-156 du 23 février 1963 de finances pour 1963 et de son décret d'application de 1964 - mais ces anciens textes ont une portée moindre que les dispositions du code de la commande publique applicables aux marchés des livres I et III (en particulier, ils ne concernent que les titulaires, et non les soumissionnaires).

Les marchés du livre V ainsi que les offres des soumissionnaires à de tels marchés, à l'instar de ceux relevant des livres I et III, doivent être contrôlés afin de vérifier que les prix proposés restent cohérents avec les coûts de revient pour les entreprises.

Cette mesure se justifie par le nombre et le volume financier très importants de marchés d'armement passés sur le fondement du livre V du code, dont certains des plus stratégiques pour les forces, comme les achats de sous-marins nucléaires lanceurs d'engins (SNLE). Les marchés d'armement passés sur le fondement du livre V du CCP représentent environ six milliards d'euros par an, en moyenne sur les dernières années.

L'absence de base légale explicite prive actuellement les acheteurs de leur capacité à imposer aux soumissionnaires et titulaires de marchés passés dans le cadre du livre V du code la réalisation d'enquête de coût.

Il est donc nécessaire de légiférer afin de dupliquer le régime actuellement en vigueur pour les marchés classiques du livre I (articles L. 2196-4 à L. 2196-6 du code) et les marchés de défense ou de sécurité (MDS) du livre III (articles L. 2396-3 et L. 2396-4) aux marchés de défense ou de sécurité du livre V.

C'est l'objet de la création de l'article L. 2521-6 du code de la commande publique qui aura pour objet d'étendre au livre V les règles des enquêtes de coûts aujourd'hui applicables aux marchés du livre I et du livre III (MDS).

De cette façon, le ministère des armées pourra imposer le contrôle des coûts à ses cocontractants sur le fondement de l'article L. 2521-6 applicable aux MDS du livre V.

2.2. OBJECTIFS POURSUIVIS

L'objectif des dispositions présentées est double.

D'une part, l'insertion d'articles législatifs, permettant d'exiger précisément des titulaires et des soumissionnaires, par voie d'arrêté, des renseignements sur les éléments de coûts de revient objectivables, clarifiera et sécurisera le dispositif de contrôle des coûts mis en œuvre par le ministère de la défense. Cela préservera du risque de contentieux.

La pratique des enquêtes de coûts, mise en œuvre depuis de nombreuses années au ministère des armées par la direction générale de l'armement, a vu son fondement juridique fortement évoluer depuis les années 1960.

En 1996, trois arrêtés interministériels[272] ont défini de manière très détaillée les modalités de tenue des comptabilités des entreprises pour les marchés passés avec les sociétés des secteurs aéronautique et spatial, de l'ingénierie et de l'électronique et des télécommunications, à des fins de détermination des coûts de revient. Il s'agissait de poser dès la passation du marché les conditions de réalisation ultérieures des enquêtes de coûts. Toutefois, constatant que les ministres avaient excédé l'habilitation donnée par la loi (qui se bornait à les habiliter à déterminer les formes selon lesquelles devaient être présentés les comptes des entreprises soumises aux enquêtes et à fixer les règles à suivre pour la tenue de comptabilités spéciales à chaque marché) « *notamment en édictant le principe d'une rémunération forfaitaire pour certains coûts de production et en en excluant d'autres du calcul du prix des produits vendus* », le Conseil d'Etat a invalidé deux de ces arrêtés, intéressant directement la défense (aéronautique et spatial ; électronique et télécommunications) à la demande du CIDEF[273].

Un nouvel arrêté a donc été adopté le 20 décembre 2000[274], définissant le cadre général dans lequel sont déterminés les coûts de revient des prestations des sociétés intervenant dans le domaine aéronautique et spatial et les domaines des télécommunications et de la construction aéronautique. Il se borne à définir les principes comptables que les titulaires des marchés doivent mettre en œuvre pour les besoins des enquêtes de coûts *a posteriori*, sans arrêter la liste des postes comptables à retenir ou à exclure pour déterminer le coût de revient.

La disposition législative proposée vise à élargir l'habilitation donnée aux ministres compétents pour que puissent être définies par voie d'arrêté les modalités de calcul des éléments comptables

---

[272] Arrêté du 1er juillet 1986 portant approbation du cahier des clauses comptables pour les sociétés d'ingénierie, les bureaux d'études et les sociétés de conseils. Cet arrêté, contrairement aux deux autres, n'a pas été abrogé en 1999 et est toujours applicable.

Arrêté du 5 mars 1996 définissant le cadre général dans lequel sont déterminés les coûts de revient des prestations des sociétés intervenant dans le domaine aéronautique et spatial.

Arrêté du 2 mai 1996 définissant le cadre général dans lequel sont déterminés les coûts de revient des prestations des sociétés intervenant dans les domaines des télécommunications et de la construction électronique.

[273] CE, 17 décembre 1999, n° 191514 et n° 191515.

[274] Arrêté du 20 décembre 2000 définissant le cadre général dans lequel sont déterminés les coûts et coûts de revient des prestations des sociétés intervenant dans le domaine aéronautique et spatial et les domaines des télécommunications et de la construction électronique.

de valorisation, offrant plus de transparence pour les opérateurs économiques qu'ils soient soumissionnaires ou titulaires de marchés tout en assurant la sécurité juridique desdits marchés.

D'autre part, le ministère cherche à étendre le régime des enquêtes de coûts aux marchés de défense et de sécurité du livre V de la deuxième partie du code de la commande publique.

L'objectif, à travers cette modification, est de permettre aux MDS du livre V d'avoir une réglementation en termes de contrôle des coûts de revient du même niveau que celle applicable aux marchés de défense ou de sécurité du livre III.

En effet, ces marchés ont, à l'instar de ceux relevant des titres I et III, besoin de faire l'objet d'enquêtes de coûts afin de contrôler l'efficience des achats. A ce jour, le contrôle réalisé s'appuie sur des dispositions consensuelles, par définition soumises à la bonne volonté du soumissionnaire.

L'application des dispositions relatives au contrôle des coûts aux marchés de défense ou de sécurité du livre V, déjà en vigueur pour les marchés publics « classiques » et les marchés de défense ou de sécurité du livre III, est pertinente car l'absence de mise en concurrence dans ces marchés stratégiques et sensibles les expose particulièrement aux risques de dérives des prix.

En effet, l'absence de mise en concurrence prive l'acheteur de capacité de négociation, qu'il semble opportun de compenser par une obligation, à la charge des soumissionnaires et des titulaires, de transparence sur les coûts de revient des prestations qui font l'objet du marché. Le contrôle de l'estimation des coûts de revient et des coûts réels aura lieu tant au stade de la passation des marchés, lorsque les soumissionnaires remettront leur offre, qu'au stade de l'exécution du marché, après attribution de ce dernier dans les mêmes conditions que pour les marchés du livre I et III.

L'objectif de ces mesures pour le ministère des armées est *in fine* un rééquilibrage de ses relations avec les entreprises de la base industrielle et technologique de défense. La définition par voie réglementaire des éléments comptables de valorisation à prendre en compte pour l'estimation du coût de revient ne s'apparente aucunement à un régime de prix administrés mais vise uniquement à déterminer une base de négociation pour apprécier la convenance des marges pratiquées par l'entreprise.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Le *statu quo* pourrait être source de contentieux persistants : en l'absence de dispositions à portée contraignante à l'égard des industriels de défense concernés[275], l'incertitude continuerait de prévaloir en ce qui concerne tant le champ d'application des enquêtes de coûts que les éléments à prendre en compte au titre de la valorisation des coûts supportés par l'industriel pour la réalisation de la prestation.

3.2. OPTION RETENUE

D'une part, en ce qui concerne les marchés publics du livre I, il est proposé d'insérer l'article L. 2196-7 dans le code de la commande publique ainsi rédigé :

« Pour l'application de la présente section, peuvent être précisées par décret, en tant que de besoin :

1° La forme selon laquelle les éléments techniques et comptables mentionnés à l'article L. 2196-5 et au second alinéa de l'article L. 2196-6 sont présentés à l'administration, si celle-ci en fait la demande ;

2° La nature des charges comprises dans la détermination du coût de revient et les modalités de leur comptabilisation. »

D'autre part, pour les marchés de défense ou de sécurité du livre III, il est proposé de modifier l'article L. 2396-3 du code de la commande publique de la manière suivante : « *Les dispositions des articles L. 2196-4, L. 2196-5 et L. 2196-7 s'appliquent* ».

Enfin, afin de rendre applicable le régime des enquêtes de coûts actuellement en vigueur pour les marchés classiques et les MDS du livre III, aux marchés de défense ou de sécurité du livre V, il est proposé d'insérer l'article L. 2521-6 ainsi rédigé :

« *La section 3 du chapitre VI du titre IX du livre III relative au contrôle du coût de revient des marchés de l'Etat et de ses établissements publics est applicable aux marchés publics de défense ou de sécurité mentionnés au chapitre V du titre 1er présent livre.* »

[275] Voir, notamment, la décision du Conseil d'Etat (10 février 2023, n° 460448, *Conseil des industries de défense françaises*, conc. C. Guibé), qui juge que la lettre par laquelle le délégué général pour l'armement donne son interprétation de la notion de coûts de revient des prestations, pour la réalisation des enquêtes de coût, ne constitue pas un « *document de portée générale susceptible de produire des effets notables sur les droits ou la situation des entreprises du secteur industriel de la défense* » et, partant, ne peut faire l'objet d'un recours devant le juge administratif.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La disposition relative à la définition des modalités de calcul des enquêtes de coûts de revient dans les marchés du livre I et du livre III implique la modification ultérieure du code de la commande publique dans sa partie réglementaire afin d'expliciter les modalités de calcul des éléments de coûts de revient des prestations et de détailler ce que recouvre la notion de coûts de revient.

La mesure relative à la duplication du régime des enquêtes de coûts de revient aux marchés du livre V s'applique exclusivement aux marchés de défense ou de sécurité relevant de ce livre. Par conséquent, cette disposition ne concerne pas les marchés autres que les MDS.

La disposition nouvelle s'articulera avec celles, de niveau réglementaire, prévoyant la possibilité de sanctions en cas d'inadéquation entre les attentes relatives aux éléments du contrôle du coût de revient et la réalisation par les titulaires ou les candidats. L'article R. 2196-8 du code de la commande publique prévoit ainsi un dispositif en deux temps :

- en amont du marché, au stade de la passation, « *lorsqu'une estimation du coût de revient est effectuée avant la notification du marché, l'acheteur indique dans les documents de la consultation et dans le marché les sanctions applicables en cas de manquement à l'obligation figurant au premier alinéa de l'article L. 2196-5* » (lequel prévoit que les soumissionnaires fournissent à l'acheteur, si celui-ci en fait la demande, tous renseignements sur les éléments techniques et comptables de l'estimation du coût de revient des prestations qui font l'objet du marché) ;

- après notification, « *si le titulaire ne fournit pas à l'acheteur, dans le délai imparti par celui-ci, les renseignements sur les éléments techniques et comptables du coût de revient des prestations qui font l'objet du marché ou fournit des renseignements inexacts, l'acheteur peut, <u>après mise en demeure restée sans effet, décider la suspension des paiements à intervenir dans la limite du dixième du montant du marché</u> lorsque le manquement est le fait du titulaire ou <u>retenir un montant équivalent</u>. Après nouvelle mise en demeure infructueuse, l'acheteur <u>peut décider de transformer cette retenue en retenue définitive</u>, sans préjudice de la résiliation éventuelle du marché aux torts du titulaire.* »

De plus, comme indiqué précédemment, la partie législative du code de la commande publique sera modifiée par le biais de l'insertion de l'article L. 2196-7 pour l'évolution du régime appliqué aux marchés civils et de l'article L. 2396-5 s'agissant des marchés de défense ou de sécurité du livre III.

Quant à la duplication du dispositif de contrôle des coûts de revient aux marchés de défense ou de sécurité du livre V du CCP, elle implique l'insertion de l'article L. 2521-6 au sein du chapitre 1er, du titre II du livre V du code de la commande publique.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Sans objet.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

La nouvelle disposition permet aux entreprises d'être parfaitement informées des modalités de calcul des coûts de revient pour les marchés publics qu'ils contractent avec l'administration. Elles pourront dès lors anticiper leur contribution aux enquêtes en mettant en place les outils permettant de répondre aux attendus des services acheteurs. La présentation des coûts selon les schémas retenus dans les futurs arrêtés leur demandera une adaptation raisonnable par rapport à leur comptabilité analytique et proportionnée au vu de l'objectivation des coûts qui en résultera.

De par son périmètre restreint (les marchés non mis en concurrence ou particulièrement complexes) et les modalités de sa mise en œuvre (les éléments techniques et comptables du coût de revient ne constituent qu'un des éléments permettant la négociation du prix), cette mesure ne peut être assimilée à un régime de dépenses contrôlées qui pèserait sur la liberté d'entreprendre.

Cette capacité de contrôle des coûts trouvera son application également lors de la passation de marchés de défense ou de sécurité relevant du livre V du code. Les entreprises devront dorénavant transmettre tous les renseignements nécessaires sur les éléments techniques et comptables de l'estimation du coût de revient des prestations qui font l'objet du marché. Sans porter atteinte à la libre détermination des prix, la mesure garantira davantage de transparence et une meilleure maitrise de la convenance des prix des marchés les plus sensibles.

4.2.3. Impacts budgétaires

L'évolution du contrôle des coûts de revient des marchés publics induit par le présent article permettra une meilleure maîtrise de la convenance des prix en évitant pour l'administration un éventuel surcoût de ses dépenses.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Grâce à l'introduction des présentes dispositions, le ministère des armées pourra effectuer un contrôle plus efficient des coûts réellement supportés par l'opérateur économique candidat, le soumissionnaire ou le titulaire du marché.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions nécessiteront la publication d'un décret pour être pleinement applicables.

5.2.2. Application dans l'espace

Les futures dispositions s'appliqueront sur l'ensemble du territoire de la République, aussi bien en métropole qu'en outre-mer en raison du principe d'identité législative qui prévaut dans le domaine des enquêtes de coûts pour les collectivités ultra-marines.

5.2.3. Textes d'application

Un décret simple explicitera les modalités de calcul des coûts de revient.

CHAPITRE IV – CREDIBILITE STRATEGIQUE

Article 26 : Renforcer l'autonomie des armées en matière sanitaire

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Le cœur de métier du service de santé des armées (SSA) est d'assurer le soutien sanitaire des forces armées et d'offrir aux militaires blessés la meilleure chance de survie et de récupération. En plus de cette mission principale, le service de santé des armées apporte une contribution conséquente dans le domaine de la santé publique et dans la mise en œuvre des plans gouvernementaux, destinés à faire face aux risques nucléaires, radiologiques, biologiques et chimiques (NRBC).

A cet effet, le SSA, qui est un service de soutien interarmées au sens de l'article L. 1142-1 du code de la défense, s'appuie sur cinq composantes qui forment un ensemble cohérent : médecine des forces, formation, ravitaillement sanitaire, recherche et médecine hospitalière. Composé en 2020 de 67% de militaires et 33% de civils, il comptait la même année 14 699 agents et 3952 réservistes.

Ses missions et ses attributions sont prévues aux articles R. 3232-11 et suivants du code de la défense.

1.1.1. En matière de soutien sanitaire des forces armées sur les théâtres d'opérations extérieures jusqu'en métropole

Plusieurs types de structures assurent la prise en charge des blessés tout au long de la chaîne santé sur le plan opérationnel, du « rôle 1 » au « rôle 4 ». Au sein même des unités de combat sont présentes des équipes sanitaires (médecine de l'avant) composées de médecins et de personnels paramédicaux formés à la prise en charge de polytraumatisés (rôle 1). Ils disposent de moyens mobiles, adaptés et performants, servis par des personnels habitués à l'urgence et entraînés aux conditions les plus difficiles. Des structures hospitalières légères sont placées au plus près des unités de combat et permettent le traitement des urgences absolues par des anesthésistes-réanimateurs et chirurgiens entraînés à agir dans des situations extrêmes (rôle 2). Le rôle 3 constitué par l'hôpital médico-chirurgical permet la stabilisation grâce à des techniques avancées de réanimation et de chirurgie ainsi que la mise en condition du militaire blessé pour son évacuation médicale stratégique par voie aérienne (MEDEVAC) vers les hôpitaux des armées ou les structures hospitalières disposant de moyens plus importants et des spécialités médicales ou chirurgicales indispensables à la suite de la prise en charge (hôpitaux médico-chirurgicaux) (rôle 4). Ces évacuations sanitaires précoces et systématiques permettant l'acheminement des

blessés vers ces établissements de soins sont au cœur de la doctrine du soutien médical français. Au cours de ces évacuations, le blessé bénéficie d'une assistance médicale constante.

Outre les compétences particulières que requiert un exercice de la médecine dans des conditions aussi délicates, cette proximité permanente du soutien sanitaire, considérée comme un facteur essentiel du moral des combattants, exige une organisation spécifique.

La chaîne de ravitaillement en produits de santé (médicaments, matériels biomédicaux, oxygène et produits sanguins...) est indispensable aux unités médicales opérationnelles (poste médical, antenne chirurgicale...) déployées hors du territoire national. Les produits fournis sont adaptés aux conditions particulières rencontrées sur les théâtres extérieurs et répondent aux exigences opérationnelles (rapidité d'exécution et de mise en œuvre).

L'approvisionnement en sang est crucial pour les troupes en opération puisque la principale cause de décès des blessés est l'hémorragie.

Actuellement, en application de l'article L. 1221-10 du code de la santé publique, seuls l'Etablissement français du sang, le centre de transfusion sanguine des armées, les établissements de santé et les hôpitaux des armées sont autorisés à conserver des produits sanguins labiles (globules rouge, plaquettes, plasma).

Pour assurer leur mission prioritaire de soutien sanitaire des forces armées, certains autres organismes du service de santé des armées doivent être en mesure d'assurer en urgence des transfusions sanguines afin d'optimiser les soins et d'augmenter les chances de survie des militaires blessés.

A ce titre, il est nécessaire d'autoriser les centres médicaux du service de santé des armées, lorsqu'ils sont situés dans des bâtiments de la marine nationale, et pour leurs équipes mobiles de soins exerçant leur mission dans les aéronefs militaires, ainsi que la brigade de sapeurs-pompiers de Paris et le bataillon des marins-pompiers de Marseille à conserver des produits sanguins labiles.

1.1.2. En matière de recherche et de médecine

Le Centre de transfusion sanguine des armées (CTSA) a pour mission première le soutien transfusionnel des forces armées, sur le territoire français et en opérations extérieures, en temps de paix, de crise ou de conflit. Il collecte le sang dans les établissements du ministère de la défense, le prépare et le contrôle afin de pouvoir distribuer aux Forces des produits sanguins labiles, tels que plasma, plaquettes et globules. La fabrication du plasma lyophilisé, appelé PLYO ou FLYP (French LYophilised Plasma) est une spécificité du CTSA.

Le CTSA mène des activités thérapeutiques et de recherche dans le cadre de la médecine régénérative. La recherche sur les cellules souches trouve une application directe en thérapie cellulaire, en hématologie pour les greffes de moelle et en chirurgie orthopédique. Celle sur la production des greffons (peau) sert à la prise en charge des grands brûlés.

Le VI de l'article L. 1222-11 du code de la santé publique prévoit que le CTSA est autorisé à réaliser la collecte, la qualification biologique du don et la préparation de produits sanguins labiles, leur distribution et leur délivrance notamment pour la satisfaction de la mission prioritaire de soutien sanitaire des forces armées.

Dans le cadre du plan NRBC, il a été décidé de développer des contre-mesures médicales relevant de la catégorie des médicaments dérivés du sang. Il est ainsi nécessaire d'autoriser le ministère des Armées à fabriquer ce type de médicaments.

Ces médicaments sont définis à l'article L. 5121-1 du code de la santé publique. Il s'agit de « tout médicament préparé industriellement à partir du sang ou de ses composants ». Ils comprennent notamment les médicaments issus du fractionnement du plasma et le plasma à finalité transfusionnelle.

Les dispositions de l'article L. 5124-14 du code de la santé publique confèrent à la société anonyme dénommée « Laboratoire français du fractionnement et des biotechnologies » un monopole de principe pour la fabrication de médicaments dérivés du sang à partir du sang ou de ses composants collectés par l'Etablissement français du sang (EFS).

L'article L. 1222-1-1 du code de la santé publique créé par l'ordonnance n° 2016-1406 du 20 octobre 2016[276] a néanmoins introduit une dérogation au profit de l'EFS pour lui permettre de poursuivre la fabrication de plasma transfusionnel, requalifié en médicament dérivé du sang par une décision du Conseil d'Etat[277] en vertu de la jurisprudence communautaire et des directives 2001/83/CE[278] et 2002/98/CE[279]. L'EFS peut seulement fabriquer des médicaments dérivés du sang de type plasma transfusionnel à l'exclusion de ceux, stabilisés, issus du fractionnement du sang sous réserve des dispositions de l'article L. 5124-14 du même code. Qu'il s'agisse donc du « Laboratoire français du fractionnement et des biotechnologies » ou de l'Etablissement français du sang, l'activité de fabrication de médicaments dérivés du sang est autorisée par la loi.

Le CTSA n'est pas autorisé actuellement à fabriquer des médicaments dérivés du sang alors que le développement et la fabrication de certains médicaments dérivés du sang par le service de santé des armées est nécessaire pour la prise en charge de personnes exposées ou des victimes d'événements employant des agents de nature nucléaire, radiologique, biologique et chimique. Ces médicaments constituent des solutions indispensables dans le cadre des contre-mesures médicales. L'usage de ces médicaments peut participer notamment à la prophylaxie (primaire et secondaire), aux prétraitement et traitement au titre du soutien médical lors des engagements

[276] Ordonnance n° 2016-1406 du 20 octobre 2016 portant adaptation et simplification de la législation relative à l'Etablissement français du sang et aux activités liées à la transfusion sanguine.

[277] Conseil d'État, 23 juillet 2014 N° 349717.

[278] Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain.

[279] Directive 2002/98/CE du Parlement européen et du Conseil du 27 janvier 2003 établissant des normes de qualité et de sécurité pour la collecte, le contrôle, la transformation, la conservation et la distribution du sang humain, et des composants sanguins, et modifiant la directive 2001/83/CE.

des forces armées hors et sur le territoire national et aussi à la contribution du ministère de la défense à la réponse de l'Etat aux risques et aux évènements NRBC.

Par conséquent, il est nécessaire de modifier l'article L. 1222-11 pour autoriser le CTSA à fabriquer, importer, exporter et exploiter les médicaments dérivés du sang définis au 18° de l'article L. 5121-1 afin de répondre à des besoins spécifiques de défense ou de sécurité nationale.

1.2. CADRE CONSTITUTIONNEL

Le Préambule de la Constitution du 27 octobre 1946 prévoit à l'alinéa 11 :

« Elle [la Nation] garantit à tous, notamment à l'enfant, à la mère et aux vieux travailleurs, la protection de la santé, la sécurité matérielle, le repos et les loisirs. Tout être humain qui, en raison de son âge, de son état physique ou mental, de la situation économique, se trouve dans l'incapacité de travailler a le droit d'obtenir de la collectivité des moyens convenables d'existence. »

1.3. CADRE CONVENTIONNEL

L'article 12 du Pacte international relatif aux droits économiques, sociaux et culturels, traité international multilatéral adopté le 16 décembre 1966 par l'Assemblée générale des Nations unies et entré en vigueur le 3 janvier 1976, stipule que « *1. Les Etats parties au présent Pacte reconnaissent le droit qu'a toute personne de jouir du meilleur état de santé physique et mentale qu'elle soit capable d'atteindre. 2. Les mesures que les Etats parties au présent Pacte prendront en vue d'assurer le plein exercice de ce droit devront comprendre les mesures nécessaires pour assurer : […] c) La prophylaxie et le traitement des maladies épidémiques, endémiques, professionnelles et autres, ainsi que la lutte contre ces maladies; d) La création de conditions propres à assurer à tous des services médicaux et une aide médicale en cas de maladie* ».

1.4. ÉLEMENTS DE DROIT COMPARE

S'agissant de la possibilité de conserver des produits sanguins labiles, l'Irlande autorise, depuis 2020, la réalisation de transfusions directement sur les lieux de l'accident. A ce titre, les ambulances sont autorisées à conserver des produits sanguins labiles.

S'agissant de la fabrication de médicaments dérivés du sang, de nombreux autres Etats européens (par exemple la Suisse ou l'Allemagne) ont fait le choix d'un modèle concurrentiel plutôt que l'octroi d'un monopole à une entreprise ou à une entité étatique désignée.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La conservation des produits sanguins labiles est strictement encadrée par les articles L.1221-10 et suivants du code de la santé publique. Une liste limitative désigne les structures qui peuvent conserver des produits sanguins labiles.

Pour la fabrication de médicaments, la loi prévoit que seuls le Laboratoire français du fractionnement et des biotechnologies et l'Etablissement français du sang peuvent fabriquer des médicaments dérivés du sang. Il est ainsi nécessaire, comme cela a été fait pour l'EFS à l'occasion de l'ordonnance n° 2016-1406 du 20 octobre 2016 précitée, de recourir à la loi pour permettre au CTSA d'en fabriquer. La loi fixe également les compétences du CTSA. Il est nécessaire de la modifier afin de prévoir la fabrication de médicaments dérivés du sang.

2.2. OBJECTIFS POURSUIVIS

D'une part, le stockage de produits sanguins labiles dans les aéronefs militaires au cours des rapatriements sanitaires, au sein des bâtiments de la marine nationale éloignés des structures de santé, dans les véhicules médicalisés de la brigade de sapeurs-pompiers de Paris et le bataillon des marins-pompiers de Marseille au cours des transports sanitaires entre les bases aériennes et les hôpitaux des armées permettrait d'optimiser les soins et d'augmenter les chances de survie des militaires blessés. Il est donc nécessaire de permettre à ces structures, en tant qu'elles sont chargées de missions spécifiques de défense, de conserver des produits sanguins labiles.

D'autre part, le Laboratoire français du fractionnement et des biotechnologies (société anonyme) ou l'Etablissement français du sang ne sont pas en mesure de fabriquer des médicaments dérivés du sang dans le but de constituer et d'entretenir un stock stratégique pour les besoins spécifiques de la défense. A l'inverse, le centre de transfusion sanguine des armées dispose de la capacité et des compétences pour fabriquer ces médicaments. Dans une logique d'autonomie stratégique comme de souveraineté nationale, il est donc nécessaire de confier cette compétence à un service de l'Etat tel que le CTSA.

L'objectif de la présente mesure est donc d'autoriser le centre de transfusion sanguine des armées à fabriquer des médicaments dérivés du sang dans le cadre du développement de contre-mesures médicales.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Pour ce qui concerne la conservation des produits labiles, il n'a été envisagé qu'une seule option, celle de la modification de l'article L. 1221-10 du code de la santé publique.

Concernant la fabrication de médicaments dérivés du sang par le centre de transfusion sanguine des armées, il a d'abord été envisagé de modifier l'article L. 5124-14 du code de la santé publique afin de créer une dérogation au monopole de principe conféré au Laboratoire français de fractionnement et de biotechnologie. Cependant, par parallélisme avec les mesures permettant à l'Etablissement français du sang de fabriquer des médicaments dérivés du sang, il a été décidé de modifier uniquement les dispositions particulières relatives au CTSA.

3.2. OPTION RETENUE

L'option retenue concernant la conservation des produits labiles est celle d'une modification de l'article L. 1221-10 du code de la santé publique afin de permettre à ces structures de conserver des produits sanguins labiles. Il est prévu que cette capacité de conservation soit réservée à des besoins spécifiques de la défense tels que le rapatriement d'un militaire blessé qui, exposé à des risques particuliers, nécessite une prise en charge rapide. Par ailleurs, les mêmes garanties que pour les établissements de santé sont applicables à ces structures (autorisation après avis du centre de transfusion sanguine des armées et sous la surveillance d'un médecin ou d'un pharmacien). Aux fins de coordination, l'article L.1221-10-2 est également modifié.

Concernant la fabrication de médicaments dérivés du sang, l'option retenue est la modification du VI de l'article L. 1222-11 du code de la santé publique afin d'y ajouter deux alinéas qui s'inspirent de l'article L. 1222-1-1 relatif à l'Etablissement français du sang.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La présente mesure modifie les articles L. 1221-10, L.1221-10-2 et L. 1222-11 du code de la santé publique.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La présente mesure est conforme à la directive 2002/98/CE du Parlement européen et du Conseil du 27 janvier 2003 établissant des normes de qualité et de sécurité pour la collecte, le

contrôle, la transformation, la conservation et la distribution du sang humain, et des composants sanguins, et modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain ainsi qu'à la directive 2001/83/CE du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

La fabrication de médicaments dérivés du sang par le centre de transfusion sanguine des armées sera financée par le budget du ministère des Armées. Le coût de développement est estimé à 11 millions d'euros.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'activité du CTSA va augmenter avec la fabrication de ces médicaments dérivés du sang. Cependant, cette montée en charge ne modifiera pas en profondeur la structuration du CTSA.

Le CTSA sera inspecté par l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) en qualité d'établissement pharmaceutique pour la fabrication de ces médicaments dérivés du sang. Cette nouvelle compétence nécessitera du personnel supplémentaire. En qualité d'exploitant, le CTSA devra respecter les critères normatifs d'un laboratoire exploitant.

4.5. IMPACTS SUR LES ARMEES

La conservation des produits sanguins labiles permet d'optimiser le soutien sanitaire des forces armées.

Par ailleurs, la mesure permettant la production de certains médicaments dérivés du sang renforce l'arsenal thérapeutique pour la protection des forces armées, notamment en matière de contre-mesures médicales. L'usage de ces médicaments peut notamment participer à la prophylaxie (primaire et secondaire), aux prétraitement et traitement au titre du soutien médical lors des engagements des forces armées hors et sur le territoire national et aussi à la contribution du ministère des Armées à la réponse de l'Etat aux risques et aux évènements NRBC.

4.6. IMPACTS SOCIAUX

4.6.1. Impacts sur la société

Sans objet.

4.6.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.6.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.6.4. Impacts sur la jeunesse

Sans objet.

4.6.5. Impacts sur les professions réglementées

Sans objet.

4.7. IMPACTS SUR LES PARTICULIERS

Le stockage de produits sanguins labiles dans les aéronefs militaires au cours des rapatriements sanitaires, au sein des bâtiments de la marine nationale éloignés des structures de santé, dans les véhicules médicalisés de la brigade de sapeurs-pompiers de Paris et le bataillon des marins-pompiers de Marseille au cours des transports sanitaires entre les bases aériennes et les hôpitaux des armées permettrait d'optimiser les soins et d'augmenter les chances de survie des militaires blessés.

La mesure permettant la production de certains médicaments dérivés du sang renforce l'arsenal thérapeutique pour la protection des militaires, notamment en matière de contre-mesures médicales. L'usage de ces médicaments peut notamment participer à la prophylaxie (primaire

et secondaire), aux prétraitement et traitement au titre du soutien médical lors des engagements des forces armées hors et sur le territoire national.

4.8. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Bien que son avis ne soit pas obligatoirement requis, l'Agence nationale de sécurité du médicament et des produits de santé a été consultée sur cette mesure.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

La mesure envisagée s'appliquera dès le lendemain de la publication de la loi au *Journal Officiel* de la République française.

5.2.2. Application dans l'espace

La mesure envisagée s'appliquera sur l'ensemble du territoire de la République française. Des mesures d'extension sont prévues à l'article 36 du présent projet de loi pour les territoires de Nouvelle-Calédonie, de Polynésie française, de Wallis-et-Futuna et des Terres australes et antarctiques françaises.

5.2.3. Textes d'application

La mesure sur la conservation des produits labiles appellera la rédaction d'un décret simple afin de préciser les modalités de l'autorisation accordée par l'autorité administrative après avis du centre de transfusion sanguine des armées.

Article 27 : Renforcement du régime légal de lutte contre les aéronefs circulant sans personne à bord présentant une menace

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Les aéronefs circulant sans personne à bord, couramment appelés « drones », sont des aéronefs dont le télépilote est la personne qui contrôle manuellement les évolutions ou, dans le cas d'un vol automatique, celle qui est en mesure à tout moment d'intervenir sur sa trajectoire ou, dans le cas d'un vol autonome, celle qui détermine directement la trajectoire ou les points de passage de ces aéronefs.

Le faible coût des drones, l'évolution de leurs technologies (autonomie, qualité des vidéos) et l'intérêt qu'ils suscitent dans la population entraînent un accroissement important de leur nombre.

Cette augmentation conduit à une utilisation accrue de l'espace aérien. Or, la circulation des drones dans l'espace aérien peut présenter des risques pour la sécurité des personnes, des sites, des autres aéronefs ou des biens.

En effet, les drones sont équipés de caméras qui peuvent transmettre des données sensibles au télépilote ou à un tiers, par exemple, sur la protection des sites, sur l'équipement des forces armées ou sur leurs modalités d'entraînement. Ces derniers peuvent, par ailleurs, survoler d'autres lieux sensibles dont les établissements pénitentiaires, les centrales nucléaires, les enceintes sportives et grands évènements (coupe du monde de rugby, G7, etc.) tout en étant susceptibles de transporter des substances interdites ou des matériels pouvant présenter un risque important pour la sécurité publique ou la défense nationale (explosifs, armes, dispositifs de piratage, etc.).

A ce titre, le rapport d'information parlementaire n° 2166[280] sur l'action aérospatiale de l'Etat de M. Ferrara et M. Lejeune relève que : « *L'usage malveillant des drones revêt plusieurs aspects. Il peut d'abord s'agir d'actions d'observation, afin de collecter du renseignement à des fins d'information et d'espionnage ou en vue de la commission d'un acte de violence, à l'instar d'une évasion de prison. De même, les drones peuvent être équipés de divers capteurs leur permettant d'opérer des écoutes. Ensuite, les drones peuvent être employés pour le transport de colis divers, voire être à même de larguer des objets, y compris explosifs, dans des zones d'accès interdit, sur des sites sensibles ou à des fins de contrebande. Leur fugacité accroît à cet égard le niveau de risque. De plus, l'usage légitime d'un drone peut également représenter un risque, du simple fait du manque de formation du télépilote ou du risque d'accident du fait d'une erreur de pilotage, d'une panne ou d'une collision.* »

[280] Rapport enregistré à la présidence de l'Assemblée nationale le 17 juillet 2019, page 9.

Le nombre de survols illicites constatés au-dessus de zones interdites de survol (dont des centrales nucléaires, des établissements pénitentiaires et des sites sensibles du ministère de la défense) est élevé et en augmentation sensible d'année en année.

Par ailleurs, lors de la mise en place d'un dispositif particulier de sûreté aérienne dans le cadre d'événements tels qu'un G7 ou le défilé du 14 juillet, les services chargés de la lutte contre les drones malveillants constatent la présence de nombreux drones dans les zones à protéger.

Pour répondre à ces préoccupations, l'article 24 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a complété l'article L. 33-3-1 du code des postes et des communications électroniques et a consacré la possibilité pour les services de l'Etat, sous certaines conditions, de recourir aux matériels de brouillage[281] contre les drones malveillants.

Néanmoins, ce mode de neutralisation ne peut agir que contre des drones dont le vol repose sur la réception de signaux radioélectriques, qu'il s'agisse de consignes émises par le pilote au sol, ou de signaux de navigation par satellite. Or, les développements technologiques rendent progressivement une partie des drones autonomes, donc insensibles au brouillage. Leur neutralisation devra reposer sur de nouvelles technologies de lutte qui deviennent progressivement disponibles aujourd'hui mais n'entrent pas dans le champ d'application de l'article L. 33-3-1 du code des postes et des communications électroniques.

C'est le cas :

- des armes à effet dirigé (AED) électromagnétiques, qui ne sont pas des brouilleurs mais visent à perturber directement le fonctionnement de l'électronique embarquée du drone et sont ainsi efficaces contre les drones opérant sans liaison externe (pilote, radionavigation) ;
- des drones intercepteurs qui bloquent le vol du drone malveillant par plusieurs moyens techniques :
    - brouillage électro magnétique embarqué ;
    - capture par filet, afin de déposer le drone potentiellement dangereux dans un endroit choisi, plutôt que le neutraliser sur place ;

[281] L'article L. 33-3-1 du code des postes et des communications électroniques dispose que : « I.- Sont prohibées l'une quelconque des activités suivantes : l'importation, la publicité, la cession à titre gratuit ou onéreux, la mise en circulation, l'installation, la détention et l'utilisation de tout dispositif destiné à rendre inopérants des équipements radioélectriques ou des appareils intégrant des équipements radioélectriques de tous types, tant pour l'émission que pour la réception. / II.- Par dérogation au premier alinéa, ces activités sont autorisées pour les besoins de l'ordre public, de la défense et de la sécurité nationale, ou du service public de la justice. / L'utilisation par les services de l'Etat de dispositifs destinés à rendre inopérant l'équipement radioélectrique d'un aéronef circulant sans personne à bord est autorisée, en cas de menace imminente, pour les besoins de l'ordre public, de la défense et de la sécurité nationales ou du service public de la justice ou afin de prévenir le survol d'une zone en violation d'une interdiction prononcée dans les conditions prévues au premier alinéa de l'article L. 6211-4 du code des transports. Un décret en Conseil d'Etat détermine les modalités de mise en œuvre de ces dispositifs, afin de garantir leur nécessité et leur proportionnalité au regard des finalités poursuivies, ainsi que les autorités compétentes pour y procéder. »

- percussion, etc.

1.2. CADRE CONSTITUTIONNEL

1.2.1. La sauvegarde des intérêts fondamentaux de la Nation est une exigence constitutionnelle susceptible de justifier une atteinte à d'autres principes à valeur constitutionnelle

Il ressort de la jurisprudence du Conseil constitutionnel et du Conseil d'Etat que les « *exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* », au premier rang desquelles figurent l'indépendance nationale et l'intégrité du territoire, qui en sont la finalité, mais également la protection du secret de la défense nationale et la libre disposition de la force armée, sont prises en compte par le juge dans son contrôle de proportionnalité en cas d'atteinte à d'autres principes à valeur constitutionnelle.

Il revient au juge d'assurer une « *conciliation qui ne soit pas déséquilibrée* » entre la sauvegarde des intérêts fondamentaux de la Nation et les autres exigences constitutionnelles[282].

1.2.2. L'objectif à valeur constitutionnelle de prévention des atteintes à l'ordre public doit être concilié avec les libertés constitutionnellement garanties

Le Conseil constitutionnel a reconnu l'objectif à valeur constitutionnel tiré de la prévention des atteintes à l'ordre public en considérant qu'il appartient au législateur d'assurer la conciliation entre, d'une part, l'exercice de libertés constitutionnellement garanties et, d'autre part, la prévention des atteintes à l'ordre public et notamment des atteintes à la sécurité des personnes et des biens[283].

Le droit de propriété figure parmi les libertés constitutionnelles devant être conciliées avec cet objectif à valeur constitutionnelle[284].

1.2.3. Les atteintes au droit de propriété doivent être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi

[282] Mme Ekaterina B., épouse D., et autres, 10 novembre 2011, n° 2011-192 QPC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif et du droit à un procès équitable ; Loi relative au renseignement, 23 juillet 2015, n° 2015-713 DC, à propos du droit des personnes intéressées à exercer un recours juridictionnel effectif, du droit à un procès équitable et du principe du contradictoire ; Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias, 10 novembre 2016, n° 2016-738 DC, à propos de la liberté d'expression et de communication ; La Quadrature du net, 9 juillet 2021, n° 2021-924 QPC, à propos du respect de la vie privée.

[283] Loi d'orientation et de programmation relative à la sécurité, 18 janvier 1995, n° 94-352 DC) ou la lutte contre le terrorisme (M. Rouchdi B. et autre, 29 mars 2018, n° 2017-695 QPC).

[284] M. Raïme A., 2 décembre 2016, n° 2016-600 QPC.

Il ressort de la jurisprudence du Conseil constitutionnel que : « *La propriété figure au nombre des droits de l'homme consacrés par les articles 2 et 17 de la Déclaration de 1789. Selon son article 17 : « La propriété étant un droit inviolable et sacré, nul ne peut en être privé, si ce n'est lorsque la nécessité publique, légalement constatée, l'exige évidemment, et sous la condition d'une juste et préalable indemnité ». En l'absence de privation du droit de propriété au sens de cet article, il résulte néanmoins de l'article 2 de la Déclaration de 1789 que les atteintes portées à ce droit doivent être justifiées par un motif d'intérêt général et proportionnées à l'objectif poursuivi.* »[285].

Ce droit est susceptible de faire l'objet d'une atteinte si l'utilisation d'un matériel a pour conséquence de faire chuter le drone, d'entrainer sa détérioration ou sa destruction. Toutefois, selon le type de drone en cause et selon le type de dispositif utilisé, le drone est susceptible de dévier de sa trajectoire, de retourner à son point de départ, d'atterrir ou de chuter au sol. L'atteinte au droit de propriété n'est alors que potentielle.

En tout état de cause, les atteintes au droit de propriété doivent être conciliées avec les exigences relevées aux points 1.2.1 et 1.2.2.

1.3. CADRE CONVENTIONNEL

La Convention relative à l'aviation civile internationale, conclue à Chicago le 7 décembre 1944, détermine les principes fondamentaux du droit international aérien. Son article 1er prévoit que : « *chaque Etat a la souveraineté complète et exclusive sur l'espace aérien au-dessus de son territoire* ».

Cette disposition est complétée par le b) de l'article 9 prévoyant que : « *Chaque Etat contractant se réserve également le droit, dans des circonstances exceptionnelles, en période de crise ou dans l'intérêt de la sécurité publique, de restreindre ou d'interdire temporairement et avec effet immédiat les vols au-dessus de tout ou partie de son territoire, à condition que cette restriction ou interdiction s'applique, sans distinction de nationalité, aux aéronefs de tous les autres Etats.* »

Enfin, l'article 36 de la Convention relative à l'aviation civile internationale prévoit que : « *Tout Etat contractant peut interdire ou réglementer l'usage d'appareils photographiques à bord des aéronefs survolant son territoire.* »

Plus spécifiquement sur les aéronefs sans pilote, l'article 8 de la Convention précise que : « *Aucun aéronef pouvant voler sans pilote ne peut survoler sans pilote le territoire d'un Etat contractant, sauf autorisation spéciale dudit Etat et conformément aux conditions de celle-ci. Chaque Etat contractant s'engage à faire en sorte que le vol d'un tel aéronef sans pilote dans des régions ouvertes aux aéronefs civils soit soumis à un contrôle qui permette d'éviter tout danger pour les aéronefs civils.* »

[285] M. Jean-Claude G., 17 janvier 2012, n°2011-209 QPC ; M. Raïme A., 2 décembre 2016, n° 2016-600 QPC.

Ces dispositions ont été déclinées en droit interne dans le livre II relatif à la circulation aérienne de la sixième partie relative à l'aviation civile du code des transports.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Comme évoqué au point 1.1, l'article 24 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, dorénavant codifié à l'article L. 33-3-1 du code des postes et des communications électroniques ne permet pas de couvrir les nouveaux matériels en ce que leurs effets ne ciblent pas spécifiquement l'équipement radioélectrique des drones. La modification de cet article du code des postes et des communications électroniques nécessite un texte de portée législative.

Par ailleurs, le droit de propriété qui est susceptible d'être altéré nécessite de recourir à la loi dès lors que l'article 34 de la Constitution prévoit notamment que : « *La loi fixe les règles concernant : les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ; les sujétions imposées par la Défense nationale aux citoyens en leur personne et en leurs biens* ».

2.2. OBJECTIFS POURSUIVIS

L'objectif poursuivi par ce dispositif est de compléter le cadre juridique existant en autorisant les services de l'Etat à utiliser d'autres dispositifs de lutte contre les drones présentant une menace pour l'ordre public, la défense ou la sécurité nationales ou les établissements pénitentiaires afin d'élargir le panel de moyens techniques offerts aux services de l'Etat concernés par la lutte contre les drones représentant une menace et de renforcer l'efficacité globale du dispositif de lutte contre les drones malveillants.

L'élargissement de ce panel offert à l'Etat est notamment motivé par l'évolution des capacités techniques des drones et des nouveaux moyens de lutte. Ainsi que l'a relevé le rapport d'information parlementaire n° 4320[286] de MM. Baudu et Lassalle relatif à « La guerre des drones » : « *D'ici deux ou trois ans, les pistolets et fusils brouilleurs actuellement employés par les forces de sécurité intérieures comme, ponctuellement par les armées, pourraient se révéler inefficaces contre les drones de dernière génération ; ».* Ce constat est complété des recommandations suivantes *: « Face au rythme débridé de l'évolution des menaces, les rapporteurs appellent de leurs vœux la poursuite « tous azimuts » des expérimentations, à l'instar de celles conduites sur le site de la direction générale de l'armement (…) autour d'une arme laser à énergie dirigée (HELMA-P). A moyen et long termes, les rapporteurs préconisent de soutenir des développements dans le domaine des drones anti-drones, des armes à impulsion*

[286] Rapport enregistré à la présidence de l'Assemblée nationale le 7 juillet 2021, pages 81 et 82

électromagnétique, de l'autonomisation de la lutte anti-drones, des technologiques passives ou encore des radars quantiques. ».

En outre, il s'agit de répondre aux enjeux de protection des sites sensibles existants mais également de préparer les événements majeurs que la France va accueillir dans les mois à venir avec la Coupe du monde de rugby de 2023 et les Jeux olympiques et paralympiques de 2024. D'ailleurs, le rapport précité précise que : « *Sur le territoire français, la lutte anti-drones (LAD) représentera l'un des enjeux majeurs de sécurité nationale au cours des années à venir, notamment dans la perspective de la Coupe du monde de rugby en 2023 et des Jeux olympiques et paralympiques de 2024* ».

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTION ENVISAGEE

Il aurait pu être envisagé d'enrichir les dispositions prévues dans le code des postes et des communications électroniques relatives au brouillage des aéronefs circulant sans personne à bord en énumérant de manière limitative les autres moyens disponibles.

Néanmoins, une telle option figerait pour l'avenir la possibilité de recourir à de nouveaux matériels et de s'appuyer sur les évolutions technologiques. Il apparaît alors plus opportun de se fonder sur un dispositif qui se veut « neutre » d'un point de vue technologique.

3.2. OPTION RETENUE

La mesure envisagée prévoit la possibilité pour les services de l'Etat d'utiliser tout dispositif destiné à rendre inopérant ou à neutraliser un aéronef circulant sans personne à bord qui représente une menace imminente pour l'ordre public, la défense et la sécurité nationales ou le service public de la justice, ou afin de prévenir le survol par un tel aéronef d'une zone interdite.

L'utilisation d'un tel matériel au regard des finalités poursuivies doit être adaptée, nécessaire et proportionnée. Ces conditions de fond sont reprises de l'actuelle rédaction de l'article L. 33-3-1 du code des postes et des communications électroniques. Un décret en Conseil d'Etat précisera les modalités de mise en œuvre des dispositifs de lutte anti-drones malveillants.

A la différence de l'actuel régime juridique limité au seul matériel de brouillage, il est prévu que la liste des dispositifs pouvant être utilisés contre les drones malveillants sera fixée par un arrêté du premier ministre afin de couvrir tous les types de dispositifs techniques (dont le brouillage) qu'ils aient pour effet de faire chuter le drone ou seulement d'altérer sa trajectoire.

Par ailleurs, dans une démarche favorisant l'accessibilité et l'intelligibilité de la norme, il est proposé de prévoir un dispositif législatif unique codifié dans un seul code. Le code de la sécurité intérieure parait être le plus approprié pour accueillir l'ensemble de ces dispositions en

ce qu'il concerne les services de l'Etat concourant à l'ordre public, à la défense et la sécurité nationales ou au service public de la justice afin de protéger les biens et les personnes. Par ailleurs, il peut être relevé que plusieurs articles du code de la sécurité intérieure font état des intérêts de la défense nationale, dont les dispositions prévues à l'article L. 611-3[287] permettant aux agents de sécurité privé de détecter les drones malveillants.

Pour des raisons de coordination rédactionnelle, le présent article supprime le second alinéa du II de l'article L. 33-3-1 du code des postes et des communications électroniques afin de fusionner le contenu de ses dispositions avec les nouvelles dispositions insérées dans le code de la sécurité intérieure.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les nouvelles dispositions sont codifiées dans un nouveau chapitre créé dans le titre Ier (ordre public) du livre II (ordre et sécurité publics) du code de la sécurité intérieure.

Comme évoqué au point précédent, le présent article supprime le second alinéa du II de l'article L. 33-3-1 du code des postes et des communications électroniques pour des raisons de coordination rédactionnelle. Cette suppression n'a pas pour effet de remettre en cause le régime du brouillage de drones malveillants qui est dorénavant fusionné dans le code de la sécurité intérieure.

4.2. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services de l'Etat concernés par la lutte contre les drones représentant une menace sont les services chargés de la sécurité intérieure, de la défense nationale et de la protection des établissements pénitentiaires ou de sites sensibles.

Les services relevant du ministère des armées et du ministère de l'intérieur sont déjà équipés de matériels de détection et de brouillage. Les autres moyens de lutte anti-drones malveillants deviennent progressivement disponibles aujourd'hui et certains d'entre eux pourraient être déployés pour les Jeux olympiques et paralympiques de 2024.

[287] L'article L. 611-3 du code de la sécurité intérieure prévoit que : « Les agents mentionnés à l'article L. 611-1 peuvent utiliser des moyens radioélectriques, électroniques ou numériques permettant la détection, aux abords des biens dont ils ont la garde, des aéronefs circulant sans personne à bord susceptibles de représenter une menace pour la sécurité de ces biens et des personnes qui s'y trouvent. Ils peuvent exploiter et, si besoin, transmettre les informations recueillies aux services de l'Etat concourant à la sécurité intérieure et à la défense nationale. »

Le commandement de la défense aérienne et des opérations aériennes est le service coordonnateur inter armées et interministériel gérant les dispositifs de protection de sûreté aérienne lors des grands événements, ce qui sera le cas également lors des Jeux olympiques et paralympiques de 2024 qui nécessiteront le déploiement de systèmes légers (ex : brouilleur) ou d'un système lourds (radars gonio, vidéos, systèmes de neutralisation).

4.3. IMPACTS SUR LES PARTICULIERS

L'utilisation d'un dispositif rendant inopérant ou neutralisant un aéronef circulant sans personne à bord qui représente une menace restreint le droit pour le télépilote d'utiliser son bien.

Toutefois, cette utilisation ou neutralisation de l'aéronef circulant sans personne à bord a notamment pour finalité de protéger la sécurité des personnes, des sites et des biens.

4.4. IMPACTS ENVIRONNEMENTAUX

Les divers moyens de lutte contre les drones malveillants ne sont la cause directe d'aucun effet sur l'environnement.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions de cet article entrent en vigueur au lendemain de la publication au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Ces dispositions ont vocation à s'appliquer dans les collectivités d'outre-mer régies par l'article 73 de la Constitution du fait du principe d'identité législative sans qu'il soit requis d'en faire mention expresse.

Dans les collectivités d'outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie soumises au régime de spécialité législative, une mention expresse d'application est nécessaire afin de rendre ces dispositions applicables[288].

Par ailleurs, aucune adaptation de ces dispositions tenant aux caractéristiques des collectivités n'apparaît nécessaire.

Ces mesures sont donc applicables sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Un décret en Conseil d'Etat devra fixer les modalités de mise en œuvre des dispositifs rendant inopérant ou neutralisant les aéronefs circulant sans personne à bord présentant une menace. Un arrêté du Premier ministre fixera la liste des dispositifs pouvant être utilisés par les services de l'Etat pour lutter contre ces aéronefs.

[288] Cf. article 7 de la loi organique n° 2004-192 du 27 février 2004 pour la Polynésie Française ; article 4 de la loi n° 61-814 du 29 juillet 1961 pour les îles Wallis et Futuna ; article 6-2 de la loi n° 99-209 organique du 19 mars 1999 pour la Nouvelle-Calédonie ; article 1-1 de la loi n° 55-1052 du 6 août 1955 pour les Terres australes et antarctiques françaises.

Article 28 : Ratification de l'ordonnance en matière spatiale – Prendre en compte, dans la loi sur les opérations spatiales, les constellations de satellites en les subordonnant au même régime que les objets spatiaux ainsi que la récupération d'étage de lanceur

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

La loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales (ci-après désignée « LOS ») a été adoptée afin de répondre à des besoins créés par l'évolution du secteur spatial et de ses acteurs en France.

La France est incontestablement une nation spatiale en ce qu'elle dispose de toutes les composantes pour exceller dans ce domaine : un port spatial[289], des industriels spécialisés dans la conception et fabrication de systèmes de lancement et de systèmes orbitaux ainsi que des fournisseurs de services fondés sur l'exploitation des données obtenues *via* les satellites. Jusqu'à la fin des années 1990, l'ensemble des activités spatiales étaient placées sous le contrôle de l'Etat, par le biais d'un nombre restreint d'entités qui étaient soit ses émanations (tel que le Centre national d'études spatiale – ci-après CNES) soit sous son contrôle direct ou indirect (tel que Arianespace). Dès lors, aucune législation sur les opérations spatiales n'était nécessaire puisque tout passait par des instructions gouvernementales. Cependant, à partir de la fin des années 1990, le paysage spatial a lentement mué et s'est ouvert à de nouveaux acteurs, du fait des privatisations et filialisations successives. L'adoption d'une loi spécifique pour encadrer leurs activités était alors nécessaire.

C'est dans ce contexte changeant que la LOS a été élaborée, afin de répondre à un triple objectif. Il s'agissait d'abord pour la France d'honorer ses engagements internationaux[290]. En effet, ces traités pouvant entraîner l'engagement de la responsabilité de la France[291] en cas de dommage

[289] Le centre spatial guyanais de Kourou.

[290] Traité du 27 janvier 1967 sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la lune et les autres corps célestes ; Accord du 22 avril 1968 sur le sauvetage des astronautes, le retour des astronautes et la restitution des objets lancés dans l'espace extra-atmosphérique ; Convention du 29 mars 1972 sur la responsabilité internationale pour les dommages causés par les objets spatiaux ; Convention du 14 janvier 1975 sur l'immatriculation des objets lancés dans l'espace extra-atmosphérique ; Accord du 18 décembre 1979 régissant les activités des États sur la Lune et les autres corps célestes, signé par la France mais non ratifié. Textes disponibles sur le lien suivant : 02-57670_F_c1-4 (unoosa.org).

[291] L'article 6 du Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la lune et les autres corps célestes prévoit que chaque Etat est responsable de ses activités et celles de ses nationaux. L'article 7 du même Traité précise que chaque Etat de lancement est responsable de réparer les dommages qu'il ou ses nationaux causent. A ce titre, l'Etat de la victime peut demander la totalité de la réparation à l'Etat qui cause le dommage.

causés par des objets spatiaux[292], il était nécessaire d'organiser la responsabilité des acteurs du secteur spatial français, tout en les sécurisant. Ensuite, la LOS garantit un niveau élevé de sécurité, que ce soit pour les biens, les personnes et l'environnement face aux risques générés par les activités spatiales[293]. Enfin, elle établit un régime assurant la viabilité à long terme des activités spatiales, notamment en imposant des règles limitant la création et la prolifération de débris dans l'espace[294].

Afin de répondre aux objectifs énoncés ci-dessus, la LOS a mis en place un régime d'autorisation préalable des activités spatiales. Il prévoit que tout opérateur français[295], qui souhaite procéder ou faire procéder à un lancement, depuis le territoire français ou depuis le territoire d'un autre Etat, ou qui souhaite assurer la maitrise en orbite d'un objet spatial doit obtenir au préalable une autorisation de la part du ministère en charge de l'espace. Sont exemptés de ce régime d'autorisation le CNES, lorsqu'il agit dans le cadre de ses missions institutionnelles[296], et l'Etat lorsqu'il conduit ces opérations dans l'intérêt de la défense nationale. Ces autorisations sont instruites et délivrées gratuitement aux opérateurs[297].

En plus de créer un régime d'autorisation des opérations spatiales, la LOS a également :

- Mis en place un registre national d'immatriculation, tenu par le CNES et permettant à l'Etat de suivre l'ensemble de la flotte satellitaire française et ainsi de répondre à ses engagements internationaux ;

- Établi le régime de responsabilité applicable aux opérations spatiales, notamment pour les dommages causés aux tiers ;

- Mis en place un régime de déclaration de leurs activités pour les exploitants primaires de données d'origine spatiale ;

- Conféré, par modification du code de la recherche[298], au Président du CNES des pouvoirs de police administrative spéciale pour l'exploitation des installations du Centre Spatial Guyanais (ci-après désigné « CSG ») et, à ce titre, une mission générale de sauvegarde consistant à maîtriser les risques techniques liés à la préparation et à la réalisation des lancements à partir du CSG afin d'assurer la protection des personnes, des biens, de la santé publique et de l'environnement, au sol et en vol.

[292] Il s'agit de tout objet se trouvant dans l'espace extra-atmosphérique tel que les satellites ou étages de lanceurs.

[293] La LOS reprend les principes de responsabilité figurant dans les traités internationaux et prévoit que l'opérateur spatial est responsable sans faute pour tout dommage qui serait causé au sol ou dans l'espace aérien. En cela, ce régime est particulièrement protecteur.

[294] En 2008, le CNES estimait à 300 000 le nombre de débris de plus d'1cm et à 30 millions ceux de plus d'1mm.

[295] Entreprises de toute taille (y compris startups, PME), universités.

[296] Article L. 331-2 du code de la recherche.

[297] Cf. tableau 2 s'agissant des opérations réalisées.

[298] Articles L. 331-6 à L. 331-8 du code de la recherche.

La loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales, a été complétée par plusieurs textes d'application visant à permettre sa mise en œuvre (v. schéma ci-dessous).

Les textes d'application ont vocation à traiter de trois thématiques :

- Le régime d'autorisation préalable des opérations spatiales ;
- L'attribution de missions au CNES ;
- Le régime de déclaration préalable pour l'exploitation des données d'origine spatiale.

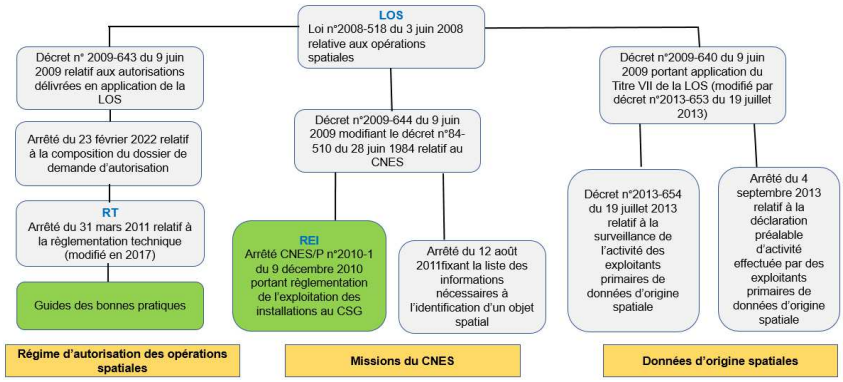


Schéma 1 – Corpus des textes juridiques applicables aux activités spatiales françaises

L'ordonnance n° 2022-232 du 23 février 2022 relative à la protection des intérêts de la défense nationale dans la conduite des opérations spatiales et l'exploitation des données d'origine spatiale[299] a conduit à une modification de la LOS visant à prendre en compte les intérêts de la défense nationale dans le cadre des opérations spatiales, notamment en exemptant l'Etat du régime d'autorisation préalable pour les opérations spatiales qu'il conduit dans l'intérêt de la défense nationale et en renforçant le contrôle du respect des intérêts de la défense nationale lors de la délivrance d'autorisation d'opérations spatiales. Par ailleurs, un régime de réquisitions spatiales spécifique a été adopté.

Bien qu'un projet de loi de ratification ait été déposé devant le Sénat le 16 mars 2022, cette ordonnance n'a jamais été formellement ratifiée.

Evolution du secteur spatial français depuis 2008

L'arrivée du *New Space*[300], dès le milieu des années 2000, marque un tournant majeur dans l'écosystème spatial en ce que des entreprises privées, majoritairement américaines et non

[299] Adoptée sur le fondement de l'habilitation prévue par l'article 44 de la loi n° 2020-1674 du 24 décembre 2020 de programmation de la recherche pour les années 2021 à 2030 et portant diverses dispositions relatives à la recherche et à l'enseignement supérieur.

[300] Nouveaux modèles économiques prônant agilité et innovation émergent du secteur privé dans le domaine spatial.

nécessairement issues du secteur spatial, parviennent à financer des solutions innovantes et à bas coût qui font entrer le secteur spatial dans une ère particulièrement concurrentielle.

Ainsi, l'accès à l'espace se privatise et le secteur spatial n'est plus un domaine réservé aux spécialistes mais est désormais ouvert à de nouveaux acteurs. Issus de l'industrie du numérique, du *big data* ou de l'aéronautique, ces derniers étendent le champ d'application des technologies spatiales[301] et imposent une vision commerciale tournée vers les besoins du client et des utilisateurs de la donnée spatiale[302].

En conséquence, on constate non seulement une augmentation significative du nombre d'opérateurs (Tableau 1 ci-dessous) et d'opérations soumises à autorisation au titre de la LOS (Tableau 2 ci-dessous), mais aussi une évolution des activités (e.g. service en orbite et constellation) et des technologies spatiales (e.g. lanceur réutilisable). A cet égard, la loi doit s'adapter à ces évolutions afin de rester suffisamment couvrante et cohérente, et de rester un outil efficace pour assurer un développement durable de l'activité spatiale en France tout en garantissant la sécurité des personnes, des biens et la préservation de l'environnement lors de toute opération spatiale. En effet, la LOS est devenue au fil de sa mise en œuvre un outil de *soft-power*, servant de référence dans les *fora* européens et internationaux traitant notamment des nouveaux enjeux du secteur spatial (e.g. CUPEEA, IADC, ISO).

Tableau 1 : Evolution du nombre d'opérateurs LOS de 2008 à 2022

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Nombre d'opérateurs de satellite			1	3	4	4	5	5	5	6	7	8	9	10	11
Nombre d'opérateurs de lancement	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Tableau 2 : Evolution du nombre de satellites et de lanceurs autorisés entre 2008 et 2022

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Nombre d'autorisations de maîtrise en orbite accordées			2	39	5	4	5	2	7	6	7	10	11	12	13

[301] Internet dans les transports, IoT, etc.

[302] Client et utilisateur pour de l'habitat connecté, opérateurs de téléphonie mobile per exemple. Plus largement, tous les services qui utilisent les données spatiales de type télécom, imagerie, positionnement.

Nombre d'autorisations de lancement accordées			6	7	10	7	11	12	11	11	11	9	7	7	6

L'évolution des technologies et le développement de nouveaux modes d'activités spatiales (constellations de satellites, émergence des lanceurs réutilisables) nécessitent d'adapter le texte de la LOS afin de pouvoir encadrer ces dernières sans les entraver.

Enfin, une modification du code de la recherche est nécessaire afin d'étendre les pouvoirs de police spéciale du président du Centre national d'études spatiales (CNES) à la maîtrise des risques techniques liés à la préparation et à la réalisation de l'ensemble des opérations spatiales exercées au Centre spatial guyanais (CSG) de Kourou et non plus des seuls « lancements ». Le terme « lancement » est en effet trop restrictif et ne permet pas de contrôler certaines opérations, telles que les retours d'étages des lanceurs ou de modules spatiaux.

1.2. CADRE CONSTITUTIONNEL

L'objectif est d'étendre l'encadrement et le contrôle d'un secteur économique. Conformément à l'article 34 de la Constitution, un tel objectif, qui est susceptible de constituer une atteinte à la liberté d'entreprendre, ne peut être réalisé que par la loi. Selon une jurisprudence constante du Conseil constitutionnel, il est loisible au législateur d'apporter à cette liberté des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte par d'atteintes disproportionnées au regard de l'objectif poursuivi[303].

Les dispositions en cause répondent d'une part à la poursuite d'un intérêt général (contrôler des activités en expansion) et, d'autre part, permettront de simplifier les démarches réclamées aux opérateurs, tout en sécurisant leurs activités (cf. *infra*).

Au regard des conventions internationales régissant le domaine spatial, les dommages causés par un opérateur privé sont considérés comme étant à la charge de l'Etat de lancement. Le contrôle de ces activités, par un système d'autorisation, répond à l'exigence de bon usage des deniers publics[304]. La nécessité du recours à la loi en 2008 impose, en raison du parallélisme des formes et des compétences, de recourir à un vecteur de même nature pour apporter des ajustements à cette législation (cf. rubrique 2.1).

1.3. CADRE CONVENTIONNEL

Cadre juridique onusien – Le droit international de l'espace est aujourd'hui régi par cinq traités internationaux, adoptés sous l'égide de l'Organisation des Nations Unies :

[303] CC, décision n° 2010-89 QPC, 21 janvier 2011, *Société Chaud Colatine*.

[304] CC, décision 2006-545 DC, 28 décembre 2006.

- Traité du 27 janvier 1967 sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la lune et les autres corps célestes ; entré en vigueur pour la France le 5 août 1970 ;
- Accord du 22 avril 1968 sur le sauvetage des astronautes, le retour des astronautes et la restitution des objets lancés dans l'espace extra-atmosphérique ; entré en vigueur pour la France le 31 décembre 1975 ;
- Convention du 29 mars 1972 sur la responsabilité internationale pour les dommages causés par les objets spatiaux ; entré en vigueur pour la France le 31 décembre 1975 ;
- Convention du 14 janvier 1975 sur l'immatriculation des objets lancés dans l'espace extra-atmosphérique ; entré en vigueur pour la France le 15 septembre 1976 ;
- Accord du 18 décembre 1979 régissant les activités des États sur la Lune et les autres corps célestes ; signé par la France le 29 janvier 1980 mais non ratifié.

Hormis le cas de l'Accord sur la Lune, les traités ont été largement ratifiés, notamment par les autres puissances spatiales.

Le Traité de 1967 pose le cadre général que les traités postérieurs viennent préciser. Sont notamment énoncés :

- Le principe de liberté d'exploration et d'utilisation de l'espace extra-atmosphérique (article I^{er} du Traité de l'espace) ;
- Le principe de non appropriation (Article II du Traité de l'espace) ;
- Le principe d'utilisation pacifique de l'espace extra-atmosphérique (Article IV du Traité de l'espace) ;
- Le principe de responsabilité internationale (*responsibility*) des Etats pour les activités de leurs nationaux (Article VI du Traité de l'espace) et le principe de responsabilité internationale (*liability*) des Etats de lancement pour dommages causés (Article VII du Traité de l'espace et Convention de 1972 sur la responsabilité) ;
- Le principe d'autorisation et de surveillance continue par les Etats des activités de leurs nationaux (Article VI du Traité de l'espace) ;
- L'obligation de mettre en place un registre national d'immatriculation (Article VIII du Traité de l'espace et Convention de 1975 sur l'immatriculation).

En ayant adopté une loi sur les opérations spatiales, la France répond :

- D'une part, aux obligations issues de ces traités, et en particulier à l'obligation d'autorisation et de surveillance des activités de ses nationaux ;
- D'autre part, organise la responsabilité des acteurs du secteur spatial français, dont les activités sont susceptibles d'entrainer la mise en jeu de la responsabilité de la France au niveau international.

Cadre européen – Le cadre européen du domaine spatial s'articule autour de deux acteurs : l'Union européenne (ci-après désignée « UE ») et l'Agence spatiale européenne (ci-après désignée « ESA »).

L'UE ne dispose que d'une compétence partagée restreinte en matière spatiale. L'article 189 du Traité sur le Fonctionnement de l'Union européenne précise que l'UE « *peut promouvoir des initiatives communes, soutenir la recherche et le développement technologique et coordonner les efforts nécessaires pour l'exploration et l'utilisation de l'espace*. ». Pour cela, elle peut entreprendre des programmes spatiaux, mais ne peut pas procéder à l'harmonisation des dispositions législatives et réglementaires des Etats membres. L'UE pourrait toutefois s'appuyer sur ses compétences en matière de marché intérieur pour légiférer sur les services offerts par des infrastructures spatiales.

L'ESA est régie par la Convention portant création d'une Agence spatiale européenne, entrée en vigueur en 1980. L'ESA conclue des accords avec des entités étatiques ou non afin de mettre en œuvre des programmes spatiaux (scientifiques ou industriels) ou pour promouvoir le spatial en Europe (notamment à travers le financement et la participation de l'ESA à certaines structures pédagogiques ou de recherche). L'ESA n'adopte pas de règles relatives au contrôle des opérations spatiales.

1.4. ÉLEMENTS DE DROIT COMPARE

D'autres puissances spatiales ont adopté des législations réglementant les activités de lancement ou de conduites d'opérations dans l'espace.

Le *Space Industry Act* britannique, du 15 mars 2018, utilise un vocabulaire moins restrictif que la loi sur les opérations spatiales françaises. Ainsi, le point 5 de l'article 12 définit le lancement comme une ou plusieurs activités spatiales impliquant le lancement d'un objet spatial. Par ailleurs, la délivrance d'une licence peut être attachée à une activité spatiale qui ne se limite pas nécessairement au lancement et à la maîtrise d'un seul objet spatial, sans toutefois que la notion de constellation ou de groupe de satellites ne soit évoquée (points 5 et 6 de l'article 12).

Le *Commercial Space Launch Activities Act*, adopté par les États-Unis, prévoit un mécanisme de permis spécifique visant les lanceurs réutilisables. Ce permis spécifique présente les mêmes caractéristiques que celui accordé à un lanceur non réutilisable et est considéré comme une licence ordinaire permettant un lancement spatial (§50906). Les États-Unis autorisent déjà l'utilisation de lanceurs réutilisables (par exemple les Falcon 9 de *Space X*).

La législation américaine ne prévoit pas de dispositions spécifiques relatives aux constellations de satellites, mais ne restreint pas non plus les autorisations délivrées par les autorités à une seule opération spatiale.

Enfin, à titre d'exemple, le *Outer Space and High Altitude activities Bill* néo-zélandais de 2017 n'envisage qu'une autorisation globale couvrant différentes activités relatives à un ou plusieurs lancements, pour une durée de cinq ans renouvelable.

Ainsi, le Royaume-Uni et les Etats-Unis ont autorisé le déploiement de premières constellations de satellites (constellation *Oneweb* comportant 648 satellites pour le Royaume-Uni et *Starlink*, de 12 000 satellites aux Etats-Unis).

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le dynamisme des initiatives spatiales de ces dix dernières années, particulièrement aux Etats-Unis avec des investisseurs américains privés liés, pour bonne partie d'entre eux, au marché du numérique (communication, géolocalisation…) appelle une vigilance renforcée quant à l'utilisation et l'exploitation de l'espace.

Dans ce contexte, des initiatives françaises émergent également et bousculent le cadre législatif et réglementaire applicable, tant sur le plan des systèmes orbitaux (constellations) que sur le plan des systèmes de lancements (lanceurs réutilisables). Face à ces évolutions, le cadre existant doit être adapté à ces nouvelles activités afin d'en permettre un développement pérenne et d'optimiser l'instruction des autorisations au titre de la LOS. En effet, la LOS, dans sa version initiale avait été pensée pour des lanceurs non réutilisables de type Ariane5 et pour des opérations de maîtrise de satellite unique.

L'intégration de nouvelles notions (éléments réutilisables du lanceur et groupe d'objets spatiaux coordonnés) ne peut cependant être effectuée simplement au niveau réglementaire : d'une part, la LOS comprend un article relatif aux définitions qui sera modifié ; d'autre part, le champ des autorisations, qui est définit par la loi, sera lui aussi adapté (cf. rubriques 3.1 et 3.2).

Pour l'accès à l'espace (lanceurs), il s'agit de prendre en compte les futurs lanceurs récupérables, dont les 'briques de base' font l'objet de développements en coopération internationale et qui arriveront sur le marché avant la fin de la décennie.

Pour les **opérations de maitrise en orbite**, il s'agit de prendre en compte les constellations (notamment en orbite basse) qui peuvent comporter plusieurs centaines voire milliers de satellites.

Concernant les « groupes d'objets spatiaux coordonnés » (constellations)

La version actuelle de la LOS, qui ne prévoit que la maîtrise d'un seul objet spatial en orbite, ne prévoit pas d'autorisation de maitrise pour un groupe d'objets spatiaux entendu comme un système unique. Elle ne permet donc pas d'imposer des exigences techniques à une constellation dans son ensemble, telles que des exigences relatives à la coordination des satellites composant la constellation, soit de manière autonome soit en passant par le sol. Ces dernières ne peuvent être imposées qu'individuellement, satellite par satellite. De plus, l'état actuel de la réglementation fait potentiellement peser une charge administrative extrêmement importante sur les industriels et l'administration en cas de lancement de constellation

comportant plusieurs dizaines, voire plusieurs centaines de satellites. Une évolution de la LOS permettra d'alléger la charge administrative pesant sur les différents acteurs, sans pour autant porter atteinte à la sécurité des personnes et des biens.

Concernant la récupération des éléments de lanceurs réutilisables :

La version actuelle de la LOS, et en particulier le régime de responsabilité qu'elle met en œuvre, se réfère aux notions de « phase de lancement » et de « phase de maitrise ». La définition de « phase de lancement » actuellement prévue dans la LOS est la suivante : *« période de temps qui, dans le cadre d'une opération spatiale, débute à l'instant où les opérations de lancement deviennent irréversibles et qui, sous réserve des dispositions contenues, le cas échéant, dans l'autorisation délivrée en application de la présente loi, s'achève à la séparation du lanceur et de l'objet destiné à être placé dans l'espace extra-atmosphérique* ». La loi n'identifie pas clairement si la récupération des éléments de lanceur réutilisable s'insère ou non dans la phase de lancement. Dans un domaine où le risque de contentieux est élevé en cas de dommages ou de victimes, une clarification des activités autorisées par la LOS est donc nécessaire.

In fine, une mise à jour de la LOS permettrait d'accompagner les opérateurs mettant en œuvre ces nouvelles activités spatiales en leur donnant un cadre légal et réglementaire lisible et stable, nécessaire à la pérennité de ces dernières. La démarche de mise à jour de la LOS est en effet menée avec le souci constant que les opérateurs français puissent développer leur modèle d'affaire dans un contexte juridiquement maitrisé afin de rester compétitifs.

2.2. OBJECTIFS POURSUIVIS

Introduction de la notion de « groupe d'objets spatiaux coordonnés »

Les projets de (méga)constellations en orbite basse fleurissent depuis plus de dix ans, aux Etats-Unis (Starlinks), en Chine, en Russie et avec des *consortia* internationaux, tels que ONEWEB dont la génération 2 impliquera l'opérateur Français Eutelsat. L'Union européenne va se doter de la constellation Iris2 et la constellation française Kinéis devrait se déployer d'ici un an.

L'objectif poursuivi, en introduisant cette notion dans la LOS, est d'accompagner ces développements du *Newspace* en permettant, notamment, l'adoption de nouvelles prescriptions règlementaires visant à assurer une meilleure coordination entre les activités spatiales. Cette coordination vise notamment à réduire le risque de collisions et ainsi à assurer la viabilité à long terme des activités spatiales.

Désormais, un groupe d'objets spatiaux coordonnés sera considéré, pour les procédures administratives de délivrance des autorisations de lancement ou de maîtrise, comme un satellite unique : l'industriel n'aura pas besoin de déposer une demande d'autorisation de lancement satellite par satellite.

Etages récupérables des lanceurs

L'introduction de la notion de récupération au sol d'un étage de véhicule après tentative de lancement dans la LOS est cohérente avec l'évolution technologique dans la conception des lanceurs. La clarification du périmètre de la phase de lancement va permettre d'assurer l'application du régime de responsabilité prévu dans la LOS à la phase de récupération des étages réutilisables de lanceur.

En apportant cette clarification, la modification de la LOS vise à offrir un cadre juridique certain pour ces activités. A ce titre, elle apporte une sécurité juridique aux opérateurs européens et notamment français, qui devrait leur permettre de développer leurs activités face une concurrence américaine (Space X) particulièrement agressive. Même si le modèle économique de tels concepts n'est pas consolidé, l'approche récupérable plutôt que consommable semble, dans le contexte actuel du développement durable terrestre, incontournable.

Enfin, l'extension des pouvoirs de contrôle du président du CNES à l'ensemble des opérations spatiales menées depuis le CSG de Kourou constitue non seulement une mesure de coordination avec les évolutions explicitées ci-dessus, mais permettra ainsi de couvrir l'ensemble des activités spatiales se déroulant au CSG (y compris les retours sur site d'objets spatiaux).

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Introduction de la notion de « groupe d'objets spatiaux coordonnés » :

Deux options, n'impliquant pas de modification de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales, ont été envisagées mais écartées :

Option 1 : Application du régime d'autorisation préalable des opérations spatiales existant à chaque satellite d'une constellation et modification de la règlementation technique uniquement

Le 3° de l'article 2 de la loi relative aux opérations spatiale dispose que « *Doit préalablement obtenir une autorisation délivrée par l'autorité administrative […] tout opérateur français qui entend assurer la maitrise d'un tel objet [objet spatial] pendant son séjour dans l'espace extra-atmosphérique* ».

L'une des options envisagées consistait à traiter le cas des constellations non pas comme un groupe d'objets spatiaux, mais de traiter chaque satellite d'une constellation de façon individuelle, c'est-à-dire d'appliquer à ces nouvelles technologies la norme actuelle, sans la faire évoluer. Dans cette hypothèse, un opérateur français souhaitant assurer la maitrise d'une constellation devrait demander autant d'autorisations de maitrise en orbite que de satellites composant sa constellation. Par conséquent, chaque opération de maitrise d'un satellite d'une constellation serait alors traitée indépendamment des opérations des autres satellites.

L'avantage d'une telle option était qu'elle pouvait être mise en œuvre sans modification de la loi relative aux opérations spatiales. Toutefois, afin de prendre en compte les problématiques associées aux constellations, il était alors envisagé de mettre à jour les arrêtés définissant la règlementation technique pour y ajouter des exigences techniques spécifiques pour des satellites faisant partie d'une constellation, comme par exemple imposer une capacité de manœuvre d'évitement de collision, exigences visant à limiter les perturbations optiques.

Cette option n'a pas été retenue car elle présentait deux difficultés majeures :

- La première, et principale, difficulté est liée à l'absence d'analyse globale de la constellation et des conséquences que pourrait avoir ce type d'activité sur l'environnement spatial. En effet, cette option ne permettait pas, notamment :

    - De prendre en compte l'effet de nombre, inhérent à une constellation, dans les calculs de probabilités réalisés dans le cadre de l'analyse de conformité technique, tels que le calcul de probabilité de faire une victime au sol ou encore de réaliser avec succès le retrait de service de l'ensemble des satellites de la constellation ;
    - D'imposer des exigences techniques relatives à la géométrie de la constellation, en vue notamment de réduire le risque de collisions en orbite entre les satellites d'une même constellation ;
    - D'avoir une vue d'ensemble sur la mission et la capacité de la constellation ;
    - De lier les satellites d'une constellation entre eux. Dans l'hypothèse où une anomalie serait identifiée sur un satellite de la constellation, d'en tirer des conséquences pour les autres satellites de la constellation pouvant être également affectés par cette anomalie qui auraient déjà été autorisés.

- La seconde difficulté est liée aux lourdeurs administratives induites par cette option. En effet, une telle option impliquait mécaniquement le dépôt d'un nombre significatif de demandes d'autorisation par l'opérateur concerné. Ces lourdeurs pèseraient à la fois sur l'opérateur (constitution des dossiers) et sur les services de l'Etat en charge du traitement des demandes (ministère concerné, CNES). Il convient de considérer que, même si, dans le cadre de satellites similaires d'une constellation le temps d'analyse des dossiers pourrait être réduit par rapport aux dossiers actuellement traités, une telle procédure ne contribuerait pas à la simplification des démarches auprès des administrations et manquerait d'optimisation.

Option 2 : Utilisation du mécanisme de licences pour les constellations et modification de la règlementation technique uniquement (écartée)

L'alinéa 2 de l'article 4 de la LOS dispose que « *Des licences attestant, pour une durée déterminée, qu'un opérateur spatial justifie des garanties morales, financières et professionnelles peuvent être délivrées par l'autorité administrative compétente en matière*

d'autorisations. Ces licences peuvent également attester de la conformité des systèmes et procédures mentionnées au premier alinéa avec la règlementation technique édictée. Elles peuvent enfin valoir autorisation pour certaines opérations ».

Il a été envisagé d'utiliser le mécanisme de licence valant autorisation afin d'éviter à l'opérateur de devoir demander une autorisation de maitrise en orbite pour chaque satellite identique de sa constellation. Dans cette hypothèse, tout comme dans l'option 1, il était possible de modifier la règlementation technique pour ajouter des exigences spécifiques applicables à chaque satellite d'une constellation.

Les licences valant autorisation permettent à un opérateur de réaliser, pendant une période déterminée (dix ans maximum), autant d'opérations identiques qu'il le souhaite sur simple information préalable de l'autorité administrative. Ces licences ne peuvent être accordées que pour des opérations de maitrise en orbite, à l'exclusion des opérations de lancements. Actuellement deux licences de ce type sont en cours et concernent des opérations réalisées par des plateformes identifiées, en orbite géostationnaire.

Si cette option apporte une solution au problème de la multiplication des demandes d'autorisation de maitrise en orbite de satellites et aux lourdeurs administratives que cela entraine, elle se heurte à la même difficulté que l'option 1 en ne permettant pas de prendre en compte les constellations dans leur globalité. En effet, une licence permet seulement de s'affranchir du processus d'autorisation préalable. Cette option ne permet donc pas davantage de répondre au besoin de réaliser une analyse globale des activités des constellations et de prendre en compte l'effet de nombre.

De plus, dans la mesure où une licence ne limite pas le nombre d'opérations pouvant être réalisées par l'opérateur, l'autorité administrative, une fois la licence accordée, n'a, *in fine*, plus de maitrise sur le nombre de satellites lancés. Or, dans le cadre des constellations, ce nombre peut être très important. A cet égard, si ce risque est relativement limité pour les satellites géostationnaires – compte tenu du coût associé à ce type d'opération – il l'est moins s'agissant de petits satellites, tels que ceux généralement utilisés dans le cadre des constellations.

Tout comme la première option, cette option 2 a donc été jugée comme apportant une réponse insuffisante aux problématiques liées aux constellations.

Etage récupérable des lanceurs

Sur ce sujet, l'objectif était de clarifier la notion de « phase de lancement » afin de préciser qu'elle intègre la récupération des étages de lanceurs. Aucune autre option que la modification de la loi n'était envisageable.

3.2. OPTION RETENUE

Introduction de la notion de « groupe d'objets spatiaux coordonnés » :

L'option retenue vise à considérer que la maitrise d'un groupe d'objets spatiaux coordonnés constitue une opération spatiale en tant que telle et doit, par conséquent, faire l'objet d'une seule autorisation de maitrise en orbite couvrant l'ensemble des opérations réalisées par les satellites qui la compose.

Dès lors, et afin de soumettre la maitrise de ce groupe d'objets spatiaux à autorisation, il est nécessaire de modifier la définition d'opération spatiale afin de l'étendre à la maitrise d'un groupe d'objet spatiaux coordonné, et non plus seulement à la maitrise d'un objet spatial.

Cependant, au titre de la responsabilité, chaque satellite faisant partie d'une constellation sera toujours considéré comme un objet spatial particulier. Ceci justifie que les modifications apportées à la LOS ne concernent que les parties du texte relatives aux autorisations ou aux transferts de maîtrise et non celles relatives à la responsabilité ou l'indemnisation de dommages.

Etage récupérable des lanceurs

L'option retenue a consisté en la modification de la définition de « phase de lancement » au 4° de l'article 1er de la LOS pour indiquer que la récupération des éléments de lanceurs réutilisables fait partie intégrante de la phase de lancement.

La définition, ainsi complétée sera la suivante : « *Phase de lancement : la période de temps qui, dans le cadre d'une opération spatiale, débute à l'instant où les opérations de lancement deviennent irréversibles et qui, sous réserve des dispositions contenues, le cas échéant, dans l'autorisation délivrée en application de la présente loi, s'achève à la séparation du lanceur et de l'objet destiné à être placé dans l'espace extra-atmosphérique.* ***La phase de lancement comprend, le cas échéant, la récupération des éléments réutilisables du lanceur*** ».

Cette précision permet de confirmer l'application des articles 14 et 15 de la LOS sur le régime de responsabilité vis-à-vis des tiers, aux cas de dommages causés pendant la récupération de ces éléments.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les modifications apportées à la loi relative aux opérations spatiales et décrites *supra* au 3.2 (introduction de la notion de « groupe d'objets spatiaux coordonnés » et complément apporté à la définition de la phase de lancement pour y introduire la notion de récupération d'élément de lanceur) concernent ses articles 1 (Définitions) 2 (Autorisations), 3, 4, 7, 8, 9, 11, 11-1 et 20-1 (pour introduire, par cohérence, la notion de groupe d'objets spatiaux coordonnés).

Par ailleurs, l'article L. 331-6 du code de la recherche est modifié.

Ces dispositions n'entraînent pas d'impact majeur sur l'ordre juridique interne ; seuls les textes d'application de cette loi doivent être modifiés.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les présentes dispositions visent à permettre à la France de faire évoluer son régime d'autorisation préalable des opérations spatiales pour l'améliorer et répondre de façon plus complète et plus adaptée au principe d'autorisation et de surveillance continue des activités spatiales de leurs nationaux tel que prévu à l'article VI du Traité de l'Espace.

Dans la mesure où il n'existe pas aujourd'hui de cadre européen encadrant les opérations spatiales et que la compétence de l'UE s'exerce à l'exclusion d'une harmonisation des cadres législatifs et règlementaires des Etats membres, la modification de la LOS n'entraînera aucun impact sur le respect par la France de ses obligations internationales.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Les présentes évolutions de la LOS visent à apporter un cadre législatif adéquat et stable pour de nouvelles activités spatiales (constellation, lanceurs réutilisables) et ainsi à offrir aux opérateurs une sécurité juridique leur permettant de développer leurs activités en la matière. En effet, l'absence de cadre législatif pour encadrer ces initiatives pourrait avoir pour effet de conduire les sociétés concernées à se tourner vers d'autres pays pour opérer leurs lanceurs ou satellites.

En proposant un cadre juridique adapté, la France pourrait encourager les entreprises françaises à s'engager dans ces activités. Cela devrait stimuler l'innovation, portée en particulier par des acteurs émergents, et *in fine* permettre le développement de nouveaux services fournis depuis l'espace au bénéfice des entreprises, citoyens et institutions (IoT par exemple).

4.2.2. Impacts sur les entreprises

Les dispositions introduites au travers de cette évolution de la LOS n'imposent, *in fine*, pas de nouvelles obligations aux opérateurs concernés. Elles visent, au contraire, à simplifier et élargir le cadre juridique applicable aux constellations et à la récupération d'étages réutilisables. Dès lors, elles conduisent à un renforcement certain de la compétitivité des entreprises françaises et à favoriser l'investissement de ces dernières sur ces thématiques.

L'impact des modifications proposées sera le même pour tous les opérateurs concernés, considérant que seuls le CNES et l'Etat lorsqu'il conduit des opérations spatiales dans l'intérêt de la défense nationale sont exemptés du régime d'autorisation.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La simplification de la procédure d'autorisation pour les constellations de satellites, en consacrant le principe d'une autorisation unique pour ces constellations, permettra de contenir l'activité des services en charge de l'instruction des demandes et de la délivrance des autorisations. Comme explicité *supra*, ces constellations peuvent regrouper un très grand nombre d'objets spatiaux, qui, selon la législation actuellement en vigueur, doivent chacun faire l'objet d'autorisation. Regrouper ces autorisations au sein d'une autorisation unique permettra de décharger l'activité de ces services, de leur permettre d'étudier les systèmes de constellation dans leur globalité, et, par conséquent, d'offrir de meilleures garanties quant à l'étude de ces demandes.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Les présentes dispositions relatives aux constellations permettront aux opérateurs de proposer un accès démocratisé à la connectivité (Internet, objets connectés) et, ainsi, de réduire la fracture numérique. Indirectement, la révision de la LOS renforcera l'accès à l'information pour les sociétés.

Si le déploiement de constellations peut avoir des effets sur l'environnement (pollution lumineuse, risque de congestion en orbite), les modifications législatives proposées visent à assurer une meilleure sécurité de ces opérations afin de mieux protéger l'environnement spatial *via* la prévention de la création de débris notamment par mise en place de règles pour limiter les risques de collision.

Enfin, en offrant de la visibilité aux opérateurs de lancement sur le cadre d'exploitation de lanceurs réutilisables, la mesure proposée permettra de stimuler le développement de tels lanceurs dont l'impact sur l'environnement est plus réduit.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

La notion *d'étage récupérabl*e permettra à l'industrie spatial de limiter ses atteintes à l'environnement puisque les étages récupérés seront réutilisés plusieurs fois. D'autre part, l'application de la loi aux nouvelles opérations de retour des lanceurs réutilisables permettra d'assurer leur innocuité environnementale.

Par ailleurs, l'introduction de la notion de constellation permettra, dans les textes d'application de la LOS, de proposer un cadre afin de limiter les effets cumulés des satellites de cette constellation.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les modifications des dispositions de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales entreront en vigueur au lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les domaines auxquels se rapportent les présentes dispositions (l'espace et la recherche) relèvent de dispositions dites « de souveraineté ». Dès lors, aucune mention d'extension ou d'application expresse dans les collectivités d'outre-mer n'est nécessaire.

5.2.3. Textes d'application

Il est prévu d'adapter les textes de mise en œuvre suivants :

- Décret n° 2009-643 du 9 juin 2009 modifié relatif aux autorisations délivrée en application de la loi n°2008-518 du 3 juin 2008 relative aux opérations spatiales : afin de clarifier les éventuelles spécificités procédurales associées aux autorisations de maitrise d'un groupe d'objets spatiaux coordonnés ;

- L'arrêté du 23 février 2022 relatif à la composition des trois parties du dossier mentionné à l'article 1er du décret n° 2009-643 du 9 juin 2009 relatif aux autorisations délivrées en application de la loi n° 2008-518 du 3 juin 2008 modifiée relative aux opérations spatiales : afin de compléter la liste des fournitures documentaires attendues conformément aux besoins de l'analyse technique pour les constellations et pour les étages de lanceurs réutilisables ;
- L'arrêté du 31 mars 2011, modifié, relatif à la règlementation technique en application du décret n° 2009-643 du 9 juin 2009 relatif aux autorisations délivrées en application de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales : afin de définir précisément les notions de constellation et de méga-constellation et de modifier les exigences techniques existantes ou d'ajouter de nouvelles exigences techniques adaptées aux nouvelles activités (constellation, récupération d'étages de lanceurs réutilisable).

Article 29 : Consolider les dispositions intéressant le nucléaire de défense

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Dans le domaine du nucléaire civil, s'agissant de la sûreté nucléaire et de la radioprotection[305], le recours à des prestataires et à la sous-traitance dans les installations nucléaires de base (installations nucléaires civiles) est encadré par l'article L. 593-6-1 du code de l'environnement. Cette disposition a été introduite au niveau législatif par la loi n° 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte (dite loi TECV). Avant 2015, les dispositions relatives au recours à des prestataires et à la sous-traitance dans les installations nucléaires de base étaient régies uniquement au niveau réglementaire par l'arrêté du 7 février 2012 fixant les règles générales relatives aux installations nucléaires de base.

L'article L. 593-6-1 du code de l'environnement dispose qu'en *« raison de l'importance particulière de certaines activités pour la protection des intérêts mentionnés à l'article L. 593-1[306], un décret en Conseil d'Etat peut encadrer ou limiter le recours à des prestataires ou à la sous-traitance pour leur réalisation »*. Cette disposition interdit également à l'exploitant de déléguer la surveillance des activités importantes effectuées par un prestataire extérieur. Les articles R. 593-9 à R. 593-13 du code de l'environnement ainsi que l'arrêté du 7 février 2012 précité précisent ces dispositions.

Cet encadrement est justifié par des contraintes liées aux risques de perte de maîtrise technique et de compétences chez les exploitants, de difficultés dans la transmission de l'information et de dilution des responsabilités.

Parmi les quatre régimes juridiques encadrant le domaine nucléaire de la défense[307], celui de la protection et du contrôle des matières nucléaires non destinées à la dissuasion concerne

[305] Article L. 591-1 du code de l'environnement : « La sûreté nucléaire est l'ensemble des dispositions techniques et des mesures d'organisation relatives à la conception, à la construction, au fonctionnement, à l'arrêt et au démantèlement des installations nucléaires de base ainsi qu'au transport des substances radioactives, prises en vue de prévenir les accidents ou d'en limiter les effets. La radioprotection est la protection contre les rayonnements ionisants, c'est-à-dire l'ensemble des règles, des procédures et des moyens de prévention et de surveillance visant à empêcher ou à réduire les effets nocifs des rayonnements ionisants produits sur les personnes, directement ou indirectement, y compris par les atteintes portées à l'environnement. »

[306] Il s'agit de la sécurité, la santé et la salubrité publiques ainsi que la protection de la nature et de l'environnement.

[307] Régime de la protection et du contrôle des matières nucléaires non affectées aux moyens nécessaires à la mise en œuvre de la politique de dissuasion : articles L. 1333-1 à L. 1333-14 du code de la défense.

Régime des installations et activités nucléaires intéressant la défense : articles L. 1333-15 à L. 1333-20 du code de la défense.

Régime des installations nucléaires intéressant la dissuasion : articles L. 1411-1 à L. 1411-7 du code de la défense

majoritairement le monde nucléaire civil, et vise à prendre en compte les enjeux de malveillance[308]. Les trois autres régimes concernent les installations et activités nucléaires intéressant la défense, les installations nucléaires intéressant la dissuasion et les matières nucléaires destinées à la dissuasion.

1.2. CADRE CONSTITUTIONNEL

L'encadrement, la limitation ou l'interdiction du recours à des prestataires ou à la sous-traitance est susceptible de porter atteinte au principe de la liberté du commerce et de l'industrie et notamment à la liberté d'entreprendre, principe à valeur constitutionnelle qui découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen[309]. Il appartient au législateur d'apporter à cette liberté des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[310].

1.3. CADRE CONVENTIONNEL

Au niveau international, la Convention sur la sûreté nucléaire et la Convention sur la protection physique des matières nucléaires, entrées respectivement en vigueur en 1996 et 1987, ne comportent pas de stipulations relatives au recours aux prestataires extérieurs et à la sous-traitance dans le domaine du nucléaire de défense.

Au niveau européen, les matières et installations nucléaires sont encadrées par le Traité instituant la Communauté européenne de l'énergie atomique, dit « traité Euratom » et par le droit dérivé qui en est issu.

Le Traité Euratom a notamment pour objectif d'établir des normes de sécurité uniformes pour protéger la population et les travailleurs, et de veiller à l'emploi des matières nucléaires à des fins civiles.

En matière d'usages militaires de l'énergie nucléaire, le Traité Euratom prévoit plusieurs dérogations. La principale porte sur le contrôle de sécurité[311] effectué par la Commission

---

Régime de protection des matières nucléaires affectées aux moyens nécessaires à la mise en œuvre de la politique de dissuasion : articles R*. 1411-11-18 à R*. 1411-11-35 du code de la défense.

[308] Ce régime a pour objectif « la protection des matières nucléaires et des activités associées mentionnées à l'article L. 1333-2 contre tout acte de malveillance ou perte de matières nucléaires, dans le but d'éviter la prolifération nucléaire et de prévenir tout risque ou inconvénient pour la santé, la salubrité, la sécurité publiques, et l'environnement pouvant en découler ainsi que le contrôle de ces matières et activités. » (article R. 1333-1 du code de la défense)

[309] Conseil constitutionnel, Loi de nationalisation, 16 janvier 1982, n° 81-132 DC.

[310] Conseil constitutionnel, Loi relative à l'archéologie préventive, 16 janvier 2001, n° 2000-439 DC.

[311] Vérifications physiques et comptables sur les matières nucléaires en vue de s'assurer de la conformité de leur utilisation par rapport à la déclaration de l'exploitant

européenne, l'article 84 prévoyant que : « *Le contrôle ne peut s'étendre aux matières destinées aux besoins de la défense qui sont en cours de façonnage spécial pour ces besoins ou qui, après ce façonnage, sont, conformément à un plan d'opérations, implantées ou stockées dans un établissement militaire*. »

Il est à noter que lorsque le Traité Euratom ne comporte aucune règle dans un domaine particulier, les règles du Traité sur le fonctionnement de l'union Européenne trouvent à s'appliquer.

Un arrêt de la CJUE de 2002[312] a reconnu et clarifié les compétences partagées d'Euratom avec les États membres dans le domaine de la sûreté nucléaire. Le Conseil a adopté une législation sur la sûreté nucléaire en 2009 [313] et une législation sur la gestion des déchets radioactifs et du combustible usé en 2011[314]. Ces deux directives ne s'appliquent qu'aux installations et activités civiles[315]. Une directive de 2013 traite par ailleurs des problématiques de radioprotection[316]. Seule la directive relative à la sûreté comporte des dispositions relatives aux contractants et sous-traitants : dès lors que leurs activités sont susceptibles d'affecter la sûreté nucléaire, l'exploitant reste responsable à l'égard de leurs activités et doit s'assurer qu'ils disposent de ressources humaines suffisantes et qualifiées.

Par ailleurs, la sécurité nucléaire, qui désigne les mesures visant à empêcher et détecter un vol, un sabotage, un accès non autorisé, un transfert illégal ou tout autre acte malveillant mettant en jeu des matières nucléaires et autres matières radioactives ou les installations associées, relève de la seule compétence des Etats membres.

Ainsi, aucune disposition de droit européen ne fait obstacle à cette mesure.

1.4. ÉLEMENTS DE DROIT COMPARE

Le Traité sur la non-prolifération des armes nucléaires, entré en vigueur en 1970, reconnaît cinq Etats dotés de l'arme nucléaire : les Etats-Unis, la Russie, le Royaume-Uni, la France et la Chine. Néanmoins, en raison de la sensibilité du sujet, peu de publications officielles sont

[312] Arrêt de la CJUE du 10 décembre 2002 dans l'affaire C-29/99, Commission/Conseil.

[313] Directive 2009/71/Euratom du Conseil du 25 juin 2009 établissant un cadre communautaire pour la sûreté nucléaire des installations nucléaires, modifiée par la directive 2014/87/Euratom du Conseil du 8 juillet 2014.

[314] Directive 2011/70/Euratom du Conseil du 19 juillet 2011 établissant un cadre communautaire pour la gestion responsable et sûre du combustible usé et des déchets radioactifs.

[315] Article 2 de la directive 2009/71 : « La présente directive s'applique à toute installation nucléaire civile soumise à autorisation »

Article 2 de la directive 2011/70 : « La présente directive s'applique à toutes les étapes:

a) de la gestion du combustible usé, lorsque ce dernier résulte d'activités civiles;

b) de la gestion des déchets radioactifs, de la production au stockage, lorsque ces déchets résultent d'activités civiles. »

[316] Directive 2013/59/Euratom du Conseil du 5 décembre 2013 fixant les normes de base relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants et abrogeant les directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom et 2003/122/Euratom.

consultables en source ouverte sur les règles en matière de recours à des prestataires extérieurs et à la sous-traitance au sein des installations nucléaires de défense de ces Etats.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les régimes relevant du code de la défense et applicables aux matières, installations ou activités nucléaires, qu'ils aient pour objectif la sécurité ou la sûreté nucléaires, ne comportent pas de dispositions sur le recours aux prestataires extérieurs et à la sous-traitance au niveau législatif. Lorsqu'elles existent, les limitations dans ce domaine ne sont prévues que par des textes de niveau insuffisant (décret ou arrêté)[317], alors même que ces régimes visent à prendre en compte aussi bien les enjeux de protection des personnes, des biens et de l'environnement que les enjeux de défense nationale.

En outre, en tant que la mesure est susceptible de porter atteinte à la liberté d'entreprendre, elle ne peut être introduite que par le législateur.

2.2. OBJECTIFS POURSUIVIS

Les dispositions envisagées visent à consolider le régime juridique applicable à l'ensemble des matières et activités nucléaires régies par le code de la défense pour garantir la sûreté et la sécurité nucléaires.

Dans le régime de la protection et du contrôle des matières nucléaires, de leurs installations et de leur transport (articles L. 1333-1 à L. 1333-14 du code de la défense), il n'existe pas de dispositions législatives relatives à l'encadrement au recours à des prestataires extérieurs et la sous-traitance pour les activités nucléaires soumises à autorisation définies à l'article L. 1333-2 du code de la défense. Si des dispositions réglementaires ont existé, elles n'avaient aucun fondement législatif et n'ont donc pas pu être maintenues ni étendues lors de la récente refonte de ce régime juridique[318]. L'ajout d'un nouvel article vise donc à conférer un fondement législatif à l'encadrement du recours aux prestataires extérieurs et à la sous-traitance que

[317] Régime de la protection et du contrôle des matières nucléaires : arrêté du 18 août 2010 relatif à la protection et au contrôle des matières nucléaires en cours de transport (articles 21 et 26) et arrêté du 10 juin 2011 relatif à la protection physique des installations abritant des matières nucléaires dont la détention relève d'une autorisation (article 18).

Régime des matières nucléaires affectées aux moyens de la dissuasion : article R. 1411-11-24 du code de la défense.

[318] Décret n° 2021-713 du 3 juin 2021 pris pour adapter le chapitre III du titre III du livre III de la partie 1 du code de la défense, et ses arrêtés d'application en date du 27 décembre 2022.

souhaitent mettre en place les ministres compétents (ministre de la défense et ministre en charge de l'énergie).

Une disposition relative au recours à des prestataires extérieurs ou à la sous-traitance est ajoutée dans le régime des installations et activités nucléaires intéressant la défense (IANID). Ce nouvel article vise, en plus de pouvoir encadrer, limiter ou interdire le recours à des prestataires extérieurs ou à la sous-traitance, à créer une obligation de surveillance des activités importantes pour la sûreté ou la radioprotection réalisées par des prestataires extérieurs ou des sous-traitants.

Une disposition similaire est également introduite dans le régime des installations nucléaires intéressant la dissuasion pour permettre de prendre en compte les risques qui peuvent émerger en cas de recours à des prestataires ou à la sous-traitance (actes malveillants ou hostiles et atteintes au secret de la défense nationale).

Enfin, l'ajout d'une section relative à la protection des matières nucléaires destinées à la dissuasion vise à conférer un fondement législatif à l'article R. 1411-24 du code de la défense qui prévoit que les transporteurs autorisés ne peuvent pas faire appel à un sous-traitant pour l'exécution des transports par moyens non militaires de matières nucléaires affectées à la dissuasion. Actuellement, aucune des dispositions législatives mentionnant les matières nucléaires affectées aux moyens nécessaires à la mise en œuvre de la politique de dissuasion, ne prévoit de règles relatives au recours à des prestataires extérieurs et à la sous-traitance.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Il aurait pu être envisagé dans certains cas de recourir à des clauses contractuelles. Toutefois, l'objectif de la mesure est de régir la possibilité pour un opérateur titulaire d'une autorisation administrative, et non d'un marché public ou privé, de recourir à des prestataires extérieurs ou à la sous-traitance. Ces opérateurs ne sont pas nécessairement placés sous le contrôle, même partiel, de l'Etat. S'agissant du régime de la protection et du contrôle des matières nucléaires, les opérateurs concernés sont en majorité privés (il peut s'agir, par exemple, des transports réalisés par Orano ou de l'exploitation de centrales nucléaires par EDF). Le Commissariat à l'énergie atomique et aux énergies alternatives, établissement public industriel et commercial, est un opérateur majeur du nucléaire civil et militaire. Des opérateurs non étatiques interviennent également dans les régimes applicables aux installations et activités nucléaires intéressant la défense, aux installations nucléaires intéressant la dissuasion, ainsi qu'aux matières nucléaires destinées à la dissuasion.

Seule l'option retenue, à savoir l'insertion dans les quatre régimes juridiques concernés de dispositions législatives, permet de répondre au besoin.

3.2. OPTION RETENUE

A l'instar des dispositions introduites dans la partie législative du code de l'environnement[319] par la loi TECV s'agissant de la sous-traitance et du recours à des prestataires extérieurs pour les installations nucléaires civiles (cf. item 1.1 *supra*), il est proposé d'apporter les mêmes garanties au niveau législatif pour les régimes du code de la défense encadrant les matières, installations et activités nucléaires.

Ainsi, dès lors que seront impliquées des matières, installations ou activités nucléaires soumises aux différents régimes prévus par le code de la défense en ce domaine, la sous-traitance et le recours à des prestataires extérieurs pourront être soumis à des limitations, justifiées par la nécessité de protéger certains enjeux. Dans ce contexte, sont insérées dans le code de la défense quatre nouvelles dispositions dont les modalités d'application seront définies par décret en Conseil d'Etat.

Concrètement, elles prévoient la possibilité d'encadrer, limiter ou interdire le recours à des prestataires extérieurs ou à la sous-traitance. Elles vont au-delà de l'article L. 593-6-1 du code de l'environnement en ce que la possibilité d'interdire ce recours est étendue. En effet, cet article autorise l'encadrement et la limitation du recours aux prestataires extérieurs ou à la sous-traitance dans les installations nucléaires de base et ne l'interdit expressément que pour la surveillance des activités importantes pour la protection des intérêts mentionnés à l'article L. 593-1 du code de l'environnement.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Le présent article prévoit la création de quatre articles au sein de la partie législative du code de la défense :

- un article L. 1333-3-1 dans le régime de la protection et du contrôle des matières nucléaires ;
- un article L. 1333-16-1 dans le régime des installations et activités nucléaires intéressant la défense ;
- un article L. 1411-7-1 dans le régime des installations nucléaires intéressant la dissuasion ;
- un article L. 1411-7-2, dans une nouvelle section relative au régime de la protection des matières nucléaires destinées à la dissuasion.

[319] Article L. 593-6-1 du code de l'environnement.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

L'ajout de ces nouveaux articles au sein du code de la défense n'emporte pas de conséquences sur les rapports entre le droit français, le droit international et le droit de l'Union européenne car la mesure relève de la seule compétence de la France.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les impacts sur les entreprises diffèrent selon les cas d'espèce : les conséquences ne seront pas les mêmes dans les cas où la sous-traitance et le recours à des prestataires extérieurs seront simplement encadrés que dans ceux où ce recours à des entreprises extérieures sera totalement interdit. Néanmoins, ces restrictions à la liberté d'entreprendre pour les entreprises sont justifiées par des raisons de sécurité et sûreté nucléaires.

Par ailleurs, la création de l'obligation pour les exploitants, dans les installations et activités nucléaires intéressant la défense, d'imposer la surveillance des fournisseurs d'équipements importants pour la sûreté nucléaire et des activités importantes pour la sûreté nucléaire, lorsqu'elles sont réalisées par des intervenants extérieurs, est susceptible d'avoir un impact en termes de ressources humaines, d'organisation et de relations contractuelles.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

La mesure envisagée entrera en vigueur le lendemain de la promulgation de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Cette mesure s'applique sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Un décret pris en Conseil d'Etat sera nécessaire pour préciser les modalités d'application de chacune de ces quatre mesures législatives.

Article 30 : Communication par l'autorité judiciaire des suites données aux affaires pénales militaires

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

En 1982, le législateur a rapproché la justice militaire et la justice de droit commun en supprimant les tribunaux permanents des forces armées sur le territoire national en temps de paix et en confiant la poursuite, l'instruction et le jugement des infractions commises par le militaire en activité aux juridictions de droit commun spécialisées en matière militaire (JDCS)[320].

La procédure pénale applicable aux militaires reste marquée par quelques particularités, dont celles énoncées à l'article 698-1 du code de procédure pénale qui prescrit au procureur de la République, à défaut de dénonciation des faits à l'autorité judiciaire par le ministre chargé de la défense ou l'autorité militaire habilitée par lui, de demander leur avis au ministre ou à ces autorités préalablement à tout acte de poursuite concernant les crimes et délits commis par les militaires sur le territoire de la République dans l'exercice de leur service et toutes les infractions commises hors du territoire national par les militaires ou à leur encontre.

Donné dans le délai d'un mois, cet avis doit figurer au dossier de la procédure à peine de nullité.

L'article 34 de la loi n° 2011-1862 du 13 décembre 2011, en complétant le premier alinéa de l'article 698-1 du code de procédure pénale, a clarifié et élargi le champ d'application de la procédure d'avis dans trois cas de figures supplémentaires :

- En cas de réquisitoire contre personne non dénommée, ce qui signifie que l'avis du ministre de la défense devra être sollicité dès lors que les éléments recueillis font apparaître qu'un militaire serait susceptible d'être poursuivi ;
- En cas de réquisitoire supplétif, consécutif à des révélations en cours d'instruction de faits nouveaux pouvant être reprochés à un militaire ;
- Et en cas de réquisitions faisant suite à une plainte avec constitution de partie civile.

L'article L. 211-24 du code de la justice militaire prévoit, pour les infractions commises en opérations extérieures, que l'avis du ministre de la défense sera demandé, lorsque, à la suite d'une décision de non-lieu, le ministère public aura décidé de requérir la réouverture de l'information sur charges nouvelles.

L'avis du ministre de la défense constitue un canal d'information aussi privilégié qu'encadré entre l'institution militaire et l'autorité judiciaire.

[320] Loi n° 82-621 du 21 juillet 1982 relative à relative à l'instruction et au jugement des infractions en matière militaire et de sûreté de l'Etat et modifiant les codes de procédure pénale et de justice militaire.

La demande d'avis transmise par le procureur de la République garantit au ministre de la défense qu'il sera systématiquement informé des faits mettant en cause un militaire dans l'exercice de son service, lui permettant de prendre toutes les mesures internes qui s'imposeraient pour faire cesser les éventuels désordres ou y remédier.

En retour, l'avis, au même titre que la dénonciation, fournit au parquet des éléments d'appréciation dont il ne dispose pas habituellement dans un dossier pénal sur le contexte opérationnel, le périmètre et les contraintes de la mission du militaire concerné, les spécifications techniques des matériels en cause, le retentissement des faits dans les armées, l'évaluation du préjudice matériel subi par l'institution, ou encore les mesures internes et/ou disciplinaires prises. C'est au vu de ces éléments que le ministre de la défense conclut à l'orientation procédurale qu'il estime la plus opportune.

L'économie de cette procédure est donc non seulement d'éclairer l'autorité judiciaire sur les spécificités militaires susceptibles d'avoir un impact sur l'appréciation pénale du dossier, mais également de tenir l'autorité militaire informée. Ainsi, lors des travaux parlementaires, Robert Badinter, garde des Sceaux à l'origine de la loi n° 82-621 du 21 juillet 1982, soutenait que « *cette disposition a pour objet de tenir compte de la spécificité militaire : l'autorité militaire doit être informée des intentions du parquet et pouvoir faire connaître son opinion* »[321].

Comme évoqué par le sénateur Marcel-Pierre Cléach dans son avis fait au nom de la commission des affaires étrangères et de la défense déposé le 23 mars 2011 sur le projet de loi relatif à la répartition des contentieux et à l'allègement de certaines procédures juridictionnelles, l'objectif de cette procédure est bien *« d'organiser un échange réciproque d'informations entre l'autorité militaire et le ministère publique »* afin notamment que l'autorité hiérarchique prenne les mesures commandées par l'implication d'un militaire dans une procédure pénale. Ainsi, « *l'échange d'information entre le ministère public et l'autorité militaire permet à cette dernière de tenir compte de l'exercice éventuel des poursuites pénales, ces éléments étant susceptibles d'avoir une incidence sur la manière de servir, la disponibilité et donc la capacité opérationnelle du militaire concerné* »[322].

1.2. CADRE CONSTITUTIONNEL

Selon la jurisprudence du Conseil constitutionnel, il découle de l'indépendance de l'autorité judiciaire fixée au premier alinéa de l'article 64 de la Constitution, autorité judiciaire à laquelle appartiennent les magistrats du parquet, un principe selon lequel le ministère public exerce

[321] J.O. débats AN, 14 avril 1982, 2ème séance, p. 1128.

[322] Avis n° 367 (2010-2011) de M. Marcel-Pierre Cléach, fait au nom de la commission des affaires étrangères et de la défense, déposé le 23 mars 2011, sur le projet de loi relatif à la répartition des contentieux et à l'allègement de certaines procédures juridictionnelles, p. 76.

librement, en recherchant la protection des intérêts de la société, son action devant les juridictions[323].

Le Conseil constitutionnel a été amené à se prononcer sur les dispositions de l'article 698-1 du code de procédure pénale. Saisi d'une question prioritaire de constitutionnalité (QPC), il a écarté le grief de méconnaissance du principe d'égalité devant la justice, estimant que le législateur a entendu garantir que puissent, le cas échéant, être portées à la connaissance de l'institution judiciaire les spécificités du contexte militaire des faits à l'origine de la poursuite ou des informations particulières relatives à l'auteur présumé eu égard à son état militaire ou à sa mission, sans créer de discriminations injustifiées. Il est souligné que cet avis ne lie pas le ministère public dans l'appréciation de la suite à donner aux faits et que, figurant au dossier de la procédure, il peut être discuté par les parties[324]. En outre, il est souligné que l'avis avant poursuites ne concerne pas les crimes ou délits flagrants.

Le Conseil constitutionnel a pu rappeler que le secret de l'enquête et de l'instruction est une garantie donnée aux citoyens pour assurer à la fois la préservation de l'ordre public en permettant la recherche des auteurs d'infractions, mais aussi une garantie du respect de la présomption d'innocence et de la protection de la vie privée. Il ne peut subir de restriction que si celle-ci est justifiée par un intérêt général et proportionnée à celui-ci[325].

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les dispositions de l'article 698-1 du code de procédure pénale ne permettent pas à l'autorité militaire de connaître les suites judiciaires données aux procédures dans le cadre desquelles elle a rendu un avis ou dénoncé les faits.

Certes, l'article L. 261-6 du code de justice militaire prévoit que dans les trois jours de la mise à exécution d'un jugement de condamnation concernant un militaire, le ministère public est tenu d'en adresser un extrait au commandant de la formation administrative auquel appartenait le condamné. Mais cet article, rendu applicable en temps de paix par l'effet de l'article 698-5 du code de procédure pénale, ne concerne que les jugements de condamnation.

Par exception au principe du secret de l'enquête et de l'instruction prévu à l'article 11 du code de procédure pénale, plusieurs textes prescrivent déjà au ministère public de communiquer les suites judiciaires données à une procédure pénale.

Une telle obligation figure notamment à l'article 40-2 du code de procédure pénale pour les dénonciations faites par les autorités publiques au titre de l'article 40, le procureur de la

[323] Décision n° 2017-680 QPC du 8 décembre 2017, paragr. 6.

[324] Décision n° 2015-461 QPC du 24 avril 2015.

[325] Décision n° 2017-693 QPC du 2 mars 2018.

République devant les aviser des poursuites ou mesures alternatives décidées à la suite de leur signalement.

De même, l'article 561-30-1 du code monétaire et financier prévoit que, pour les faits susceptibles de relever du blanchiment du produit d'une infraction ou du financement du terrorisme ayant fait l'objet d'une note d'information de la cellule de renseignement financier nationale au procureur de la République, ce dernier doit l'informer de l'engagement d'une procédure judiciaire, du classement sans suite ainsi que des décisions prononcées par les juridictions répressives.

Outre ces retours de signalement, la loi n° 2016-457 du 14 avril 2016 relative à l'information de l'administration par l'autorité judiciaire et à la protection des mineurs a instauré deux régimes d'information en créant un article 11-2 et un article 706-47-4 dans le code de procédure pénale. Le premier est un régime général et facultatif d'information par l'autorité judiciaire de l'autorité publique d'emploi de certaines décisions pénales concernant leurs agents ou les personnes placées sous leur contrôle, le second un régime spécifique à la protection des mineurs et qui présente un caractère obligatoire (infractions graves, à caractère violent ou de nature sexuelle commises par des personnes en contact habituel avec des mineurs).

Le premier dispositif qui ne concerne que les crimes et délits punis d'emprisonnement reste donc optionnel et limité aux hypothèses où le ministère public estime cette transmission nécessaire, en raison de la nature des faits ou des circonstances de leur commission, pour mettre fin ou prévenir un trouble à l'ordre public ou pour assurer la sécurité des personnes ou des biens.

En matière d'affaires pénales militaires, il apparait nécessaire de consacrer dans la loi le principe de la communication systématique des suites judiciaires par l'autorité judiciaire à l'autorité militaire, quelles que soient la peine encourue, l'infraction poursuivie ou l'activité du mis en cause.

En effet, le contexte géopolitique actuel, qui requiert une projection importante de personnels à l'étranger mais également un déploiement conséquent de militaires sur le territoire national, renforce la nécessité pour l'institution militaire de disposer de personnels dont l'implication dans une procédure pénale n'est pas de nature à entraver leurs missions ou les enjeux opérationnels. Ce contexte de multiplication des fronts d'engagement, notamment par l'émergence de nouvelles zones de conflit, mobilise un nombre croissant de personnels. Dans le même esprit que ce que relevait en 2016 la circulaire d'application de l'article 11-2 du code de procédure pénale[326], l'objectif de cette information est de permettre à l'autorité d'emploi de prendre les mesures qu'elle estime nécessaires.

La connaissance des suites judiciaires des affaires pénales militaires est particulièrement indispensable. Les infractions en cette matière étant principalement en lien avec l'exercice du

[326] Circulaire du 4 août 2016 de présentation des dispositions de procédure pénale de la loi n° 2016-457 du 14 avril 2016 relative à l'information de l'administration par l'autorité judicaire et à la protection des mineurs et de son décret d'application n° 2016-612 du 18 mai 2016 (NOR : JUSD1622465C).

service[327], leurs conséquences majeures sur l'employabilité des personnels concernés peuvent être majeures : aptitude/autorisation de port d'armes, interdiction d'entrer en contact avec la victime, les coauteurs ou complices ou les témoins, interdiction de paraitre dans des lieux déterminés, autorisation de conduite des véhicules militaires, autorisation de sortie du territoire national pour les projections en opérations extérieures (OPEX) notamment.

Il semble tout indiqué que, dans le cadre restreint du contentieux pénal militaire pour lequel un avis a été rendu ou une dénonciation faite, l'autorité militaire qui s'est prononcée sur les suites judiciaires qu'elle préconisait, soit renseignée sur la décision prise finalement par le parquet.

2.2. OBJECTIFS POURSUIVIS

Afin de permettre un meilleur suivi des affaires pénale et fluidifier les relations, il convient de créer un fondement légal à la transmission des informations entre les juridictions spécialisées et l'institution militaire.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTION ENVISAGEE

Une circulaire du garde des sceaux en date du 9 septembre 1984[328] rappelait aux juridictions de droit commun spécialisées la nécessité d'informer les autorités militaires des décisions judiciaires prononcées à l'encontre des militaires. Il aurait pu être envisagé de prévoir une nouvelle circulaire ministérielle ou une convention entre le ministère de la justice et le ministère des armées décrivant ce circuit de transmission de l'information.

Or, les dispositions de procédure pénale relèvent du domaine de la loi et tout texte qui permet une dérogation au secret de l'enquête et de l'instruction, prévu à l'article 11 du code de procédure pénale, doit s'intégrer dans un dispositif cohérent et respectueux de la hiérarchie des normes. L'option d'une simple modification réglementaire ou infra-réglementaire doit être écartée.

Il ne serait pas pertinent d'insérer dans le code de justice militaire ou dans le code de la défense le texte de niveau législatif permettant cette communication. Il apparaît essentiel qu'elle soit corrélée aux dispositions de l'article 698-1 du code de procédure pénale qui fixe le régime de la demande d'avis avant poursuites et de la dénonciation.

[327] A l'exception des infractions commises hors du territoire national par les militaires ou à leur encontre (article 697-4 du CPP), infractions qui ne sont pas systématiquement en lien avec le service.

[328] Circulaire faisant le bilan de la première application de la loi du 21 juillet 1982 et complétant les instructions contenues dans une première circulaire d'application du 6 décembre 1982 (Réf. CRIM.84 – 14 – E.1/9.9.84).

3.2. OPTION RETENUE

Il est proposé de créer un alinéa 4 à l'article 698-1 du code de procédure pénale pour que l'autorité militaire soit avisée des suites judiciaires données aux affaires pénales militaires compte tenu des conséquences administratives, disciplinaires et opérationnelles qui peuvent en découler.

La rédaction de cette mesure transposera la structure de l'article 40-2 du code de procédure pénale qui concerne les signalements d'infractions pénales à l'autorité judiciaire par les agents publics.

Il sera ainsi prévu que le procureur de la République avisera le ministre de la défense ou l'autorité militaire habilitée par lui, des poursuites ou des mesures alternatives aux poursuites qui ont été décidées à la suite de la dénonciation ou avis mentionnés au premier alinéa. En cas de classement sans suite de la procédure, il communiquera sa décision en indiquant les raisons juridiques ou d'opportunité qui l'ont justifiée.

Cela permettra à l'autorité militaire d'être éclairée sur le motif de classement sans suite de la procédure (infraction insuffisamment caractérisée, absence d'infraction, motif juridique, ou carence du plaignant par exemple).

En l'absence de transmission spontanée par le ministère public, l'autorité militaire disposera d'un fondement légal permettant de solliciter le parquet compétent et d'obtenir ainsi les suites données à une affaire pénale militaire (poursuites engagées, alternative ou classement sans suite) sans contrevenir aux dispositions de l'article 11 du code de procédure pénale.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

La modification de l'article 698-1 du code de procédure pénale dans ces termes n'est pas de nature à constituer une atteinte à l'indépendance de l'autorité judiciaire, cette communication qui intervient dans un second temps ne peut interférer sur la décision d'engager ou non des poursuites ou de mettre en œuvre des mesures alternatives.

Cette disposition ne concernera de surcroît qu'une partie du contentieux pénal militaire, les crimes et délits flagrants et les poursuites engagées devant les JDCS contre des civils par exemple, étant exclus *de facto* du champ de la procédure d'avis avant poursuites.

Par ailleurs, une mesure d'harmonisation légistique doit être prise aux premier et troisième alinéas, la dénomination *ministre de la défense* sera retenue pour se substituer à celle de *ministre chargé de la défense*.

4.2. IMPACTS SUR LES SERVICES JUDICIAIRES

Cette mesure ne concerne que les tribunaux judiciaires compétents pour connaître des procédures pénales militaires, soit les neuf juridictions de droit commun spécialisées sur le territoire national. Sans formalisme procédural particulier, la communication des suites judiciaires pourra être réalisée par le greffe spécialisé par ailleurs doté de personnels militaires (greffiers militaires). Elle ne devrait donc pas avoir d'impact significatif sur les services judiciaires.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal Officiel* de la République française. S'agissant d'un texte fixant les modalités de poursuites et les formes de la procédure, il est d'application immédiate aux procédures pénales en cours pourvu qu'une décision définitive n'ait pas encore été rendue.

5.2.2. Application dans l'espace

Ces dispositions ont vocation à s'appliquer dans les collectivités d'outre-mer régies par l'article 73 de la Constitution du fait du principe d'identité législative sans qu'il soit requis d'en faire mention expresse.

Dans les collectivités d'outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie soumises au régime de spécialité législative, une mention expresse d'application est nécessaire afin de rendre ces dispositions applicables via la mise à jour de l'article 804 du code de procédure pénale modifié à cette fin par l'article 36 du présent projet de loi.

Par ailleurs, aucune adaptation de ces dispositions tenant aux caractéristiques des collectivités n'apparaît nécessaire.

Ces mesures sont donc applicables sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Les présentes dispositions ne requièrent aucun texte d'application.

Article 31 : Création d'un régime d'autorisation relatif aux activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin en mer territoriale

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Avant de poser un câble ou un pipe-line sous-marin, un opérateur doit effectuer des études préalables[329] pour confirmer le tracé envisagé. Ces études sont de différents types : relevés bathymétriques[330], prélèvements de sédiments (carottage) ou encore études UXO (UneXploded Ordnance) pour détecter l'éventuelle présence d'engins explosifs immergés. En fonction des techniques utilisées, ces études peuvent avoir un impact sur le sous-sol (carottage) ou sur l'environnement (impact des sonars sur la faune marine notamment).

En droit national, l'article 1er du décret n° 2017-956 du 10 mai 2017 fixant les conditions d'application des articles L. 251-1 et suivants du code de la recherche331 relatifs à la recherche scientifique marine (RSM[332]) en mer territoriale exclut les activités de pose de câbles du régime de la RSM en faisant référence à l'article 28 de l'ordonnance n° 2016-1687 du 8 décembre 2016 relative aux espaces maritimes relevant de la souveraineté ou de la juridiction de la République française. Toutefois, l'article 28 de l'ordonnance ne s'applique que sur le plateau continental et dans la zone économique exclusive et ne traite pas explicitement des activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin.

Dans les faits, les préfectures maritimes ou les services des délégués du gouvernement pour l'action de l'Etat en mer (AEM) outre-mer ont des pratiques diverses (régime de RSM, application directe de la CNUDM) pour traiter ces types de demandes dans la zone économique exclusive ou dans la mer territoriale.

---

[329] Réalisées le plus souvent par des prestataires privés ou plus exceptionnellement par des organismes publics (SHOM, IFREMER, Marine nationale).

[330] Bathymétrie : science de la mesure des profondeurs et du relief de l'océan en vue de déterminer la topographie du sol de la mer.

[331] L. 251-1 du code de la recherche : « Toute activité de recherche scientifique marine, menée dans la mer territoriale, dans la zone économique exclusive et dans la zone de protection écologique définies par *l'ordonnance n° 2016-1687 du 8 décembre 2016* relative aux espaces maritimes relevant de la souveraineté ou de la juridiction de la République française, est soumise à une autorisation assortie, le cas échéant, de prescriptions dans les conditions et selon les modalités fixées par décret en Conseil d'Etat ».

[332] La recherche scientifique marine est réglementée en application de la partie XIII de la Convention des Nations unies sur le droit de la mer. Cette convention vise à favoriser la recherche menée à des fins pacifiques et la diffusion des connaissances, sans gêner les autres utilisations de la mer, en fixant le cadre nécessaire pour organiser le contrôle et la régulation de cette activité. Le décret du 10 mai 2017 ne concerne que les activités qui ne bénéficient pas d'un autre type d'autorisation (pêche scientifique, exploitation minières, pose de câble ou pipeline sous-marin…).

Ce constat a conduit le Secrétaire général de la mer à animer un groupe de travail interministériel sur cette problématique. Les travaux ont débouché sur la modification du décret n° 2013-611[333] par le décret n° 2021-1942 du 31 décembre 2021[334]. Toutefois, en l'absence de disposition législative spécifique à la mer territoriale, le Conseil d'Etat a validé le projet du gouvernement uniquement sur le plateau continental et la zone économique exclusive, estimant que les études préalables à la pose de câbles ne relevaient pas de la « *recherche scientifique marine* » au sens de l'article L. 251-1 du code de la recherche. Dans ces espaces, les activités d'études préalables à la pose d'un câble ou d'un pipeline sous-marin font désormais l'objet d'un régime de notification (article 18-1 à 18-5 du décret n° 2013-611).

A ce jour, les activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipeline en mer territoriale ne sont encadrées par aucune réglementation nationale.

1.2. CADRE CONSTITUTIONNEL

Le Conseil d'Etat a eu l'occasion de rappeler la compétence du législateur, s'agissant de la création d'un nouveau régime d'autorisation administrative en matière de câbles sous-marins, à l'occasion de la dernière modification, en 2021, du décret n° 2013-611 du 10 juillet 2013 précité. Le régime d'autorisation affecte en effet la liberté d'entreprendre, constitutionnellement garantie et c'est au législateur de définir les conditions dans lesquelles il peut y être porté atteinte, pour des motifs d'intérêt général ou répondant à une exigence constitutionnelle[335].

1.3. CADRE CONVENTIONNEL

La Convention des Nations unies sur le droit de la mer signée à Montego Bay le 10 décembre 1982 ne précise pas le régime juridique applicable aux activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin. En effet, ce type d'activité, rendu possible par les avancées technologiques, est relativement récent au regard de la période de négociation de la CNUDM (années 1970).

---

[333] Décret n° 2013-611 du 10 juillet 2013 relatif à la réglementation applicable aux îles artificielles, aux installations, aux ouvrages et à leurs installations connexes sur le plateau continental et dans la zone économique exclusive et la zone de protection écologique ainsi qu'aux câbles et pipelines sous-marins.

[334] Décret n° 2021-1942 du 31 décembre 2021 modifiant le décret n° 2013-611 du 10 juillet 2013 relatif à la réglementation applicable aux îles artificielles, aux installations, aux ouvrages et à leurs installations connexes sur le plateau continental et dans la zone économique exclusive et la zone de protection écologique ainsi qu'au tracé des câbles et pipelines sous-marins.

[335] Décision n° 2000-439 DC du 16 janvier 2001 - Loi relative à l'archéologie préventive
"(...) *13. Considérant qu'il est loisible au législateur d'apporter à la liberté d'entreprendre, qui découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen de 1789, des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi ; (...) »*

Son article 2 stipule que la souveraineté de l'Etat côtier s'étend à la mer territoriale ainsi qu'au fond de cette mer et à son sous-sol. Les activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line ne relevant pas du régime du « passage inoffensif », l'Etat côtier est compétent pour fixer les règles applicables à ces activités dans sa mer territoriale.

1.4. ÉLEMENTS DE DROIT COMPARE

Il existe des réglementations étatiques diverses qui peuvent être appliquées en matière d'activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin.

Certains Etats appliquent le régime de la recherche scientifique marine, d'autres des cadres juridiques *ad hoc*. L'interprétation de la CNUDM reste toutefois la même concernant la nécessité de solliciter l'autorisation de l'Etat côtier, la mer territoriale étant un espace placé sous sa souveraineté en vertu de l'article 2 de la Convention.

Toutefois, aucune réglementation spécifique aux activités d'études préalables n'a été identifiée.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Dérogatoires au droit de passage inoffensif, les activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin dans la mer territoriale peuvent revêtir une grande sensibilité au regard des senseurs mis en œuvre.

La création d'un régime d'autorisation préalable est donc nécessaire afin d'encadrer ces activités et prendre en compte les incidences sur la sécurité de la navigation, la protection de l'environnement ou des biens culturels maritimes, ou la sauvegarde des intérêts de la défense nationale.

Ainsi, s'agissant d'un sujet relevant du domaine de la loi (cf. 1.2), une modification de l'ordonnance n° 2016-1687 du 8 décembre 2016 relative aux espaces maritimes relevant de la souveraineté ou de la juridiction de la République française est nécessaire.

2.2. OBJECTIFS POURSUIVIS

La présente disposition poursuit un double but :

- harmoniser sur l'ensemble des espaces maritimes la réglementation relative aux activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin. Cette harmonisation s'inscrit dans la démarche de l'Etat d'assurer une

meilleure lisibilité des mesures relatives à la pose de câbles sous-marins et à leur arrivée sur le territoire national[336] ;

– faire respecter la souveraineté de l'Etat pour certaines missions relevant du droit de passage inoffensif dans les eaux territoriales, en particulier pour des impératifs de défense nationale.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Au cours des travaux de modification du décret n° 2013-611 précité et en l'absence de disposition législative particulière, le Conseil d'Etat n'a pas estimé possible de créer par décret un régime d'autorisation dans la mer territoriale activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin.

Par ailleurs, l'application du régime de RSM semble peu adaptée à ces études préalables qui ne correspondent pas à l'esprit développé dans la CNUDM visant à accroître les « *connaissances scientifiques sur le milieu marin dans l'intérêt de l'humanité toute entière* » (article 246).

3.2. OPTION RETENUE

Il est donc proposé de créer un article 41 *bis* dans l'ordonnance n° 2016-1687 du 8 décembre 2016 relative aux espaces maritimes relevant de la souveraineté ou de la juridiction de la République française afin de créer un régime d'autorisation pour les activités d'études préalables à la pose ou à l'enlèvement[337] d'un câble ou d'un pipe-line sous-marin en mer territoriale. Une modification de l'article 55 est également proposée à l'article 36 du présent projet de loi afin de prendre en compte les particularités d'application outre-mer.

Il est également proposé de prendre en compte la création de ce nouveau régime dans l'architecture de l'ordonnance du 8 décembre 2016 en remplaçant l'intitulé du titre III « Encadrement de la recherche en mer » par « Encadrement de la recherche et des études en mer ».

Les incidences sur la sécurité de la navigation, la protection de l'environnement ou des biens culturels maritimes, ou la sauvegarde des intérêts de la défense nationale devront être prises en compte au cours de l'instruction des demandes d'autorisation.

---

[336] Instruction du Premier ministre du 13 novembre 2020 relative à l'attractivité du territoire français en matière de câbles sous-marins de communication.

[337] Les règles applicables à la pose et à l'enlèvement sont fixées par la convention d'utilisation du domaine public maritime (article L. 2124-1 et suivants du CG3P).

Une modification du décret n° 2013-611 précité sera par la suite nécessaire afin de définir cette procédure d'autorisation selon une architecture comparable à celle du régime de notification des études préalables en ZEE et sur le plateau continental. *In fine*, l'autorité de l'Etat compétente localement[338], ou l'autorité compétente localement pour les collectivités régies par l'article 74 de la Constitution, la Polynésie française et la Nouvelle-Calédonie, en lien avec l'autorité locale chargée de la police du droit de passage inoffensif en mer territoriale, devra notifier à l'opérateur l'autorisation, éventuellement assortie de prescriptions, ou le refus.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Le dispositif retenu se traduit par la création d'un article 41 bis dans le titre III de l'ordonnance n° 2016-1687 du 8 décembre 2016 relative aux espaces maritimes relevant de la souveraineté ou de la juridiction de la République française pour les activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin en mer territoriale. Il permet de compléter le cadre juridique applicable aux espaces maritimes.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Ces dispositions sont compatibles avec la réglementation internationale, en particulier la Convention des Nations unies sur le droit de la mer signée à Montego Bay le 10 décembre 1982. Selon son article 79.4, l'Etat côtier dispose en mer territoriale d'une souveraineté pleine et entière et peut donc établir des conditions s'appliquant aux câbles qui pénètrent dans sa mer territoriale.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

En harmonisant les normes applicables, les présentes dispositions pourront concourir à l'attractivité de la France en matière de câbles sous-marins de communication.

4.2.2. Impacts sur les entreprises

La création de ce régime d'autorisation permettra de fixer un régime unique d'autorisation applicable aux activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-

[338] Représentants de l'Etat en mer en métropole, dans les collectivités régies par l'article 73 de la Constitution, à Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

line sous-marin. Le décret n° 2013-611 sera ensuite modifié en s'inspirant des récentes dispositions sur la notification des études préalables à la pose de câble ou de pipe-line sous-marin en zone économique exclusive ou sur le plateau continental.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités de la Nouvelle-Calédonie, de la Polynésie française, de Saint-Barthélemy, de Saint-Martin et de Saint-Pierre-et-Miquelon continueront, conformément à leurs compétences[339], d'autoriser ou d'interdire localement les activités d'études préalables à la pose ou à l'enlèvement de câbles et de pipelines sous-marins, en associant les autorités de l'Etat chargées des mesures de police visant à faire respecter le droit de passage inoffensif, en particulier au titre des exigences de la défense nationale.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La création de ce régime d'autorisation permettra d'harmoniser les pratiques des services de l'Etat et de faciliter la prise de décision en donnant un fondement juridique unique.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.2. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.3. Impacts sur la jeunesse

Sans objet.

4.5.4. Impacts sur les professions réglementées

Sans objet.

[339] Cf. articles 27 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie française, pour la Polynésie française, L.O. 6214-6 du code général des collectivités territoriales (CGCT), pour Saint-Barthélemy, et L.O. 6314-6 du CGCT, pour Saint-Martin, ainsi que l'avis du Conseil d'Etat n° 380759 du 8 novembre 2007, pour la Nouvelle-Calédonie et pour St-Pierre-et-Miquelon.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

La création de ce régime d'autorisation permettra de prendre en compte la préservation de l'environnement marin dans l'étude des dossiers d'activités d'études préalables à la pose ou à l'enlèvement d'un câble ou d'un pipe-line sous-marin.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire et aucune consultation facultative n'a été conduite.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article entre en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions de cet article sont applicables à Saint-Barthélemy, à Saint-Martin, à Saint-Pierre-et-Miquelon, en Polynésie française et en Nouvelle-Calédonie, sous réserve des compétences dévolues à ces collectivités, ainsi que dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

5.2.3. Textes d'application

Cette mesure législative se concrétisera par une modification du décret n° 2013-611 du 10 juillet 2013 relatif à la réglementation applicable aux îles artificielles, aux installations, aux ouvrages et à leurs installations connexes sur le plateau continental et dans la zone économique exclusive et la zone de protection écologique ainsi qu'aux câbles et pipelines sous-marins sera nécessaire (cf. 3.2 *supra*).

CHAPITRE V – SECURITE DES SYSTEMES D'INFORMATION

Article 32 : Prescrire des mesures de filtrage de noms de domaine (DNS) aux hébergeurs, fournisseurs d'accès à Internet (FAI) ou registrars en cas de menaces susceptibles de porter atteinte à la sécurité nationale

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

1.1.1. Contexte général et architecture informatique

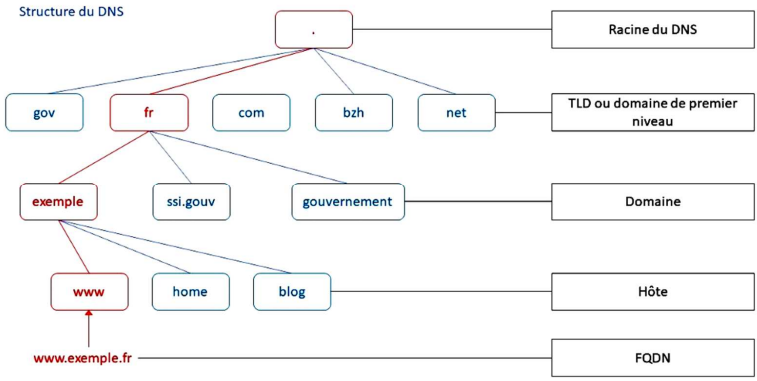
Fonctionnement général du système DNS

Le « Domain Name System » (système de nom de domaine) ou DNS est un service permettant de faire correspondre un nom de domaine à une adresse IP (*Internet Protocol*) – le numéro attribué à titre permanent ou provisoire à chaque périphérique relié à Internet, adresse qui prend la forme d'une suite de numéros (par exemple, « 45.60.12.53 ») et est compréhensible par une machine.

Le nom de domaine (URL ou *Uniform Resource Locator* en français, « localisateur uniforme de ressource », sous la forme « exemple.fr »), plus facile à retenir et à retranscrire pour l'internaute, constitue l'alias alphanumérique de l'adresse IP. Les machines appelées serveurs de nom de domaine (ou serveurs DNS) permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.

Le système DNS s'appuie sur une structure arborescente. L'ensemble des noms de domaine constituent ainsi un arbre inversé où chaque nœud est séparé du suivant par un point. On appelle « nom de domaine » chaque nœud de l'arbre. Le nom absolu, correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (*Fully Qualified Domain Name*). A titre d'exemple, « legifrance.gouv.fr. » constitue une adresse FQDN.

Lorsqu'une requête relative à un nom de domaine est effectuée, des serveurs sont successivement interrogés pour retrouver l'adresse IP correspondante. Si l'on cherche par exemple le nom de domaine « exemple.fr », dans un premier temps, un serveur racine est interrogé, qui renvoie vers le serveur faisant autorité pour le domaine de premier niveau, appelé le *Top Level Domain* (« .fr » dans l'exemple). Dans un second temps, le serveur autorité de premier niveau renvoie l'adresse du serveur faisant autorité sur le second niveau (ici, « exemple.fr »), et cela jusqu'à ce que la requête soit résolue.



Il s'agit donc d'**une base de données distribuée** (aucun serveur ne comprend l'ensemble des données du système DNS) **et hiérarchisée** (les serveurs de plus bas niveau dépendent des serveurs supérieurs pour opérer).

Les principaux acteurs du système DNS susceptibles d'être concernés

Les acteurs du DNS susceptibles d'être concernés par des agissements malveillants sont pour l'essentiel les suivants :

- **les fournisseurs d'accès Internet (FAI)** : ces opérateurs, au travers de leurs réseaux, connectent les systèmes d'information de leurs clients au réseau Internet et sont donc amenés à faire transiter sur leurs réseaux tous les flux, légitimes ou malveillants ;
- **les hébergeurs de données** : ces opérateurs mettent à la disposition des créateurs de sites web des espaces de stockage sur des serveurs sécurisés afin que leurs sites soient accessibles sur Internet. Les hébergeurs de données peuvent, sans le vouloir, héberger des données malveillantes, telles que des centres de commande et contrôle (dits « serveurs C2 ») qui permettent à un acteur malveillant de contrôler ses outils d'attaque à distance ;
- **les registres comme l'Association française pour le nommage Internet en coopération - AFNIC (registre, notamment, du « .fr ») et les bureaux d'enregistrement des noms de domaine établis en France** : ces entités gèrent la réservation de noms de domaine. D'une part, les registres de noms de domaine maintiennent et gèrent les noms de domaine (correspondance entre le nom de domaine et la personne ou l'organisation propriétaire). D'autre part, les bureaux d'enregistrement se voient déléguer par les registres la commercialisation des noms de domaine (réservation des noms de domaine pour une durée limitée). Ils proposent souvent, en plus de la location des noms de domaine, un service de DNS permettant au loueur d'enregistrer directement l'adresse IP d'un serveur pour en permettre la résolution.

1.1.2. Les mesures de filtrage prévues en droit positif

Des mesures de filtrage, dont certaines utilisent le DNS, existent déjà en droit positif. Elles reposent sur un certain nombre de techniques :

- le simple **retrait** des contenus illicites ;
- le **déréférencement** : la ressource litigieuse n'est pas supprimée mais n'est plus accessible via un moteur de recherche, n'étant plus référencée dans la liste proposée par ce dernier ;
- le **blocage par adresse IP**, qui consiste à mettre en place une liste noire d'adresses IP afin que les communications vers celles-ci soient bloquées ;
- le **blocage par DNS** qui revient à filtrer le nom de domaine. Il empêche l'internaute de se connecter à la ressource associée au nom de domaine (principalement les sites Internet), ressource qui est rendue inaccessible pour l'ensemble des utilisateurs ;
- **l'interruption de l'accès** sans demande de retrait préalable.

Des obligations mises à la charge des opérateurs

L'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) prévoit une **obligation de retrait par les prestataires** techniques, spontanément (§ I, 7) ou après notification (§ I, 5), en cas de contenu illicite.

Pour rappel, la loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, qui obligeait les plateformes à retirer certains contenus illicites (incitations à la haine, etc.), avait été partiellement censurée par le Conseil constitutionnel en ce qu'elle *« incit[ait] les opérateurs de plateforme en ligne à retirer les contenus qui leur sont signalés, qu'ils soient ou non manifestement illicites »* et portait donc une atteinte inconstitutionnelle à l'exercice de la liberté d'expression et de communication[340].

Le blocage judiciaire

Différentes dispositions législatives autorisent des mesures judiciaires de restriction d'accès :

- l'article 6, § I, 8 de la loi n° 2004-575 du 21 juin 2004 précitée crée la procédure dite du « référé internet » : l'autorité judiciaire peut prescrire en référé à un hébergeur ou à un FAI *« toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne »*, en matière d'atteintes aux personnes (apologie des crimes contre l'humanité, *etc.*) ;
- l'article L. 336-2 du code de la propriété intellectuelle[341] prévoit que les titulaires de droits peuvent demander au juge d'ordonner en référé toutes mesures propres à prévenir ou à faire cesser une atteinte à un droit d'auteur ou à un droit voisin ;

[340] Cons. const., décision du 18 juin 2020, n° 2020-801 DC.

[341] Modifié par la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite loi Hadopi I.

- l'article 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne dispose que le président de l'Autorité de régulation des jeux en ligne peut saisir le juge en référé pour obtenir le blocage d'un site. La procédure est dite « référé jeux en ligne ». Le décret n° 2011-2122 du 30 décembre 2011[342] a précisé que les fournisseurs d'accès à Internet doivent alors utiliser le blocage par DNS ;
- en vertu de l'article 706-23 du code de procédure pénale, l'arrêt d'un service de communication au public en ligne peut être prononcé par le juge des référés pour des faits d'apologie du terrorisme, lorsqu'ils constituent un trouble manifestement illicite, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir ;
- selon l'article L. 163-2 du code électoral, le juge des référés peut prescrire, pendant les trois mois précédant une élection, toutes mesures proportionnées et nécessaires pour faire cesser une diffusion délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne d'informations inexactes ou trompeuses de nature à altérer la sincérité du scrutin à venir.

Le blocage administratif

En application de l'article 6-1 de la loi LCEN précitée, la procédure de blocage administratif en cas de provocation ou d'apologie du terrorisme ou de pédopornographie exige, pour être mise en œuvre, une demande préalable de retrait de l'autorité administrative. En l'absence de réponse dans les 24 heures, la même autorité sollicite un blocage du site auprès des opérateurs, sous peine de sanction pénale. Il s'agit alors d'un blocage par DNS.

Enfin, l'article L. 521-3-1 du code de la consommation confère aux agents de l'autorité administrative chargée de la concurrence et de la consommation la possibilité d'enjoindre aux offices et bureaux d'enregistrement des noms de domaine de procéder au blocage d'un nom de domaine, de supprimer celui-ci ou de le transférer à cette autorité.

1.2. CADRE CONSTITUTIONNEL

Les dispositions envisagées ont pour objet de prévenir des menaces susceptibles de porter atteinte à la sécurité nationale. Elles poursuivent donc l'objectif de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation[343].

1.2.1. Les principes constitutionnels de liberté de communication et de liberté d'entreprendre

[342] Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée.

[343] CC, 10 novembre 2011, *Mme Ekaterina B., épouse D., et autres*, n° 2011-192 QPC ; CE, 30 décembre 2021, *La quadrature du net et autres*.

Le Conseil constitutionnel a pu affirmer à plusieurs reprises que l'accès à l'internet est une manifestation de la liberté de communication consacrée à l'article 11 de la Déclaration des droits de l'homme et du citoyen (DDHC) mais aussi de la liberté d'entreprendre visée à l'article 4 de la DDHC[344]. Il a aussi affirmé dans une décision du 6 octobre 2010 que le choix et l'usage des noms de domaine faisaient l'objet d'une protection constitutionnelle : *« en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne »,* leur encadrement *« affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre »*[345].

Pour s'assurer de la constitutionnalité d'une disposition législative limitant un droit ou une liberté, le Conseil constitutionnel s'assure d'abord que la mesure envisagée poursuive un objectif autorisé. Les dispositions envisagées visant à faire cesser les agissements malveillants qui passent par le système DNS et constituent une menace susceptible de porter atteinte à la sécurité nationale, il ne fait guère de doute que tel est le cas ici.

Il faut ensuite que l'atteinte portée aux droits et libertés soit proportionnée à l'objectif poursuivi. Pour s'en assurer, le Conseil constitutionnel met en œuvre un triple test de proportionnalité, à l'occasion duquel il contrôle la nécessité, l'adaptation et la proportionnalité *stricto sensu* de l'atteinte[346]. La condition de l'adaptation est ici remplie, puisque la mesure envisagée permet d'atteindre le but de sécurisation des systèmes d'information. L'atteinte aux libertés qu'elle est susceptible d'entraîner est nécessaire au regard de l'évolution des menaces et parce que, comme développé *supra*, il n'existe pas, dans le droit positif, d'autres outils juridiques permettant de réaliser l'objectif poursuivi. Enfin, elle est proportionnée en ce que l'atteinte aux libertés est limitée à ce qui est strictement nécessaire et que la mise en œuvre du dispositif est entourée de garanties (voir *infra*, point 3.2.2.).

Cette conclusion est corroborée par la jurisprudence passée du Conseil constitutionnel. Comme cela a été exposé *supra* (1.1.2.), il existe une proximité en termes de moyens d'action entre les mesures déjà prévues en droit positif et la mesure envisagée. Elles portent des atteintes équivalentes à la liberté de communication et à la liberté d'entreprendre, à tel titre que le juge sera amené à apprécier de manière similaire leur proportionnalité[347].

De surcroît, le dispositif envisagé n'implique aucune appréciation du contenu du site par l'autorité administrative, à la différence des certaines mesures de filtrage existantes qui supposent d'apprécier l'existence d'une infraction pénale. En l'espèce, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sera amenée à se référer à des éléments

[344] Cons. const., déc. 10 juin 2009, n° 2009-580 DC ; Cons. const., déc. 6 oct. 2010, n° 2010-45 QPC.

[345] Cons. const., déc. 6 oct. 2010, n° 2010-45 QPC.

[346] Cons. const., déc. 10 mars 2011, n° 2011-625 DC.

[347] Cf. notamment Cons. const., déc. 10 mars 2011, n° 2011-625 DC et CE, 15 févr. 2016, Association French Data Network, n° 389140 et n° 389896.

techniques objectivables permettant de caractériser et neutraliser les menaces et attaques informatiques détectées.

Ces éléments techniques, à prévoir par un texte réglementaire, pourront par exemple s'apparenter à ceux visés par l'article R. 9-12-6 du code des postes et des communications électroniques pour l'application de l'article L. 2321-2-1 du code de la défense et contrôlés par l'ARCEP (éléments de nature à justifier l'existence de la menace susceptible de porter atteinte à la sécurité des systèmes d'information).

1.2.2. Le principe constitutionnel d'égalité devant les charges publiques

Le Conseil constitutionnel examine les obligations légales imposées aux acteurs privés à la lumière du principe d'égalité devant les charges publiques qui résulte de l'article 13 de la Déclaration de 1789 et selon lequel « *pour l'entretien de la force publique, et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens, en raison de leurs facultés* ».

Outre le domaine fiscal, le Conseil constitutionnel juge de façon constante que, *« [s]i cet article n'interdit pas de faire supporter, pour un motif d'intérêt général, à certaines catégories de personnes des charges particulières, il ne doit pas en résulter de rupture caractérisée de l'égalité devant les charges publiques »*[348].

Les mesures proposées sont susceptibles d'engendrer des surcoûts à la charge des FAI, des hébergeurs ou de l'office d'enregistrement des noms de domaine en « .fr » ou des bureaux d'enregistrement établis sur le territoire français. Bien qu'elles ne soient pas entièrement étrangères à leur activité, elles ne s'imposeront cependant pas de la même manière à tous les acteurs, à tel titre que le choix a été privilégié de les compenser. Le montant de la compensation de ces surcoûts pourrait être déterminé après consultation des entités concernées au regard de leurs pratiques existantes (coût d'un blocage, prix d'un transfert de nom de domaine qui va de 2 à 100 euros par an et par nom de domaine pour une dizaine de demandes par an, etc.).

1.3. CADRE CONVENTIONNEL

Le **principe de neutralité d'Internet**, consacré en droit positif[349], garantit l'égalité de traitement des contenus sur Internet, et donc leur libre circulation. Il est, notamment, affirmé

[348] Cons. const., déc. du 24 janvier 2020, n° 2019-821 QPC.

[349] Principe introduit en droit interne par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique et prévu à l'article L. 33-1 du code des postes et des communications électroniques.

par le règlement (UE) 2015/2120 du 25 novembre 2015[350] et interprété pour la première fois par la Cour de justice de l'Union européenne (CJUE) dans une décision du 15 septembre 2020[351].

Néanmoins, le principe de neutralité d'Internet n'est pas absolu. Le règlement (UE) 2015/2120 précité prévoit des exceptions à ce principe, qui sont mentionnées au paragraphe 3 de son article 3 et explicitées aux considérants 13 à 15 de son Préambule. En particulier, les fournisseurs de services d'accès à Internet pourront prendre diverses mesures, notamment le blocage de certains contenus, pour se conformer aux actes législatifs de l'Union ou à la législation nationale qui est conforme au droit de l'Union, auxquels ces fournisseurs sont soumis, ou aux mesures, conformes au droit de l'Union, donnant effet à ces actes législatifs de l'Union ou à cette législation nationale, y compris les décisions d'une juridiction ou d'une autorité publique investie des pouvoirs nécessaires.

Ainsi le principe ne fait-il pas obstacle à la mise en place de dispositifs législatifs de restriction d'accès à un service de communication au public en ligne, s'ils sont justifiés par un impératif de sauvegarde de l'ordre public. En France, l'article L. 33-1 du CPCE dispose par exemple que *« I. L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve du 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 incidents de sécurité ayant eu un impact significatif sur leur fonctionnement ; […] e)* ***Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique****, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ».*

Les restrictions d'accès qui résulteront de l'application de la disposition ici envisagée entreront donc dans le champ de l'exception prévue au a) du 3 de l'article 3 du règlement 2015/2120.

---

[350] Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union : *« Le présent règlement vise à établir des règles communes destinées à garantir un traitement égal et non discriminatoire du trafic dans le cadre de la fourniture de services d'accès à l'internet et les droits correspondants des utilisateurs finaux. Il vise à protéger les utilisateurs finaux et à garantir, en même temps, la continuité du fonctionnement de l'écosystème de l'internet en tant que moteur de l'innovation ».* Les utilisateurs ont, ainsi, droit « *d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet* », tandis que les FAI ont le devoir de traiter « *tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés* ».

[351] CJUE 15 septembre 2020, *Telenor*, affaires jointes C-807/18 et C-39/19.

1.4. ELEMENTS DE DROIT COMPARE

D'autres pays ont mis en place des solutions fondées sur des résolveurs DNS afin de lutter contre les cyberattaques et la cybercriminalité. En revanche, les cybermenaces ciblées par ces dispositifs peuvent varier en fonction des Etats.

Ainsi, les projets britanniques et américains visent à préserver leurs administrations des cyberattaques (sites reconnus comme malveillants) ainsi que contre les risques d'espionnage des requêtes et les attaques informatiques d'usurpation de requête DNS. Les solutions belge et canadienne ont élargi le périmètre à différents types d'arnaques en ligne (sites frauduleux, logiciels, malveillants, hameçonnage pour le Canada et concernant le BAPS, tous types d'hameçonnage en dehors du camp des domaines hébergeant du contenu) pour le grand public.

2. NECESSITE DE LEGIFERER ET OBJECTIF POURSUIVI

2.1. NECESSITE DE LEGIFERER

Cette disposition doit être adoptée au niveau législatif, eu égard, d'abord, à son impact sur l'activité des opérateurs. La disposition vient en effet préciser les mesures susceptibles d'être enjointes, la manière dont ces mesures sont contrôlées et les modalités de compensation des surcoûts pour lesdits opérateurs.

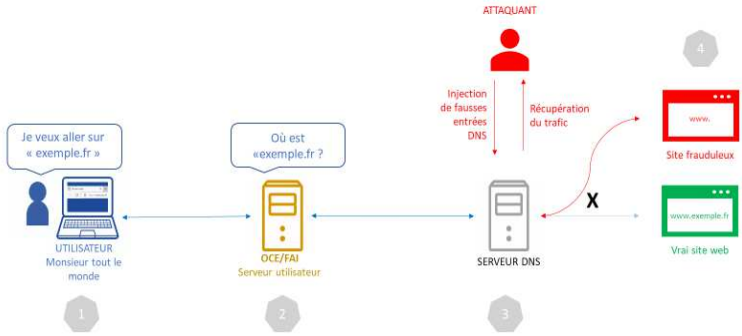
De plus, la disposition est susceptible de s'inscrire dans le champ de l'une des exceptions au principe de la neutralité d'Internet imposé par le règlement UE du 25 novembre 2015 et le code des postes et des communications électroniques, celle des mesures de cyberdéfense.

Une disposition législative est donc nécessaire pour définir un cadre et apporter les garanties suffisantes afin d'éviter les atteintes disproportionnées aux libertés publiques (liberté d'entreprendre, liberté de communication) et au principe de neutralité de l'Internet.

2.2. OBJECTIF POURSUIVI : LA SECURISATION DU SYSTEME DNS

Aujourd'hui, la grande majorité des attaques informatiques ont impliqué l'usage du DNS[352] en employant les noms de domaine sans que la sécurisation mise en œuvre par les acteurs du système et les éventuelles offres commerciales de filtrage ne soient suffisantes pour protéger les victimes. Par exemple, un attaquant peut dérouter le flux d'un domaine particulier vers un site Internet malveillant qu'il contrôle (la correspondance entre le nom de domaine et l'adresse IP n'est plus celle initialement définie et valide) afin de se faire passer pour le site originel ou de perturber l'activité du site en question, voire l'empêcher.

[352] La plupart des 831 incidents qui ont été traités par l'ANSSI en 2022 ont impliqué l'usage du DNS.



Exemple d'une vulnérabilité du DNS

Les réformes successives ont permis de mettre à la charge des acteurs, et notamment des FAI et des hébergeurs, un certain nombre d'obligations de sécurisation des systèmes d'information[353] (règles de sécurité des systèmes d'information). La disposition envisagée conduirait à les associer davantage, en lien avec l'ANSSI, à des opérations de cyberdéfense, qui s'avèrent aujourd'hui toujours plus nécessaires au regard de cette menace croissante. Les opérateurs contribueraient ainsi à assurer aux utilisateurs finaux un flux sécurisé de données dans le cadre de leur navigation sur Internet.

Cela permettrait également une augmentation significative des capacités nationales de détection des attaques informatiques et donnerait à l'ANSSI la capacité de neutraliser des menaces graves et avérées susceptibles d'affecter la sauvegarde de la sécurité nationale.

Une demande aux hébergeurs de données et aux FAI de procéder au blocage ou à la redirection d'un nom de domaine entièrement maîtrisé par un attaquant vers un serveur neutre permettrait d'informer les usagers de la suspension du nom de domaine.

Une redirection vers un serveur sécurisé permettrait à l'ANSSI d'observer le comportement malveillant pour en identifier les marqueurs et alerter les victimes.

En outre, demander à l'office d'enregistrement et aux bureaux d'enregistrement de procéder à l'enregistrement, au renouvellement, à la suspension ou au transfert des noms de domaine concernés permettrait de s'assurer que le blocage ne peut pas être contourné.

Enfin, la possibilité pour l'ANSSI d'alerter les victimes d'une compromission ou d'une vulnérabilité contribuera au renforcement général du niveau de sécurité.

[353] L'article L. 2321-2-1 du code de la défense permet à l'ANSSI de mettre en œuvre des dispositifs de détection sur le serveur d'un hébergeur, un FAI ou d'un OCE lorsqu'elle a connaissance d'une menace afin de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information Autorité publiques, des OIV ou des OSE. L'ANSSI peut recueillir des données et analyser les seules données techniques pertinentes (capture de trafic) et uniquement pour caractériser la menace. Sur le fondement de l'article L. 33-14 alinéa 2 du CPCE, l'ANSSI peut demander aux OCE d'exploiter, sur leurs propres dispositifs de détection, des marqueurs techniques qu'elle leur fournit pour caractériser une attaque sur des OIV, OSE ou AP.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Une option envisagée consistait à ajouter un article à la LCEN (dispositif Pharos). S'agissant du périmètre de la mesure, cette option présentait l'avantage de viser certains opérateurs communs (FAI et hébergeurs notamment), mais pas les registrars.

De plus, le dispositif Pharos ne poursuit pas la même finalité puisqu'il vise, dans le domaine de l'économie numérique et non de la sécurisation des systèmes d'information, à lutter contre des contenus illicites susceptibles de constituer des infractions pénales.

Enfin, en matière de lisibilité et de sécurité juridique, les compétences de l'ANSSI en tant qu'autorité de défense des systèmes d'information sont concentrées dans le code de la défense.

Cette option est apparue, pour ces différentes raisons, insatisfaisante.

Une seconde option consistait à modifier l'article L. 33-1 et l'article D. 98-7 du CPCE. Ces articles déjà existants auraient pu théoriquement fonder le dispositif mais, au regard de sa portée et du risque d'atteinte aux libertés publiques, un niveau législatif a été privilégié.

De surcroît, les dispositifs de filtrage existants dans d'autres domaines sont du niveau loi.

Enfin, comme rappelé précédemment, en matière de lisibilité et de sécurité juridique, les compétences de l'ANSSI en tant qu'autorité de défense des systèmes d'information sont concentrées dans le code de la défense.

Aucune option à droit constant ne semble donc permettre de prévenir ni de remédier efficacement aux attaques commises par le truchement du DNS.

3.2. OPTION RETENUE

La présente disposition dote l'ANSSI du pouvoir de demander le filtrage de noms de domaine utilisés ou instrumentalisés par des cyber-attaquants. Sa mise en œuvre est conditionnée par le constat préalable d'une menace susceptible de porter atteinte à la sécurité nationale.

La distinction entre deux types de mesures de filtrage procède en particulier du critère de la bonne foi du titulaire du nom de domaine.

Si le titulaire n'est pas à l'origine de l'utilisation dévoyée de son nom de domaine, il existe alors une gradation des mesures :

- dans un premier temps, l'ANSSI peut enjoindre à celui-ci de prendre, dans un délai qu'elle lui impartit, les mesures adaptées pour neutraliser la menace ;
- s'il n'a pas pris les mesures adaptées dans le délai énoncé, l'ANSSI peut demander le blocage ou la suspension du nom de domaine concerné.

A contrario, si le titulaire du nom de domaine a précisément enregistré celui-ci à des fins d'attaque, les mesures de filtrage pourraient aller jusqu'à :

- la redirection, du nom de domaine concerné vers un serveur neutre ou sécurisé et maîtrisé par l'ANSSI ;
- ainsi qu'à l'enregistrement, au renouvellement, à la suspension, ou au transfert à l'ANSSI du nom de domaine, qui en devient dans ce dernier cas le titulaire.

En dépit d'une proximité en termes de moyens d'action, notamment concernant le blocage par DNS, les mesures préexistantes ne partagent avec la disposition envisagée ni l'élément déclencheur (contenu illicite, atteinte au droit d'auteur, absence d'autorisation pour un opérateur de jeu en ligne ou altération de la sincérité du scrutin) ni les finalités (lutte contre le terrorisme, la pédopornographie ou les pratiques commerciales trompeuses).

3.2.1. Présentation du dispositif

Le dispositif envisagé vise à sécuriser le système de noms de domaine contre les agissements d'acteurs malveillants. Les mesures proposées ne seront mises en œuvre qu'en cas de menace susceptible de porter atteinte à la sécurité nationale. Celle-ci est identifiée par l'ANSSI au moyen de « marqueurs techniques » utilisés dans le cadre de ses missions, définis à l'article R. 9-12-2 du code des postes et des communications électroniques (CPCE) comme des *« éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante ou d'identifier une menace susceptible d'affecter la sécurité des systèmes d'information »*. L'ANSSI identifie de manière quotidienne des noms de domaines utilisés par des attaquants, ces noms de domaine constituant eux-mêmes des marqueurs techniques. Elle procède de la même manière pour caractériser une menace en application de l'article L. 2321-2-1 du code de la défense (CODEF) et en justifier l'existence auprès de l'Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la presse (ARCEP)[354].

Une distinction est faite selon que le nom de domaine malveillant a été enregistré de bonne foi par son propriétaire légitime ou qu'il a été enregistré dans le seul but de compromettre la sécurité des systèmes d'information, cela afin de limiter les conséquences qu'une mesure de filtrage pourrait avoir sur le propriétaire d'un nom de domaine sans intention de commettre une attaque informatique.

Lorsqu'est identifié un propriétaire qui a enregistré le nom de domaine de bonne foi, l'ANSSI peut, dans un premier temps, lui demander de prendre les mesures adaptées pour neutraliser les effets de l'attaque commise au moyen de son nom de domaine. Si le propriétaire ne prend pas ces mesures dans le délai imparti, l'ANSSI peut, dans un second temps, ordonner aux hébergeurs et aux FAI de mettre en œuvre une mesure de blocage, ou enjoindre aux registres et bureaux d'enregistrement de suspendre le nom de domaine.

[354] Article R. 9-12-6 du CPCE.

Lorsque le nom de domaine est entièrement maîtrisé par un attaquant qui l'a enregistré dans le seul but de commettre des agissements malveillants, susceptibles de porter atteinte à la sécurité nationale, la menace justifie que l'ANSSI puisse agir sans délai. Elle peut alors enjoindre aux hébergeurs de données et aux FAI de procéder à son blocage ou à sa redirection vers un serveur neutre ou un serveur sécurisé.
Dans cette même hypothèse, l'ANSSI peut aussi enjoindre à l'office d'enregistrement et aux bureaux d'enregistrement de procéder à l'enregistrement, au renouvellement, à la suspension ou au transfert des noms de domaine concernés.

La redirection avec phase d'observation, qu'il s'agisse d'une redirection par les hébergeurs ou les FAI vers un serveur sécurisé et maîtrisé par l'ANSSI, ou d'une redirection à partir d'un nom de domaine récupéré et maîtrisé directement par l'ANSSI, permet d'observer le mode opératoire de l'attaquant et d'identifier, *in fine*, de nouvelles victimes.

3.2.2. Les garanties prévues

Des mesures adaptées à la spécificité de la situation

Une mesure de filtrage est susceptible d'avoir des conséquences préjudiciables pour le propriétaire d'un nom de domaine légitime qui est utilisé comme un vecteur d'attaque. Aux fins d'assurer la conciliation entre la sauvegarde de la sécurité nationale, d'une part, et la liberté d'entreprendre et la liberté de communication, d'autre part, il est d'abord prévu que l'ANSSI demande au propriétaire légitime de prendre des mesures ciblées pour éviter des conséquences négatives en termes d'accessibilité de son site internet (suppression ciblée d'une ressource du site internet comme une page, un contenu etc.), et ce dans un délai imparti.

Ce n'est qu'à l'expiration du délai imparti au propriétaire pour agir, lorsque ce dernier n'a pas pris les mesures adaptées, qu'elle peut demander le blocage auprès des FAI ou des hébergeurs, ou la suspension du nom de domaine (c'est-à-dire la suspension de tout le site internet) auprès de l'office d'enregistrement des noms de domaine en « .fr » ou des bureaux d'enregistrement établis sur le territoire français.

Seule l'hypothèse d'un nom de domaine enregistré exclusivement à des fins malveillantes par l'attaquant ou un prête-nom présentant une menace susceptible de porter atteinte à la sécurité nationale justifiera que l'ANSSI prenne des mesures de façon immédiate en s'adressant aux mêmes acteurs que visés dans le paragraphe précédent.

Lorsque la menace requerra une mesure aux fins de caractérisation de la menace, celle-ci sera entourée de garanties supplémentaires afin d'encadrer la collecte des données utiles et leur utilisation (cf. *infra*).

La limitation matérielle et temporelle des mesures

Quant à leur contenu et leur durée, les mesures prises sont strictement nécessaires et proportionnées à l'objectif précis poursuivi, à savoir la prévention, la caractérisation et la neutralisation de la menace.

Par ailleurs, la phase d'observation à la suite de la redirection par les hébergeurs ou les FAI vers un serveur sécurisé et maîtrisé par l'ANSSI est limitée à un délai de deux mois, renouvelable une fois en cas de persistance de la menace après avis conforme de l'ARCEP.

Le contrôle de l'ARCEP et la voie de recours devant le juge administratif

Les nouvelles prérogatives accordées à l'ANSSI sont assorties d'un contrôle *a posteriori* par une autorité administrative indépendante, l'ARCEP. Compte-tenu de ses compétences dans le secteur des communications électroniques et afin d'assurer la cohérence globale du dispositif, elle apparaît la mieux à même de vérifier le respect de ses conditions d'application. Par ailleurs, l'ARCEP a déjà été désignée comme autorité chargée du contrôle des activités de l'ANSSI dans le cadre de la mise en œuvre des articles L. 2321-2-1 et L. 2321-3 alinéa 2 du code de la défense.

Comme présenté *supra*, le renouvellement des mesures de redirection est soumis à un avis conforme de l'ARCEP. Il est entendu que ce contrôle de l'ARCEP portera également sur la justification de la menace et la proportionnalité de la mesure.

Les injonctions de l'ANSSI visant à demander aux FAI, aux hébergeurs, à l'office ou aux bureaux d'enregistrement ces mesures de filtrage seront, comme tout acte administratif unilatéral, susceptibles de recours devant le juge administratif, conformément à l'article L. 411-2 du code des relations entre le public et l'administration (CRPA), et ce y compris en référé.

La collecte de données en phase d'observation

La collecte et la conservation de certaines données techniques strictement nécessaires pour caractériser les attaques informatiques (telles par exemple les adresses IP source et destination, les types de protocoles utilisés, les métadonnées de sessions de navigation, le nombre et la taille des paquets échangés) est déjà prévue à l'article L. 2321-3, alinéa 2, du code de la défense.

Les données dont l'exploitation est nécessaire à la compréhension des modes opératoires des attaquants ne seront obtenues et exploitées qu'à des fins de défense des systèmes d'information et uniquement en cas de menace susceptible de porter atteinte à la sécurité nationale. Les finalités du dispositif, à savoir la caractérisation, la neutralisation des attaques et l'information des victimes, ne nécessitent pas d'accéder à des données de contenu. Les données collectées sont détruites dans un délai de dix ans à compter de la date de la collecte. Enfin, l'ANSSI détruit sans délai toute donnée qui ne serait pas strictement nécessaire à la prévention, la caractérisation et la neutralisation des effets d'une attaque informatique.

Par ailleurs, le dispositif mis en place par l'ANSSI ayant notamment pour objectif d'alerter les victimes des attaques, elle devra préalablement les identifier, ce qui implique de fait la collecte et le traitement de données à caractère personnel dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Il est proposé l'ajout d'un article L. 2321-2-3 dans le code de la défense.

Par ailleurs, par le truchement de l'article 35 du présent projet de loi et afin d'énoncer les modalités de contrôle de l'ARCEP sur la mise en œuvre du dispositif ainsi créé, les articles L. 2321-5 du code de la défense et L. 36-7, L. 36-14 et L. 130 du CPCE sont modifiés.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Le règlement (UE) 2015/2120 précité prévoit des exceptions au principe de neutralité d'Internet qui sont mentionnées au paragraphe 3 de son article 3 et explicitées aux considérants 13 à 15 de son Préambule. En particulier, les fournisseurs de services d'accès à Internet pourront prendre diverses mesures, notamment le blocage de certains contenus, pour se conformer aux actes législatifs de l'Union ou à la législation nationale qui est conforme au droit de l'Union, auxquels ces fournisseurs sont soumis, ou aux mesures, conformes au droit de l'Union, donnant effet à ces actes législatifs de l'Union ou à cette législation nationale, y compris les décisions d'une juridiction ou d'une autorité publique investie des pouvoirs nécessaires.

De telles exceptions figurent dans les mêmes termes dans la déclinaison française du règlement (article L. 33-1 du CPCE)[355].

En tant qu'elle tend à assurer la sécurité des systèmes d'information, la disposition ici envisagée entre donc dans le champ des exceptions prévues par le règlement européen sur la neutralité de l'Internet et par la loi nationale.

[355] *« I. - L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve du 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 incidents de sécurité ayant eu un impact significatif sur leur fonctionnement ; […]

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

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Cette mesure vise à renforcer la capacité d'action de l'autorité nationale de sécurité des systèmes d'information. Elle n'affecte pas les prestations commerciales qui pourraient être offertes par des entités privées, il n'y a donc pas d'impact sur le marché au niveau macro-économique.

4.2.2. Impacts sur les entreprises

Cette mesure imposant de nouvelles obligations mais non de nouveaux investissements pour les FAI, les hébergeurs, l'office d'enregistrement des noms de domaine en « .fr » ou les bureaux d'enregistrement établis sur le territoire français, il est prévu une compensation des surcoûts que ces demandes peuvent générer pour ces entités.

Il convient de mentionner que certains FAI étrangers (British Telecom, Telstra) ont déjà mis en place des mesures de sécurité par défaut[356]. Plus récemment, une étude de juillet 2020 de l'*Australian Strategic Policy Institute* évoque le fait que les FAI pourraient être obligés ou incités à prendre certaines mesures de sécurité proactives de type blocage de certains sites ou suppression du trafic illégitime ou usurpé[357].

4.2.3. Impacts budgétaires

L'impact budgétaire pour l'Etat de la compensation des surcoûts apparaît limité compte tenu des prix actuellement pratiqués sur le marché de l'enregistrement de noms de domaines.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Eu égard aux obligations nouvelles qui pèseraient sur les FAI, les hébergeurs, l'office d'enregistrement des noms de domaine en « .fr » ou les bureaux d'enregistrement établis sur le territoire français, il est prévu une extension des missions de contrôle *a posteriori* de l'ARCEP pour veiller au respect des finalités recherchées.

[356] https://www.ncsc.gov.uk/blog-post/bts-proactive-protection-supporting-ncsc-make-our-customers-safer.
[357] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette disposition va contribuer à renforcer la sécurité des systèmes d'information en France par la sécurisation du système de noms de domaine contre les agissements d'acteurs malveillants en cas de menace susceptible de porter atteinte à la sécurité nationale. Il permettra de neutraliser l'utilisation dévoyée d'un nom de domaine par un cyber attaquant, d'améliorer la compréhension des modes opératoires d'attaque et donc, d'agir en conséquence.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

En cas de blocage de nom de domaine, les particuliers n'accèdent plus aux pages concernées. Pour autant, la mise en œuvre des mesures n'est prévue que dans des hypothèses de menaces susceptibles de porter atteinte à la sécurité nationale, ce qui autorise à penser que l'impact pour les particuliers est mesuré.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément à l'article L. 36-5 du code des postes et des communications électroniques, cette disposition a été présentée à l'Autorité de régulation des communications électroniques (ARCEP) qui a rendu son avis le 9 mars 2023[358].

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Les conditions d'application du dispositif proposé seront définies par décret en Conseil d'Etat.

[358] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2024-2030.

Article 33 : Prévoir la communication à l'ANSSI de certaines données techniques de cache de serveurs de systèmes de noms de domaines (DNS)

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Le « Domain Name System » (système de nom de domaine) ou DNS est un service permettant de faire correspondre un nom de domaine à une adresse IP (Internet Protocol) – le numéro attribué à titre permanent ou provisoire à chaque périphérique relié à Internet, adresse qui prend la forme d'une suite de numéros (par exemple, « 45.60.12.53 ») et est compréhensible par une machine.

Les machines qui reçoivent les demandes de résolution de noms de domaine (traduction d'un nom de domaine en adresse FQDN) sont appelées des « résolveurs DNS (pour *Domain Name System*) ». Il existe des résolveurs DNS spécialisés par périmètre (téléphonie mobile, secteur d'activité, *etc*.) chez les opérateurs de communications électroniques.

Afin de gagner du temps pour retourner une réponse à l'utilisateur, les résolveurs DNS conservent les correspondances entre les adresses IP (*Internet Protocol*) et les noms de domaine de manière temporaire : c'est ce que l'on appelle les données de cache. En effet, si des utilisateurs différents effectuent une même demande de nom de domaine, le résolveur DNS n'a plus à interroger les différents serveurs de noms de domaine puisqu'il a déjà conservé l'information. Ces serveurs disposent ainsi des données suivantes :

- l'adresse IP source, c'est-à-dire l'adresse IP de la machine de l'utilisateur qui fait la demande de résolution de nom de domaine en adresse IP ;
- le nom de domaine demandé (le nom de domaine (URL ou *Uniform Resource Locator* en français, « localisateur uniforme de ressource », sous la forme « exemple.fr »), plus facile à retenir et à retranscrire pour l'internaute, constitue l'alias alphanumérique de l'adresse IP) ;
- la date de la demande (horodatage) ;
- les adresses IP des différentes machines interrogées. Contrairement aux adresses IP source, ces IP n'identifient pas indirectement des individus mais uniquement des machines.

On appelle fournisseur de système de résolution de noms de domaine toute personne mettant à disposition un service permettant la traduction d'un nom de domaine en un numéro unique identifiant un appareil connecté à Internet.

A ce jour, aucun texte ne propose cependant de définition d'un fournisseur de système de résolution de noms de domaine, ni ne permet à une autorité de s'adresser à ces fournisseurs ou aux opérateurs de communications électroniques pour obtenir une copie d'une partie des

données de cache (uniquement celles qui sont non identifiantes) que ces acteurs conservent de manière temporaire pour des besoins liés à une meilleure qualité de service.

1.2. CADRE CONSTITUTIONNEL

Le fait pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de récupérer des données n'est pas susceptible de porter atteinte aux libertés individuelles dans la mesure où elle ne collecterait pas les adresses IP source, qui sont les seules à permettre d'identifier indirectement des personnes physiques. Il est donc impossible pour elle de déterminer ou de suivre les utilisateurs qui essayent d'accéder aux différentes ressources (accès demandés à tel ou tel nom de domaine). L'ANSSI ne collectera que des données de serveurs, c'est-à-dire de machines derrière lesquelles il n'y a pas de personne physique. Cette disposition n'affecte donc pas le droit au respect de la vie privée, pas davantage que la liberté d'expression et de communication.

Afin d'éviter que l'ANSSI ne collecte davantage de données que les données techniques dont elle a besoin pour caractériser une attaque, l'ARCEP contrôlera, à travers un accès permanent à la base stockant ces données, que les données collectées sont bien celles que l'ANSSI a le droit de collecter et uniquement celles-ci. De plus, elle pourra également contrôler que les personnes qui ont collecté ces données au sein de l'ANSSI sont bien les agents qui ont été individuellement désignés et spécialement habilités pour le faire.

Par ailleurs, l'impact sur les libertés économiques est également très modeste : les opérateurs de communications électroniques et les fournisseurs de systèmes de résolution de noms de domaine se bornent à transmettre à l'ANSSI des données qu'ils collectent déjà dans le cadre de leur activité propre.

Il résulte de ce qui précède que cette disposition, nécessaire pour améliorer les capacités de cyberdéfense, n'affecte pas ces droits et libertés de manière disproportionnée aux buts qu'elle poursuit.

1.3. CADRE CONVENTIONNEL

Cette disposition n'affecte pas le droit au respect de la vie privée, protégé par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Par ailleurs, elle n'affecte que très marginalement les libertés économiques protégées par la Charte des droits fondamentaux de l'Union européenne, d'une manière proportionnée aux buts poursuivis d'amélioration des capacités françaises de cyberdéfense.

1.4. ELEMENTS DE DROIT COMPARE

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le DNS est une infrastructure essentielle d'Internet. A ce titre, elle est très utilisée par les attaquants[359] qui peuvent utiliser des noms de domaine pour gérer leur infrastructure d'attaque. En observant leur usage du DNS, il est possible d'obtenir des informations sur leur infrastructure et ses évolutions.

A ce jour, il n'existe pas de cadre juridique permettant à un OCE ou à un fournisseur de système de résolution de noms de domaine de fournir à l'ANSSI une copie des journaux des requêtes DNS (données de cache ou historique des évènements) faites par leurs clients.

Le dispositif envisagé permettrait à l'ANSSI de connaître les requêtes DNS qui ont été effectuées par les clients, légitimes et malveillants, de manière anonymisée, pour identifier l'infrastructure de l'attaquant et suivre son activité. On pourrait, par exemple, considérer une situation opérationnelle dans laquelle les attaquants mettraient en place des serveurs d'attaque spécifiques pour leurs victimes en France. Une entrée du résolveur (ou journaux) pourrait être collectée pendant les recherches. Par ce biais, l'ANSSI pourrait alors accéder aux données relatives à la requête DNS, son horodatage et au résolveur ayant résolu la requête. Les résolveurs étant spécialisés par périmètre (téléphonie mobile, secteur d'activité, etc.) chez les OCE et les fournisseurs de système de résolution de noms de domaine, les données obtenues par l'ANSSI permettraient de caractériser plus finement l'attaque et la stratégie de l'attaquant.

Par ailleurs, dans les secteurs du stockage de fichiers, de la messagerie ou de la bureautique, la tendance est à un recours croissant à l'informatique en nuage (cloud computing[360]) des fournisseurs de système de résolution de noms de domaine. Or les échanges entre Internet et les services en nuage sont chiffrés, ce qui empêche le suivi des attaquants usuellement réalisé par l'ANSSI. Fournir à l'ANSSI un accès à une partie de l'information contenue dans les caches DNS de ces fournisseurs lui confèrera une certaine visibilité sur les activités d'acteurs malveillants.

Ainsi, et dans la mesure où le dispositif envisagé, en imposant à des entreprises de communiquer à l'ANSSI une copie de journaux des requêtes DNS de leurs clients, est susceptible de restreindre la liberté d'entreprendre, il nécessite de prendre une mesure législative. Cette mesure implique ainsi de modifier la partie législative du code de la défense.

[359] La grande majorité des 831 incidents traités par l'ANSSI en 2022 impliquait l'usage du DNS.

[360] Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire.

Un tel niveau de norme est également nécessaire pour introduire un contrôle *a posteriori* de l'ARCEP sur la collecte des données considérées.

2.2. OBJECTIFS POURSUIVIS

La disposition vise à améliorer la connaissance des modes opératoires des cyber-attaquants qui utilisent les noms de domaines pour mener leurs attaques informatiques, en permettant notamment d'identifier les serveurs mis en place par les attaquants et de remonter la chronologie de leurs attaques.

Plus précisément, les finalités poursuivies par cette mesure sont les suivantes :

- renforcer et compléter la base de connaissances de la menace. En effet, disposer de ces sources permettrait de compléter les informations de résolutions DNS obtenues à partir d'autres sources de données passives DNS plus classiques (base de données historique du *Computer Incident response center Luxembourg* ou CIRCL, *domain tools*), étant noté qu'aucune IP source n'est collectée non plus par ces acteurs ;
- renforcer la capacité de détection de l'ANSSI vis-à-vis de comportements malveillants réalisés sur le territoire national (plus particulièrement sur des serveurs présents sur le territoire national) ;
- affiner la capacité de qualification lors de l'analyse de la menace.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Nulle autre option à droit constant ne permet d'obtenir l'objectif visé car seuls les opérateurs concernés disposent de ces données.

3.2. OPTION RETENUE

La loi n° 2018-607 relative à la programmation militaire pour les années 2019-2025[361] a renforcé les capacités de l'ANSSI à accomplir ses missions en améliorant ses capacités de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés.

Le dispositif envisagé vise la communication de certaines données de cache de résolveurs DNS en s'appuyant sur les opérateurs de communications électroniques (OCE), parmi lesquels on trouve les fournisseurs d'accès Internet (FAI) et les fournisseurs de système de résolution de

[361] 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.

noms de domaine. En effet, ces opérateurs, au travers de leurs réseaux, connectent les systèmes d'information de leurs clients au réseau mondial et peuvent donc être amenés à faire transiter sur leurs réseaux des flux malveillants, notamment au moyen des résolveurs DNS qu'ils mettent à disposition de leurs clients.

La nouvelle disposition imposerait aux OCE et aux fournisseurs de système de résolution de noms de domaine de transmettre régulièrement à l'ANSSI leurs données de cache DNS anonymisées (uniquement le nom du serveur de réponse, son adresse IP ainsi que l'horodatage de la réponse) à des fins d'analyse et de caractérisation de la menace. En revanche, ces données seraient nettoyées de toute adresse IP source, seule susceptible de permettre indirectement l'identification d'un utilisateur, personne physique, et constituant de ce fait une donnée à caractère personnel au sens de la législation sur la protection des données à caractère personnel[362]. En effet, l'objectif n'est pas d'identifier l'auteur des requêtes faites au serveur mais uniquement le type de réseau utilisé par l'attaquant. Les OCE et les fournisseurs de système de résolution de noms de domaine devront donc mettre en place un moyen permettant de copier et de communiquer de façon récurrente les données de cache DNS préalablement anonymisées.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Un article L. 2321-3-1 est créé dans le code de la défense pour introduire la présente mesure.

Par ailleurs, afin de prévoir le contrôle *a posteriori* de l'ARCEP sur les données collectées par l'ANSSI, il est prévu à l'article 35 du projet de loi une modification du périmètre d'application des articles L. 2321-5 du code de la défense et L. 36-14 du code des postes et des communications électroniques.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Sans objet.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

[362] Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

4.2.2. Impacts sur les entreprises

Les OCE et les fournisseurs de système de résolution de nom de domaine réalisent d'ores et déjà les journaux de logs pour leurs besoins internes. De plus, les OCE doivent conserver ces données pour répondre à certaines obligations juridiques dans le cadre du code des postes et des communications électroniques. Il s'agirait uniquement d'envoyer une copie des données techniques non identifiantes à l'ANSSI. L'impact de cette mesure sera donc très limité : en termes de coûts, elle n'impliquera que le coût de mise en œuvre et de supervision du processus, notamment en cas d'automatisation du service.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Cette disposition confère à l'ANSSI de nouveaux moyens dans le cadre de sa mission de défense des systèmes d'information. Ses agents se verront transmettre les données de cache DNS, qu'ils pourront ainsi analyser.

L'ARCEP se voit par ailleurs confier la responsabilité de contrôler la mise en œuvre de ce nouveau dispositif par les agents de l'ANSSI.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette disposition permettra de renforcer la sécurité des systèmes d'information de l'ensemble des utilisateurs d'internet en France.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Cette disposition n'emporte aucun impact sur les particuliers. En effet, seules les adresses IP machine seront transmises aux agents de l'ANSSI. Or ces données, à l'inverse des adresses IP source, ne permettent pas d'identifier les personnes, même indirectement.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 36-5 du code des postes et des communications électroniques Cette disposition a été présentée à l'ARCEP qui a rendu son avis le 9 mars 2023[363].

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire de la République.

[363] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2024-2030.

5.2.3. Textes d'application

Les conditions d'application du dispositif proposé seront définies par décret en Conseil d'Etat, pris après avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Il déterminera notamment les données techniques transmises par les opérateurs aux agents de l'ANSSI.

Article 34 : Obliger les éditeurs de logiciel victimes d'un incident informatique sur leurs systèmes d'information ou ayant une vulnérabilité critique sur un produit ou un service à en informer l'ANSSI et leurs clients français

1. ÉTAT DES LIEUX

1.1. SITUATION ACTUELLE

De nombreux incidents observés par et rapportés à l'ANSSI au cours de l'année 2022 ont pour origine l'exploitation de vulnérabilités disposant pourtant de correctifs mis à disposition par les éditeurs et ayant fait l'objet d'avis ou de bulletins d'alerte, toujours disponibles sur le site du CERT-FR. Pour les plus critiques, ces publications ont été accompagnées de campagnes de signalement. Ces vulnérabilités concernent des logiciels particulièrement courants et utilisés par de très nombreuses organisations publiques comme privées. Certaines de ces vulnérabilités, parmi les plus exploitées, sont corrigées depuis 2021[364].

L'objectif est que les utilisateurs des logiciels soient bien informés des vulnérabilités et puissent prendre les bonnes mesures pour éviter des incidents.

Il n'existe pas, en l'état actuel du droit, de dispositif prévoyant que les éditeurs de logiciels déclarent à l'ANSSI et informent leurs utilisateurs des incidents ou vulnérabilités critiques affectant l'un de leurs produits ou systèmes d'information.

Le droit positif prévoit certes d'ores et déjà certaines obligations d'information pesant sur différents acteurs du numérique.

- **Les responsables de traitement de données personnelles** doivent :
    - Notifier à la Commission nationale de l'informatique et des libertés (CNIL) toute violation de données à caractère personnel qui présente un risque pour les droits et libertés des personnes physiques, avec une première analyse des circonstances de cette violation ainsi que les premières mesures mises en place pour l'endiguer[365] ;
    - Informer les personnes concernées de cette violation de données à caractère personnel, lorsqu'elle engendre un risque élevé pour leurs droits ou leurs libertés[366]. Si le responsable de traitement ne procède pas de lui-même à cette communication, la CNIL

[364] Cf. rapport menaces et incidents du CERT-FR.

[365] Article 33 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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) ; articles 58 et 83 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[366] Article 34 du RGPD ; articles 58 et 83 de la loi n° 78-17 précitée.

peut exiger qu'il le fasse[367]. Cette notification, d'abord applicable aux secteurs des communications électroniques, a été étendue à tous les responsables de traitement afin de les responsabiliser davantage s'agissant des mesures de sécurité à mettre en place sur leurs traitements de données à caractère personnel.

- **Certains acteurs de la cybersécurité**, comme :

  - les opérateurs d'importance vitale (OIV) doivent notifier à l'ANSSI tout incident touchant l'un de leurs systèmes d'information d'importance vitale[368] ; les opérateurs de services essentiels (OSE) ou les fournisseurs de services numériques (FSN), dès lors qu'un incident significatif touche l'un de leurs systèmes d'information nécessaires à la fourniture de ces services[369] ;
  - l'ANSSI prend des mesures d'information du public, pour les opérateurs de services essentiels (OSE) ou des fournisseurs de services numériques (FSN), ou par les fournisseurs de services numériques (FSN) à la demande de l'ANSSI, lorsque cette information est nécessaire pour prévenir ou traiter un incident (loi n° 2018-133 précitée).

Les opérateurs de communications électroniques doivent notifier à l'autorité compétente les incidents de sécurité ayant eu un impact significatif sur leur fonctionnement[370].

1.2. CADRE CONSTITUTIONNEL

Le Conseil constitutionnel peut être amené à examiner les obligations légales imposées aux sociétés à l'aune de la liberté d'entreprendre qui procède de l'article 4 de la Déclaration des droits de l'homme et du citoyen selon lequel : « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui* ». Le Conseil constitutionnel a confirmé, qu'elle comprend deux objets, à savoir : « *non seulement la liberté d'accéder à une profession ou à une activité économique mais également la liberté dans l'exercice de cette profession ou de cette activité* » (cons. n° 7)[371].

Il a notamment jugé que ne porte pas atteinte à la liberté d'entreprendre la loi qui crée une obligation déclarative pour certaines sociétés dans le but de transmettre à l'administration des informations relatives à leur implantation et des indicateurs économiques, comptables et fiscaux de leur activité[372].

---

[367] Article 58 du même règlement ; article 20 de la loi n° 78-17 précitée.

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

[369] Articles 7 et 13 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

[370] Article L. 33-1 du code des postes et des communications électroniques (CPCE).

[371] Décision n° 2012-285 QPC du 30 novembre 2012 (corporations d'Alsace-Moselle).

[372] Décision n° 2015-725 DC du 29 décembre 2015 (cons. 33, J.O. du 30 décembre 2015, p. 24763.

1.3. CADRE CONVENTIONNEL

La notification d'un incident procède en partie d'une dynamique imposée au niveau du droit de l'Union européenne, qu'il s'agisse d'incident portant sur les réseaux ou systèmes d'information[373] ou d'une violation des données à caractère personnel[374].

Néanmoins, il n'existe pas de texte de droit de l'Union européenne ou international permettant d'envisager une notification par les éditeurs de logiciels des incidents informatiques ou de vulnérabilités critiques affectant leurs produits et services, alors même que ces incidents et vulnérabilités sont susceptibles d'être le point d'entrée d'attaques menées sur les systèmes d'information des utilisateurs.

La liberté d'entreprendre est également garantie par l'article 16 de la Charte des droits fondamentaux de l'Union européenne. Cet article protège la liberté d'exercer une activité économique ou commerciale, la liberté contractuelle et la concurrence libre[375]. La Cour de justice de l'Union européenne (CJUE) juge sur son fondement que la liberté d'entreprise ne constitue pas une prérogative absolue mais peut être soumise à un large éventail d'interventions de la puissance publique susceptibles d'établir, dans l'intérêt général, des limitations à l'exercice de l'activité économique.

1.4. ELEMENTS DE DROIT COMPARE

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

Cette disposition doit être adoptée au niveau législatif dès lors qu'elle vient modifier la partie législative du code de la défense eu égard, d'abord, à son impact sur l'activité d'opérateurs que sont les éditeurs de logiciel.

En outre, la disposition vient en effet préciser l'obligation qui est la leur de notifier un incident informatique ou une vulnérabilité critique ainsi que la possibilité pour l'Agence nationale de la sécurité des systèmes d'information de leur enjoindre d'informer leurs utilisateurs en cas de risque d'atteinte à la sécurité des systèmes d'information de ces derniers.

[373] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) ; Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

[374] Ibid.

[375] CJUE, 22 janvier 2013, Sky Österreich, aff. C-283/11 ; CJUE, 17 octobre 2013, Schaible, aff. C-101/12 ; CJUE, 16 juillet 2020 OC e. a., aff. C-686/18.

La possibilité pour l'ANSSI de rendre publics cette vulnérabilité ou cet incident, ainsi que son injonction aux éditeurs si celle-ci n'a pas été mise en œuvre, relève également du domaine de la loi.

2.1. NECESSITE DE LEGIFERER

2.1.1. Les risques systémiques des vulnérabilités

Une vulnérabilité, *a fortiori* lorsqu'elle est significative, peut constituer, même lorsqu'elle concerne un système, un logiciel ou un service non caractérisé comme particulièrement sensible, un moyen indirect d'atteindre des entités elles-mêmes sensibles. Une telle vulnérabilité permet le pré-positionnement de potentiels attaquants en vue d'une cyberattaque.

Par exemple, les attaquants peuvent exploiter une vulnérabilité dans le cadre d'une attaque par rebond envers les utilisateurs recourant aux biens ou services de l'éditeur concerné, en vue d'une exfiltration, d'une modification ou du piégeage des données, ou encore d'une altération, voire de la destruction d'un système. Dans un tel cas de figure, le risque peut devenir systémique dans le cas d'un déploiement en masse sur l'ensemble d'un parc informatique d'un produit ou d'un service.

2.1.2. L'absence de base juridique pour prescrire une information des utilisateurs de biens ou services vulnérables

S'il existe une obligation de signalement aux personnes concernées des violations de données à caractère personnel (cf. 1.1 *supra*), il n'existe pas de cadre juridique équivalent concernant les données techniques générées lors d'activités malveillantes (par exemple en cas d'exfiltration de données, de sabotage, etc.) ou les vulnérabilités de produits.

Par conséquent, en l'absence d'effets sur les données à caractère personnel, les utilisateurs recourant aux produits fournis par des éditeurs de logiciel ne disposent pas de moyens juridiques pour être informés des éventuels risques qu'ils encourent en cas d'incident ou de vulnérabilité.

2.1.3. L'absence d'outils actuels mobilisables par l'ANSSI pour informer les utilisateurs

Actuellement, il est exclu que l'ANSSI soit autorisée à intervenir auprès de l'ensemble des utilisateurs recourant aux biens et services de ces éditeurs, son périmètre d'action se restreignant à l'Etat, aux autorités publiques et à certains opérateurs publics et privés.

L'Agence ne dispose pas non plus des moyens nécessaires pour informer ces utilisateurs, pour plusieurs raisons :

- les éditeurs de logiciels victimes d'incidents sont parfois réticents à l'idée de fournir à l'ANSSI la liste des utilisateurs recourant à leurs produits (au motif du secret des affaires) ;

– compte tenu de la confidentialité des listes des OIV et des OSE, l'ANSSI n'est pas non plus en mesure de fournir à la victime une liste ciblée d'entités sensibles à informer prioritairement.

2.1.4. L'efficacité de l'outil du signalement

Avant que le législateur européen ne se saisisse de la question des données à caractère personnel via le règlement général de protection des données (RGPD), les rares entreprises qui signalaient des violations relatives aux données à caractère personnel concernées par un incident informatique ou qui informaient de la découverte d'une vulnérabilité sur leurs produits ou services n'étaient mues que par des considérations réputationnelles.

La création d'obligations déclaratives par le RGPD a eu un effet de levier significatif sur le nombre de signalements. A titre d'illustration, dans son rapport annuel 2021, la CNIL indique une augmentation de 79 % des notifications de violations de données. Il est à noter que cette obligation a agi comme un accélérateur majeur de la sécurisation des entreprises. Pour la même année 2021, la CNIL indique que 81 393 organismes – privés et publics confondus – ont également désigné un délégué à la protection des données.

2.1.5. La nécessité d'intégrer l'ANSSI au processus de notification

Les éditeurs peuvent sous-estimer les conséquences, pour leurs utilisateurs et pour l'écosystème numérique, de l'existence de vulnérabilités. Surdéterminant les réactions potentielles des marchés financiers ou des investisseurs, ils peuvent ainsi s'avérer réticents à transmettre à leurs utilisateurs d'éventuelles faiblesses dans leurs produits.

De surcroît, l'éditeur seul ne dispose pas toujours des capacités techniques suffisantes pour identifier les utilisateurs de produits ou de services vulnérables et les alerter de manière efficace.

2.1.6. L'efficacité de la mesure

Si l'ANSSI peut enjoindre à l'éditeur de procéder à cette information, sans que cette injonction ne soit assortie d'une sanction, l'absence de caractère contraignant de la mesure n'annihile pas la portée utile de celle-ci, au-delà de son caractère incitatif.

Elle crée en effet un cadre légal afin que les grands éditeurs puissent transmettre les informations à l'ANSSI – cadre aujourd'hui inexistant. Encadrer juridiquement cette mesure les protègerait lorsqu'ils procèdent à de telles notifications (comme c'est actuellement le cas : les grands éditeurs de logiciels, tels que les GAMAM (Google, Apple, Meta, Amazon, Microsoft), informent très régulièrement leurs clients des failles découvertes dans leurs produits et des moyens d'y remédier (patch)).

Cela offrirait un levier important à l'égard des petits éditeurs (notamment hexagonaux) qui n'appliquent pas forcément les bonnes pratiques de gestion de vulnérabilités et sont parfois

réticents à informer leurs clients. Cela permettrait en outre, en cas de réticences persistantes, de signaler les incidents et vulnérabilités significatives à leur place, et ainsi d'obtenir l'effet recherché – à savoir l'information des utilisateurs concernés par les incidents et menaces.

Le défaut d'information par l'éditeur et l'injonction de l'ANSSI qui peut en découler peuvent être accompagnés d'une information des utilisateurs (ce qui contribuerait à inciter les éditeurs), mais aussi d'une information publique relative au manquement de l'éditeur. Une telle communication serait, pour sa part, plus susceptible encore d'inciter les éditeurs de logiciel à faire preuve de transparence, sauf à risquer de perdre d'importantes parts de marché.

La circonstance qu'il n'y aurait pas, dans un premier temps, de sanction associée à une absence de notification peut en outre constituer une première étape permettant d'habituer les acteurs du marché, sans exclure qu'à l'avenir, une sanction autre que seulement réputationnelle soit introduite par le législateur.

En outre, il peut arriver que des éditeurs n'aient pas connaissance de l'usage qui est fait de leur produit, par exemple chez des opérateurs d'importance vitale ou dans certains emplois confidentiels (matériels embarqués dans des usages de défense nationale, par exemple). A cet égard, cet article permettrait à l'ANSSI d'informer ces utilisateurs finaux sensibles.

Dans la mesure où la disposition envisagée crée une obligation pesant sur les entreprises, à plus forte raison à portée extraterritoriale, il est nécessaire de recourir à la loi.

Dans la mesure où cette disposition vise à renforcer les moyens dont disposent l'ANSSI dans sa mission d'autorité nationale de sécurité des systèmes d'information, elle sera insérée dans le code de la défense.

2.2. OBJECTIFS POURSUIVIS

Cette mesure contribuera à renforcer la cyber-protection des entités françaises d'intérêt et renforcera les pratiques de bonne gouvernance cyber de la part des éditeurs de logiciel vis-à-vis des utilisateurs recourant à leurs produits.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

L'ANSSI approche aujourd'hui les éditeurs sur ces sujets de manière amiable sans toujours rencontrer le succès escompté. L'option consistant à continuer à les sensibiliser de façon informelle ne permettrait donc pas d'atteindre les objectifs poursuivis.

3.2. OPTION RETENUE

3.2.1. Présentation du dispositif envisagé

Cette disposition crée à la charge des éditeurs de logiciel une double obligation. Celle de déclarer auprès de l'ANSSI les incidents sur leurs systèmes d'information et les vulnérabilités identifiées dans leurs produits et systèmes d'information, et celle d'en informer les utilisateurs recourant au produit concerné.

Si l'éditeur ne se conforme pas à cette obligation, l'ANSSI peut leur enjoindre de le faire, sans que cette injonction ne soit assortie de sanction autre que la possibilité pour l'ANSSI de rendre publics la vulnérabilité ou l'incident, ainsi que de rendre publique l'injonction quand l'éditeur n'y a pas donné suite.

Les éditeurs concernés sont ceux qui fournissent le produit affecté sur le territoire français, à des sociétés ayant leur siège social sur le territoire français ou à des sociétés contrôlées, au sens de l'article L. 233-3 du code de commerce, par des sociétés ayant leur siège social sur le territoire français.

Cette mesure vise à garantir que les potentielles victimes parmi les utilisateurs, en particulier les plus sensibles, soient correctement informées afin qu'elles puissent, par la suite, mettre en œuvre, le cas échéant, des mesures de remédiation adaptées, une fois la vulnérabilité sécurisée par l'éditeur.

3.2.2. Garanties prévues

En l'espèce, il n'y a pas d'atteinte à la liberté d'entreprendre.

Pour restreindre un droit fondamental, une mesure doit être nécessaire et adéquate. S'il était considéré que la mesure est susceptible de porter une telle atteinte, elle serait justifiée par la poursuite de deux objectifs, celui de sauvegarde de la sécurité des systèmes d'information et celui d'alerte des utilisateurs recourant aux biens et services de ces éditeurs de logiciel, qui seront prévenus des vulnérabilités auxquelles ils pourraient être exposés.

Plus généralement, la mesure proposée poursuit l'objectif d'intérêt général tenant à la sauvegarde de la sécurité nationale par un meilleur niveau de cybersécurité. La mesure vise en effet à permettre à l'ANSSI d'assurer sa mission de sécurité et de défense des systèmes d'information définie par le Premier ministre conformément à l'article L. 2321-1 du code de la défense.

Partielle et limitée, cette atteinte à la liberté d'entreprendre, si elle est avérée, est en tout état de cause proportionnée aux objectifs poursuivis. En l'espèce, le dispositif prévu est strictement circonscrit, et sa mise en œuvre encadrée par des garanties afin d'en assurer la proportionnalité.

En effet :

- il ne concerne que les éditeurs de logiciel et les utilisateurs recourant à leurs produits sur le territoire français, y compris les entreprises ayant leur siège social en France et les sociétés contrôlées par elles ;
- les mesures demeurent ponctuelles, c'est-à-dire que l'obligation de déclarer et l'obligation d'informer ne seront mises en œuvre que lorsque les éditeurs de logiciel :
  - soit seront victimes d'un incident sur leurs systèmes d'information ;
  - soit auront une vulnérabilité significative sur un produit vendu à des utilisateurs sur le territoire français, y compris les entreprises ayant leur siège social en France et les sociétés contrôlées par elles ;
- seule l'ANSSI sera destinataire des notifications des éditeurs de logiciel ;
- seuls les éditeurs de logiciel pourront informer les utilisateurs de leur produits, à moins que l'ANSSI ne soit contrainte de rendre publics la vulnérabilité significative ou l'incident, faute pour l'éditeur de l'avoir fait lui-même. Leur manière de procéder pourra éventuellement être prévue contractuellement avec ces derniers.

Il n'y a pas davantage d'atteinte au secret des affaires, protégé par la loi n° 2018-670 du 30 juillet 2018 portant transposition de la directive 2016/943/UE du 8 juin 2016 sur la protection des savoir-faire et informations commerciales non divulgués, dès lors que les informations concernées par l'article 34 ne répondent pas aux critères de l'information protégée, énoncés à l'article L. 151-1 du code de commerce.

En outre et en tout état de cause, l'article L. 151-7 du même code prévoit que le secret des affaires *« n'est pas opposable lorsque l'obtention, l'utilisation ou la divulgation du secret est requise ou autorisée par le droit de l'Union européenne, les traités ou accords internationaux en vigueur ou le droit national, notamment dans l'exercice des pouvoirs d'enquête, de contrôle, d'autorisation ou de sanction des autorités juridictionnelles ou administratives »*.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Il est proposé l'ajout d'un article L. 2321-4-1 dans le code de la défense.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La notification d'un incident procède en partie d'une dynamique imposée au niveau du droit de l'Union européenne, qu'il s'agisse d'incident portant sur les réseaux ou systèmes d'information[376] ou d'une violation des données à caractère personnel[377].

Néanmoins, il n'existe pas de texte de droit de l'Union européenne ou international permettant d'envisager une notification par les éditeurs de logiciels des incidents informatiques ou de vulnérabilités critiques affectant leurs produits et services, alors même que ces incidents et vulnérabilités sont susceptibles de constituer le point d'entrée d'attaques menées sur les systèmes d'information des utilisateurs.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Cette mesure contribuera à renforcer la cyber-protection des entités françaises d'intérêt et renforcera les pratiques de bonne gouvernance cyber de la part des éditeurs de logiciel vis-à-vis des utilisateurs recourant à leurs produits.

L'impact micro-économique de cette mesure peut être considéré comme significatif. La mise en œuvre de cette disposition pourra engendrer :

- une charge administrative supplémentaire et significative pour les éditeurs de logiciel victimes d'un incident sur leurs systèmes d'information ou ayant une vulnérabilité critique sur un produit ou un service vendu ;
- la prise en compte contractuelle de l'obligation de notification aux utilisateurs recourant aux produits de ces éditeurs.

Il convient toutefois, parallèlement, de mesurer le coût potentiel que la mesure permettrait justement d'économiser. Si ces vulnérabilités étaient exploitées par un attaquant, cela engendrerait inévitablement un coût important à payer pour procéder à la remédiation des systèmes d'information endommagés. Il faut aussi considérer les utilisateurs ayant subi un préjudice et susceptibles de réclamer réparation. Enfin, le coût en termes d'image serait potentiellement très significatif, surtout en cas de dissimulation de la vulnérabilité ou de l'incident ayant privé les utilisateurs de la possibilité d'en limiter les effets.

[376] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) ; Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

[377] Ibid.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Cette disposition étend les prérogatives de l'ANSSI puisqu'elle crée à la charge des éditeurs de logiciels une double obligation. Celle de déclarer auprès de l'ANSSI les incidents sur leurs systèmes d'information et les vulnérabilités significatives identifiées dans leurs produits et systèmes d'information, et celle d'en informer les utilisateurs recourant à leurs produits affectés. De plus, si l'éditeur ne se conforme pas à cette obligation, l'ANSSI pourra leur enjoindre de le faire, informer les utilisateurs ou rendre publics cette vulnérabilité ou cet incident ainsi que son injonction aux éditeurs si celle-ci n'a pas été mise en œuvre.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

La disposition va contribuer à renforcer la sécurité des systèmes d'information en France.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Les utilisateurs recourant aux biens et services des éditeurs de logiciels seront obligatoirement informés par les éditeurs des incidents sur leurs systèmes d'information et des vulnérabilités identifiées dans leurs produits et systèmes d'information. Cette mesure vise ainsi à garantir que les potentielles victimes parmi les utilisateurs, en particulier les plus sensibles, soient correctement informées afin qu'elles puissent mettre en œuvre, le cas échéant, une fois la vulnérabilité sécurisée par l'éditeur, des mesures de remédiation adaptées.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Les présentes dispositions ne requièrent aucune consultation obligatoire. Elles ont toutefois été soumises pour information à l'ARCEP en même temps que les autres articles du présent projet de loi relatifs à la sécurité des systèmes d'information.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront aux éditeurs de logiciels français et étrangers qui fournissent un produit à des utilisateurs sur l'ensemble du territoire de la République, y compris à des sociétés ayant leur siège social en France ou à des sociétés contrôlées par elles, au sens de l'article L. 233-3 du code de commerce.

Elles peuvent à cet égard avoir une portée extraterritoriale (comme le RGPD), car elles visent à protéger des utilisateurs ayant un lien juridique de rattachement au territoire national.

5.2.3. Textes d'application

Les conditions d'application du dispositif proposé seront définies par décret en Conseil d'Etat.

Article 35 : Renforcer les capacités de détection des cyberattaques et d'information des victimes

A- Adapter le dispositif de détection des cyberattaques en permettant la mise en place de dispositifs de circonstance dans les centres de données, le prélèvement de données sur des serveurs identifiés comme malveillants et la conservation de données directement utiles à la prévention et à la caractérisation des menaces

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Issu de l'article 34 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, l'article L. 2321-2-1 du code de la défense permet à l' Agence nationale de la sécurité des systèmes d'information (ANSSI), lorsqu'elle a connaissance d'une menace, de mettre en œuvre, sur les réseaux de communications électroniques exploités par les opérateurs de communications électroniques (OCE), les hébergeurs ou les fournisseurs d'accès Internet, des dispositifs mobilisant des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information des autorités publiques, des opérateurs d'importance vitale ou des opérateurs de service essentiel.

L'article R. 2321-1-3 du code de la défense définit ces marqueurs techniques comme des *« éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante ou d'identifier une menace »*. L'ANSSI peut les mettre en œuvre pour la durée utile et dans la mesure strictement nécessaire à la caractérisation de la menace. Elle peut recueillir des données et analyser les seules données techniques pertinentes aux fins d'une telle caractérisation.

Par ailleurs, en vertu de l'article L. 2321-5 du code de la défense, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) est chargée de veiller au respect par l'ANSSI des conditions d'application de l'article précité.

Les modalités de ce contrôle sont définies à l'article L. 36-14 du code des postes et des communications électroniques (CPCE), précisant que :

- l'ANSSI informe la formation de règlement des différends, de poursuite et d'instruction de l'ARCEP du champ et de la nature des mesures précitées ;
- l'ARCEP dispose, à sa demande et dans le respect du secret de la défense nationale, d'un accès aux informations ou documents nécessaires pour s'assurer du respect des conditions d'application de ces dispositions ;

- l'ARCEP peut adresser des recommandations à l'ANSSI aux fins d'assurer la régularité des mesures ci-dessus exposées, et peut lui enjoindre d'interrompre ses opérations ou de supprimer les données techniques recueillies si elle estime que les suites données à ces recommandations sont insuffisantes ;
- le président de l'ARCEP, enfin, peut saisir le Conseil d'Etat d'un recours lorsque l'ANSSI ne se conforme pas à une injonction qui lui a été adressée.

1.2. CADRE CONSTITUTIONNEL ET CONVENTIONNEL

L'article L. 2321-2-1 du code de la défense autorise l'ANSSI à procéder à un recueil d'informations sans l'accord de celui qui est concerné, et à exploiter les données techniques ainsi recueillies. Cela est manifestement de nature à porter atteinte à différents droits constitutionnellement garantis – plus particulièrement au droit au respect à la vie privée[378], mais aussi au droit à la protection des données à caractère personnel, au droit au secret des correspondances et au droit à la liberté d'expression protégés par les articles 2, 4 et 11 de la Déclaration des droits de l'homme et du citoyen de 1789.

L'article L. 2321-2-1 du code de la défense n'a pas fait l'objet d'un contrôle de constitutionnalité par le Conseil constitutionnel. Néanmoins, le Conseil d'Etat a considéré, au vu de l'ensemble des garanties apportées, et en particulier le contrôle de l'ARCEP, et eu égard à l'intérêt général qui s'attache à prévenir les menaces visant plus particulièrement les systèmes d'information des autorités publiques et des opérateurs d'importance vitale ou susceptibles de les affecter, que de telles mesures ne portaient aux droits garantis par la Constitution ou aux engagements internationaux de la France qu'une atteinte justifiée et proportionnée[379].

De surcroît, le Conseil d'Etat a rejeté un recours pour excès de pouvoir formé contre le décret du 13 décembre 2018[380] pris, notamment, pour l'application de l'article précité[381]. La haute juridiction a jugé que ces dispositifs mettaient en œuvre les exigences constitutionnelles liées à la sauvegarde des intérêts fondamentaux de la Nation et la prévention des atteintes à l'ordre public. De plus, elle considérait qu'il n'y avait pas lieu de transmettre au Conseil constitutionnel la question prioritaire de constitutionnalité soulevée et écartait l'ensemble des moyens tirés de la méconnaissance du droit de l'Union européenne.

[378] Cons. const., 23 déc. 23 juillet 1999, n° 99-146 DC. Le droit au respect de la vie privée peut être concilié avec d'autres exigences. L'atteinte à la vie privée doit être proportionnée à l'objectif poursuivi et que des garanties suffisantes sont mises en œuvre pour limiter cette atteinte.

[379] Avis CE, 1er fév. 2018, n° 394142.

[380] 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.

[381] CE, 30 décembre 2021, n° 428028, *La Quadrature du Net et autres.*

1.3. ELEMENTS DE DROIT COMPARE

La mise en place de dispositifs permettant de mieux détecter et observer les cyberattaques est une pratique courante dans de nombreux pays, notamment :

- en **Allemagne** où la loi sur la sécurité des technologies de l'information autorise les autorités fédérales en charge de la sécurité des systèmes d'information à prendre des mesures de détection des failles de sécurité dans les installations de l'État fédéral ou de certaines entreprises si des faits permettent de supposer que ces dernières ne sont pas protégées et que leur sécurité est menacée. Les autorités sont également autorisées à utiliser des systèmes et procédures afin de collecter des données nécessaires à l'évaluation du fonctionnement des logiciels malveillants et des modes opératoires d'attaques. Ces activités de détection et d'observation sont généralement réalisées sous le contrôle du ministère fédéral de l'Intérieur qui exerce une surveillance juridique et technique ou du Commissaire fédéral à la protection des données et à la liberté d'information. En outre, des voix de recours existent auprès des tribunaux compétents pour les personnes affectées par les activités de sécurisation des systèmes d'information des autorités fédérales allemandes. A noter que les autorités allemandes ne peuvent en revanche pas avoir accès au contenu d'un serveur sauf si son propriétaire y consent.

- en **République Tchèque** où le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques offre des services de détection des attaques et d'observation des modes opératoires d'attaque aux entités régulées. L'Agence Nationale de Cybersécurité tchèque (NÚKIB) est habilitée à réaliser ces activités conformément à la loi. La prestation de ce type de services est généralement déterminée en fonction des capacités de l'agence et de ses priorités stratégiques.

- à **Singapour** où l'Agence de cybersécurité (CSA) coordonne les efforts de cyberdéfense de divers organismes gouvernementaux et mène notamment des actions de cyberdéfense avancées lorsqu'elles sont jugées nécessaires afin de détecter les attaques et observer la menace. La loi sur la sécurité informatique de Singapour autorise le Ministre à ordonner à toute personne ou organisation de prendre les mesures ou de se conformer aux exigences nécessaires pour prévenir, détecter ou contrer toute menace à l'encontre d'un ordinateur ou d'un système informatique ou d'une catégorie d'ordinateurs ou de systèmes informatiques en cas de menace imminente sur un service essentiel ou sur la sécurité nationale, la défense, les affaires étrangères, l'économie, la santé, la sécurité publique et l'ordre publique à Singapour.

- en **Italie**, des travaux législatifs sont en cours afin d'envisager la mise en place d'éventuelles capacités de détection supplémentaires. Les procédures de gouvernance et de contrôle seront également conçues dans le cadre de cette analyse législative.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

Il est proposé de parfaire le dispositif existant en amendant l'article L. 2321-2-1 du code de la défense pour permettre à l'ANSSI d'accéder aux données, métadonnées et contenus strictement nécessaires à la compréhension de la menace, à l'identification des victimes et à la protection de la Nation.

2.1. NECESSITE DE LEGIFERER

Une évolution du dispositif prévu par l'article L. 2321-2-1 est nécessaire à plusieurs titres.

La réalisation d'une attaque informatique suppose que son auteur contrôle un certain nombre de machines, qui forment son arsenal d'attaque, aussi appelé infrastructure d'attaque. Elles sont utilisées à toutes les étapes de l'attaque, par exemple pour entrer dans un système et compromettre des équipements de la victime, ou encore pour corrompre ou dérober des données.

Par souci évident de discrétion, l'attaquant n'utilise pas ses moyens propres dans cet arsenal. Il a donc recours à la location de machines (de manière légale), ou bien à des machines dont il aura préalablement pris le contrôle de manière illégale. Dans les deux cas, ces machines peuvent appartenir à des opérateurs de communications électroniques, des hébergeurs, ou des fournisseurs d'accès à Internet en France ou même à leurs sous-traitants, dès lors que ces derniers accèdent et manipulent des informations de ces opérateurs ou administrations avec le même niveau de criticité et les mêmes privilèges que leurs donneurs d'ordre.

Le dispositif actuel permet d'obtenir, pendant une durée limitée, des informations sur le trafic réseau de cette machine (flux entrants et sortants vers/depuis la machine). Toutefois, en pratique, les données accessibles demeurent très limitées, permettant seulement de savoir avec quelles autres machines l'attaquant communique, ainsi que la méthode de communication utilisée (aussi appelée protocole). Par ailleurs, il est également fréquent que l'attaquant utilise des protocoles procédant au chiffrement des communications, lesquels ne permettent pas de déterminer si ces dernières sont malveillantes.

Le dispositif existant ne permet donc pas de faire face à la réalité contemporaine de la menace.

Par ailleurs, des accès assez larges sont généralement accordés aux sous-traitants (accès au SI, aux informations, *etc*.), alors que les mesures de sécurité qu'une entité sensible s'impose sont souvent bien moindres, voire inexistantes chez les sous-traitants, lesquels ne disposent en outre pas des mêmes moyens financiers et humains que les entités sensibles et ne sont pas soumises aux mêmes obligations légales. Il en résulte que les attaquants, pour atteindre, *in fine*, des entités sensibles, utilisent fréquemment leurs sous-traitants comme porte d'entrée.

2.1.1. Clarifier la lettre du texte pour permettre la collecte par l'ANSSI de l'ensemble des données d'un flux ciblé, comme le prévoyait l'esprit de la loi n° 2018-607 précitée

A l'occasion de la mise en œuvre du dispositif prévu par l'article L. 2321-2-1 du code de la défense, une divergence d'interprétation du texte entre l'ANSSI et l'ARCEP est apparue. Cette dernière a retenu une lecture restrictive de la notion de données susceptibles d'être collectées par l'ANSSI : elle considère que seules les données techniques peuvent être collectées. En revanche, selon l'ANSSI, si seules les données techniques peuvent être conservées, la collecte des données devrait porter plus largement sur l'intégralité du flux ciblé. Une telle interprétation résulte d'une lecture combinée des alinéas 3 et 4 de l'article.

L'analyse de l'ANSSI apparaît corroborée par les travaux parlementaires sur la loi n° 2018-607 précitée. Qu'il s'agisse de l'Assemblée nationale ou du Sénat, les parlementaires ont admis que les éléments collectés pouvaient porter atteinte à la vie privée, même de manière incidente, dès lors que les garanties apportées étaient clairement spécifiées pour que cette atteinte ne soit pas disproportionnée.

A titre d'exemple, M. Philippe Bonnecarrère, rapporteur pour avis de la commission des lois, expliquait ainsi :

> *« La recherche des virus oblige […] intrinsèquement à regarder dans le document, non pour le lire – je vous en donne acte, madame la ministre –, mais pour vérifier la présence d'un caractère anormal. […].*
>
> *Nous voulons tout simplement mettre en place une garantie en renvoyant à un décret en Conseil d'État la définition des éléments pouvant être vérifiés et collectés, car ils porteront à l'évidence, au-delà des seules adresses mail, sur les contenus.* »[382].

La lecture de ces travaux préparatoires démontre que l'intention du législateur était d'autoriser l'ANSSI à récupérer du trafic ou des flux et que les « données autres » couvrent bien l'ensemble des données que l'ANSSI peut recueillir à l'occasion de sa mission mais doit détruire si elles ne s'avèrent pas utiles à la prévention ou à la caractérisation de la menace. Qui plus est, c'est bien la rédaction à laquelle le Gouvernement était favorable, visant à ne pas « limiter » les données récupérées par l'ANSSI, qui a été retenue dans le cadre des travaux de la commission mixte paritaire.

C'est aussi, du reste, l'interprétation du Conseil d'État dans son avis précité sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025. Il effectue en effet une distinction entre les « données techniques », collectables et analysables par l'ANSSI, et les autres « données » (c'est-à-dire non techniques), pour leur part collectables par l'ANSSI, mais devant être immédiatement détruites si elles ne s'avèrent pas pertinentes aux seules fins de la caractérisation de la menace :

> « *[Le dispositif] permet également à l'ANSSI, lorsque la menace dont elle est informée est susceptible de porter atteinte à la sécurité des systèmes d'information des mêmes autorités publiques ou opérateurs, de procéder elle-même à de telles détections pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace, de recueillir des données et d'analyser les seules données techniques pertinentes aux seules fins de cette caractérisation* »[383].

[382] Extrait des débats parlementaires lors de la 1ère lecture devant le Sénat (séance du 22 mai 2019).

[383] Avis CE, 1er fév. 2018, n° 394142.

Il apparaît donc que la capture du trafic devrait être autorisée à la condition qu'elle soit suffisamment justifiée, notamment auprès de l'ARCEP, et que toute donnée qui serait finalement non utile à la prévention ou à la caractérisation de la menace soit immédiatement détruite (avec une trace de cette destruction).

Cependant, l'interprétation restrictive du texte par l'ARCEP contraint actuellement l'ANSSI à circonscrire significativement son recueil des données, en se limitant uniquement aux seules données techniques (métadonnées), ce qui la prive des données de contenu et des informations présentes souvent nécessaires pour obtenir une qualification pertinente de la menace et de portée plus étendue (mode opératoire, identification d'autres victimes, découverte d'un code malveillant jusque-là inconnu, *etc*.). Une clarification du texte, conforme à l'esprit de la loi lorsqu'elle a été votée en 2018, paraît donc nécessaire.

2.1.2. Obtenir une copie du serveur ciblé en cas de menace particulière et importante d'incident de sécurité sur les SI

Outre qu'elle est ambiguë, la rédaction actuelle de l'article, si elle a permis d'augmenter les capacités d'action de l'ANSSI, s'avère insuffisante à deux titres.

La mise en œuvre de marqueurs spécifiques pour détecter des événements suppose une connaissance préalable de l'attaquant qui ne peut être obtenue que par l'analyse de l'ensemble de données figurant sur une machine compromise.

L'article L. 2321-2-1 du code de la défense, dans sa rédaction actuelle, ne permet pas à l'ANSSI d'agir en anticipation d'une menace et l'empêche de protéger efficacement ses bénéficiaires.

Le texte actuel prévoit que l'ANSSI peut placer chez certains opérateurs des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information (SI) des autorités publiques et opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du présent code ou à l'article 5 de la loi n° 2018-133 du 26 février 2018[384]. Cependant, ce moyen d'action, s'il permet de prévenir certaines attaques, implique que l'ANSSI connaisse déjà en amont les modes opératoires utilisés par les attaquants et en ait tiré des marqueurs spécifiques pour pouvoir les détecter. Il ne lui permet donc pas de détecter un acteur inconnu ou non caractérisé et ne permet que des actions en réaction.

L'ANSSI doit donc pouvoir accéder au contenu de la machine infectée (copie du disque dur, copie de la mémoire vive) afin de récupérer les configurations et le détail des codes malveillants ou implants utilisés par l'attaquant, les données qu'il a dérobées, les journaux de connexions de l'attaquant ou encore les éléments secrets permettant de déchiffrer le trafic malveillant.

L'ANSSI n'a aujourd'hui accès qu'aux effets des activités malveillantes (les flux réseaux) et non à leurs causes (code, logs, contenu stocké).

[384] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

L'ANSSI peut accéder aujourd'hui aux données techniques des flux réseaux. Or, ces flux réseaux sont déclenchés par des actions lancées en amont par des acteurs malveillants à partir de codes et logiciels malveillants, d'outils de « commande et contrôle » (outils sous le contrôle des attaquants à partir desquels ils lancent les attaques), de chevaux de Troie, etc. Seul l'accès à la source des actions malveillantes lancées en amont permet de comprendre leur nature, leur forme et d'analyser plus globalement la situation. Cela suppose de pouvoir accéder au code de l'action malveillante, aux outils et aux fichiers logs (ou « journaux systèmes », enregistrant l'ensemble de l'activité d'un SI et permettant de déterminer l'enchaînement des actions réalisées sur un système donné) pour comprendre la nature des actions malveillantes. A cette fin, il est nécessaire d'effectuer des copies de machines compromises.

A titre d'illustration, en 2017, en observant certaines actions malveillantes chez une victime, l'ANSSI est parvenue à reconstruire le fichier de configuration d'un serveur de contrôle d'un attaquant. Il a ensuite pu identifier un serveur physique sous le contrôle de cet attaquant hébergé chez un hébergeur français. Cependant, toutes les communications qui entraient et sortaient de cette machine passaient par le réseau ToR (qui permet d'assurer l'anonymat de ceux qui l'utilisent par une série de chiffrement des requêtes) et, par conséquent, étaient inexploitables en l'état. Le Parquet a ouvert une enquête en flagrance et le service enquêteur a requis l'ANSSI pour procéder à l'analyse du serveur identifié. Cela a permis d'identifier toutes les victimes attaquées, mais également toutes les cibles potentielles de l'attaquant, non encore activées, qui étaient répertoriées sur le serveur analysé. Ces dernières ont pu faire l'objet d'un suivi dédié de l'ANSSI et se prémunir contre les actions de cet attaquant.

2.1.3. Face à une évolution toujours croissante de la menace, permettre à l'ANSSI d'étendre le périmètre du dispositif aux opérateurs de centres de données.

L'ANSSI est aujourd'hui confrontée à une évolution de la menace, puisque les acteurs malveillants se professionnalisent et profitent des failles liées à la territorialité des cadres légaux. L'ANSSI observe la fréquente utilisation par des attaquants de serveurs compromis (pour être intégrés à une infrastructure d'attaque), loués par des hébergeurs étrangers auprès d'opérateurs de centres de données - au sens de l'article L. 32 du CPCE - basés sur le territoire national. En effet, le cyberattaquant, proche du niveau étatique, cherche systématiquement à limiter les possibilités d'imputation de son attaque, en créant une infrastructure d'anonymisation selon deux méthodes :

- l'achat de *serveurs privés virtuels* (ou VPS pour *Virtual Private Server*) qui sont des chaînons créés pour l'usage exclusif de l'attaquant et complètement maîtrisés par lui, mais dont l'achat de façon parfaitement anonyme est complexe ;
- la compromission des éléments d'infrastructure (serveurs, routeurs, pare-feu, *switchs*, etc.) et l'installation sur ces derniers de programmes relais qui sont autant de chaînons d'anonymisation.

En conséquence, quand l'ANSSI a à traiter d'attaques contre les intérêts les plus importants de la nation, le recours à des serveurs compromis est quasiment systématique.

Or, en l'état du droit, l'ANSSI ne peut pas installer ses dispositifs chez les opérateurs de centres de données dont c'est l'activité exclusive, car ils ne sont ni hébergeurs ni fournisseurs d'accès à Internet au sens de la loi n° 2004-575 pour la confiance dans l'économie numérique.

2.1.4. Adapter les garanties et la proportionnalité de l'atteinte aux libertés

Un tel élargissement du champ d'application de l'article L. 2321-2-1 du code de la défense au niveau matériel (infrastructure) et organique (opérateurs de centre de données) ne remet pas en question le caractère proportionné de la mesure au regard des objectifs d'intérêt général poursuivis par l'ANSSI. Les garanties suivantes apparaissent en effet dûment protectrices :

- le ciblage préalable de la machine compromise faisant l'objet de la copie ;
- la destruction immédiate des données par l'ANSSI dès lors que celles-ci sont jugées inutiles pour la prévention et la caractérisation de la menace ;
- le contrôle de l'application de ces nouvelles mesures par l'ARCEP.

L'élargissement du champ d'application de l'article précité est compensé par un encadrement accru, puisque l'ANSSI ne pourra opérer des demandes que sur un périmètre et pour une durée limités, et toujours aux seules fins de prévention et de caractérisation des menaces visant plus particulièrement les SI des autorités publiques, des opérateurs d'importance vitale et des opérateurs essentiels au sens de la loi n° 2018-133 du 26 janvier 2018 susmentionnée ou susceptibles de les affecter par le biais de leurs sous-traitants.

S'agissant de l'accès aux données, elles ne seront obtenues et exploitées que par des agents individuellement désignés et spécialement habilités, et uniquement à des fins de défense des systèmes d'information des opérateurs ou autorités précités. De surcroît, elles seront détruites dans un délai déterminé, mais ne pouvant excéder la durée strictement nécessaire, c'est-à-dire immédiatement lorsqu'elles ne sont pas utiles et deux ans lorsqu'elles le sont.

Les captures réalisées par l'ANSSI au moyen du dispositif ainsi amendé, bien que susceptibles de concerner un champ plus large, seront toujours ciblées, justifiées et soumises au contrôle d'une autorité administrative indépendante, pour éviter que des données autres que celles utiles à la prévention ou à la caractérisation de la menace ne soient conservées. Outre une clarification de la loi, la nouvelle rédaction envisagée s'accompagne d'une adaptation des garanties associées, notamment à travers l'aménagement du contrôle de l'ARCEP afin de s'assurer que l'ANSSI respecte l'application des dispositions amendées.

2.2. OBJECTIFS POURSUIVIS

Le principal objectif de cette mesure est d'améliorer la connaissance de l'ANSSI en ce qui concerne les modes opératoires des cyberattaquants :

- en ayant accès aux informations d'intérêt, essentielles pour comprendre et appréhender la situation, notamment présentes dans le contenu des communications réseau (identité des victimes, nature de l'attaque, instructions envoyées par l'attaquant aux machines

sous son contrôle, etc.), ou bien sur le disque et la mémoire de la machine utilisée par l'attaquant (outils malveillants développés par l'attaquant, méthodes de travail, base de connaissance sur ses victimes, etc.) ;

- en élargissant le périmètre de la mesure aux opérateurs de centres de données.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Une modification de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a pu être envisagée mais n'a pas été considérée comme satisfaisante dès lors que :

- elle ne prenait en compte qu'une partie des modifications que requiert la mesure nouvelle ;
- elle tendait à complexifier le droit positif en ajoutant dans la loi du 21 juin 2004 des prescriptions dont l'objet a une finalité de sécurité nationale.

3.2. OPTION RETENUE

Cette composante complète l'article L. 2321-2-1 du code de la défense à trois égards :

- elle étend les données recueillies au contenu des communications réseaux et plus largement en obtenant la copie du serveur utilisé par l'attaquant ;
- par ailleurs, elle inclut les opérateurs de centre de données dans le périmètre des opérateurs sur lesquels l'ANSSI pourrait apposer des marqueurs techniques ou obtenir la copie de leurs serveurs ;
- enfin, elle inclut les sous-traitants des autorités publiques, des opérateurs d'importance vitale et des opérateurs de services essentiels au profit desquels l'ANSSI peut détecter et caractériser des événements susceptibles d'affecter la sécurité de leurs systèmes d'information.

En outre, le contrôle de l'ARCEP est adapté pour prévoir des garanties supplémentaires, notamment au titre de la copie du serveur utilisé par l'attaquant.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La présente disposition requiert une modification de l'article L. 2321-2-1 du code de la défense et de l'article L. 36-14 du code des postes et des communications électroniques.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

S'agissant d'une mesure dont l'objet porte sur la sécurité nationale, elle relève de la compétence des Etats membres en vertu du traité sur le fonctionnement de l'Union européenne. Les modifications de l'article L. 2321-2-1 du code de la défense ne mettent pas en cause des dispositions du droit de l'Union européenne.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

La mesure concerne les opérateurs de centre de données dans le périmètre des opérateurs sur lesquels l'ANSSI pourrait apposer des marqueurs techniques ou obtenir la copie de leurs serveurs.

Par ailleurs, elle inclut les sous-traitants des autorités publiques, des opérateurs d'importance vitale et des opérateurs de services essentiels au profit desquels l'ANSSI peut détecter et caractériser des événements susceptibles d'affecter la sécurité de leurs systèmes d'information.

Les prestations effectuées au titre de l'article L. 2321-2-1 du code de la défense donnent aujourd'hui lieu à compensation (arrêté du 18 février 2020 pris en application de l'article R. 2321-1-5 du code de la défense). Une modification de cet arrêté pour la compensation des coûts liés à la copie des machines sera nécessaire.

De même, les coûts pour un opérateur de centres de données résultant de la mise en place du système de détection seront compensés en vertu de l'arrêté susmentionné. Ces coûts reviennent à moins d'un millier d'euros par an, correspondants pour l'essentiel à la consommation électrique et à l'espace occupé par le dispositif mobilisant des marqueurs techniques.

4.2.3. Impacts budgétaires

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Impliquant la totalité des bureaux effecteurs de la Sous-direction opérations de l'Agence (soit plus de 70% des effectifs de cette sous-direction), l'analyse des captures réseau brutes effectuées par les dispositifs de détection de l'ANSSI ainsi que l'analyse des données issues des copies de machines compromises nécessitent des ressources dédiées importantes, tant pour l'analyse en elle-même que pour le développement d'outils d'analyse automatisés. Ceci doit être pris en compte dans le schéma d'emploi de l'ANSSI.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette mesure devrait contribuer à renforcer la sécurité des systèmes d'information en France.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 36-5 du CPCE, la présente disposition a été présentée à l'ARCEP, quia rendu son avis le 9 mars 2023[385].

5.2. MODALITES D'APPLICATION

5.2.1 Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal Officiel* de la République française.

5.2.2 Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire de la République.

5.2.3 Textes d'application

Les conditions d'application du dispositif proposé seront définies par décret en Conseil d'Etat et les modalités de compensation des prestations seront prévues par arrêté.

[385] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2024-2030.

B- Rendre obligatoire la mise en place de capacités de détection chez les opérateurs de communications électroniques (OCE)

1. ETAT DES LIEUX

1.1. CADRE GENERAL

En matière de cyberdéfense et de cybersécurité, le législateur a initialement privilégié la protection plutôt que la détection, en sécurisant les systèmes d'information sensibles (notamment ceux des opérateurs d'importance vitale (OIV)) et en dotant les services de l'Etat d'une capacité de réponse aux attaques[386]. Toutefois, ces mesures législatives se sont révélées insuffisantes pour faire face à la prolifération de la menace[387] et aux risques découlant de l'exposition des systèmes d'information des particuliers (cf. exemples cités *supra* relatifs à la compromission de serveurs).

Avant la loi n° 2018-607 du 13 juillet 2018 précitée, il n'existait aucune disposition législative portant sur les capacités de détection et de caractérisation des attaques informatiques des opérateurs de communications électroniques (OCE). Or, les opérateurs, dans la mesure où ils connectent les utilisateurs au réseau mondial et voient passer par leurs réseaux l'ensemble des flux, occupent une position clé pour permettre la détection des attaques, d'autant plus qu'ils servent souvent de point d'appui aux attaquants pour cibler leurs clients. L'article 34 de la loi n° 2018-607 a donc cherché à renforcer la capacité nationale de détection des attaques informatiques en y associant plus étroitement les OCE. Elle a ainsi créé un dispositif visant à mieux impliquer les OCE dans la cyberdéfense, en lien avec l'ANSSI. Ce dispositif est codifié à l'article L. 33-14 du CPCE ainsi qu'au deuxième alinéa de l'article L. 2321-3 du code de la défense (CODEF).

L'objectif de ces dispositions législatives était, à des fins de défense et de sécurité des systèmes d'information :

- d'une part, d'autoriser les OCE à mettre en œuvre, sur leurs réseaux, des systèmes de détection des attaques informatiques visant leurs abonnés (article L. 33-14, alinéa 1er, du CPCE). Il s'agit de dispositifs techniques qui comparent en temps réel l'activité d'un réseau à des marqueurs d'attaque (ces marqueurs sont des éléments techniques propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé). Ceux-ci analysent automatiquement le trafic sans s'intéresser au contenu, en se limitant à le comparer aux marqueurs d'attaque. Le trafic n'est pas stocké ;
- d'autre part, de fixer, en matière de détection, les modalités d'échanges techniques entre ces opérateurs et l'ANSSI. Pour leur permettre de détecter des attaques sophistiquées, l'ANSSI

[386] Article L. 2321-2 du code de la défense.

[387] 831 attaques informatiques ont été traitées par l'ANSSI en 2022.

fournit aux opérateurs des marqueurs d'attaque. En cas d'attaque informatique associée à l'un de ces marqueurs, les systèmes de détection déployés par les opérateurs produisent une alerte de sécurité, contenant uniquement les informations techniques liées à l'attaque. L'opérateur informe alors l'ANSSI de cette alerte et, si l'attaque détectée concerne un OIV, un opérateur de services essentiels (OSE)[388] ou une autorité publique, celle-ci peut demander des informations techniques complémentaires pour caractériser l'attaque et établir des mesures de protection et de remédiation adaptées[389].

La loi a assorti ces nouveaux moyens opérationnels de garanties. Ainsi, l'ARCEP est chargée de veiller au respect par l'ANSSI des conditions d'application de l'alinéa 2 de l'article L. 2321-3 du CODEF. Les pouvoirs dévolus à l'ARCEP dans ce cadre sont fixés par l'article L. 34-16 du CPCE.

1.2. CADRE JURIDIQUE

Le Conseil d'Etat a rejeté un recours pour excès de pouvoir dirigé contre le décret d'application de l'article L. 33-14 du CPCE. Il a notamment jugé qu'il n'y avait pas lieu de transmettre au Conseil constitutionnel la question prioritaire de constitutionnalité soulevée contre cette disposition législative. Il a aussi écarté l'ensemble des moyens tirés de la méconnaissance du droit de l'Union européenne dirigés, par voie d'exception, à l'encontre de celle-ci[390]. La constitutionnalité et la conventionnalité du dispositif prévu à l'article L. 33-14 précité sont donc désormais bien établies.

Par ailleurs, le Conseil constitutionnel a eu l'occasion de se prononcer sur la compensation financière versée par l'État aux OCE, notamment dans une décision du 5 février 2021, où il a considéré que *« [l]a sécurisation des réseaux de communication mobile, par l'autorisation préalable de l'exploitation de certains appareils, est directement liée aux activités des opérateurs qui utilisent et exploitent ces réseaux afin d'offrir au public des services de communications électroniques. Dès lors, en adoptant les dispositions contestées, le législateur n'a, en tout état de cause, pas reporté sur des personnes privées des dépenses qui, par leur nature, incomberaient à l'État »*[391].

Il ressort de ces décisions que la compensation par l'Etat des dépenses que les opérateurs de communications électroniques engagent pour se conformer à leurs obligations légales n'est obligatoire que lorsque ces dépenses sont étrangères à leur activité.

---

[388] Au sens de l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, qui fait référence aux « opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services ». Ces opérateurs sont désignés par le Premier ministre.

[389] Alinéas 2 à 4 de l'article L. 33-14 du CPCE et alinéa 2 de l'article L. 2321-3 du code de la défense.

[390] CE, 30 déc. 2021, *La Quadrature du Net* et autres, n° 428028.

[391] Cons. const., déc. du 5 février 2021, n° 2020-882 QPC.

1.3. ELEMENTS DE DROIT COMPARE

Plusieurs Etats étrangers ont mis en place des obligations en matière de cyberdéfense aux opérateurs de communications électroniques mais tous n'ont pas rendu obligatoire la mise en place de capacités de détection, notamment :

- En **Allemagne**, la loi sur les télécommunications précise que les fournisseurs de services de télécommunications peuvent utiliser des systèmes de détection d'attaques qui sont définis dans la loi sur la sécurité des technologies de l'information comme des mesures techniques et organisationnelles appropriées pour se protéger contre les perturbations externes (catastrophes ou cyberattaques) susceptibles d'entraîner une détérioration significative ou de constituer un risque de sécurité des réseaux et services de télécommunications. La loi sur la sécurité des technologies de l'information prévoit également l'obligation pour les exploitants d'infrastructures critiques, dont font également partie certains fournisseurs de services de télécommunications, de prendre des précautions organisationnelles et techniques appropriées (dont l'utilisation de systèmes de détection des attaques). Ces systèmes doivent enregistrer et évaluer de manière continue et automatique les paramètres et caractéristiques des opérations en cours. Ils doivent aussi être en mesure d'identifier et de prévenir les menaces de manière continue et de prévoir des mesures correctives appropriées.

- En **République Tchèque**, seulement les opérateurs de communications électroniques les plus importants sont des opérateurs de services essentiels. En revanche, l'ensemble des opérateurs de communications électroniques sont régulés au titre de la loi sur la cybersécurité. Or, cette loi dispose que les entités régulées n'ont pas l'obligation d'introduire et de mettre en œuvre des mesures de sécurité ou de signaler des incidents. Cependant, elles sont tenues de prendre des mesures pour réagir en cas de déclaration d'un état d'urgence cyber. Les opérateurs de communications électroniques sont également réglementés par une loi sectorielle qui oblige les opérateurs à signaler les incidents cyber aux autorités compétences respectives. Avec la directive NIS2, la République Tchèque prévoit des évolutions dans l'architecture de supervision des opérateurs des communications électroniques.

- A **Singapour**, la loi sur la sécurité des réseaux ne comprend pas d'exigences particulières vis-à-vis des opérateurs de communication électronique. En revanche, des exigences ex-ante en matière de cybersécurité sont imposées aux propriétaires d'infrastructures critiques telles que des audits de cybersécurité et des évaluations des risques.

- En **Italie**, le code des communications électroniques oblige les opérateurs de communications électroniques à adopter des mesures de sécurité, y compris des procédures visant à détecter les incidents qui doivent ensuite être notifiés au Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. En outre, les opérateurs de télécommunications italiens sont également tenus de déployer un marquage technique spécifique défini par l'Agence de cybersécurité au sein de leurs outils de détection dans des situations spécifiques.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le dispositif prévu par l'article L. 33-14 du CPCE n'a pas produit tous les effets escomptés en termes de sécurisation des réseaux de télécommunications et de détection des cybermenaces.

D'une part, il repose intégralement sur les capacités de détection existantes des opérateurs. Or celles-ci sont très hétérogènes et ne sont généralement pas suffisantes pour mener des actions de détection précises et ciblées sur la base des marqueurs fournis par l'ANSSI.

D'autre part, les opérateurs ont peu développé leurs capacités en matière de détection, dans la mesure où le dispositif n'est pas obligatoire et que sa mise en œuvre nécessite des investissements à leur charge. En l'absence d'une véritable obligation juridique, ils ne considèrent pas comme une priorité le fait de procéder aux investissements nécessaires à la mise en place d'une capacité de détection adéquate pour faire fonctionner pleinement le dispositif.

Seule une intervention législative est susceptible d'imposer aux OCE qui ont été désignés OIV des mesures contraignantes pour mettre en œuvre des dispositifs permettant d'exploiter les marqueurs techniques fournis par l'ANSSI. En outre, la mesure envisagée modifie la partie législative du code des postes et des communications électroniques.

2.2. OBJECTIFS POURSUIVIS

Eu égard au développement de la menace cyber, il est indispensable de s'appuyer davantage sur les opérateurs. En effet, une cyberattaque transite toujours par le réseau d'un opérateur, dissimulée dans un flux massif de données. Le développement de la capacité des opérateurs à détecter efficacement les traces des cyberattaques serait une avancée majeure dans la lutte contre les cyberattaques touchant les entreprises et les administrations françaises.

Ainsi, s'il contribue au renforcement de la cybersécurité offerte par les OCE à leurs abonnés, le développement de leurs capacités de détection vise essentiellement à répondre aux besoins de la défense et de la sécurité des SI en permettant l'exploitation des marqueurs de l'ANSSI.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Une option envisagée était de rendre obligatoire, pour l'ensemble des opérateurs, la mise en œuvre, sur leurs réseaux, des systèmes de détection des attaques informatiques visant leurs abonnés. Toutefois, il s'avère qu'au regard des objectifs poursuivis (détection des attaques sur des flux importants), une telle obligation s'avèrerait disproportionnée pour des OCE n'ayant pas été désignés OIV. Cette option a par conséquent été écartée.

3.2. OPTION RETENUE

Il est donc proposé de rendre obligatoire la mise en œuvre de systèmes de détection des attaques informatiques pour les seuls OCE désignés OIV. En effet, plus l'opérateur est important, plus les flux qui transitent par son réseau sont conséquents, ce qui permet de maximiser l'efficacité des marqueurs fournis par l'ANSSI.

Pour des raisons légistiques, la disposition envisagée renvoie aux opérateurs mentionnés à l'article L. 1332-1 du code de la défense, désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La mesure proposée implique la modification de l'article L. 33-14 du CPCE.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La mesure envisagée, en ce qu'elle modifie l'article L. 33-14 du CPCE est conforme au cadre européen des communications électroniques transposé dans le CPCE, qui fait de la détection des attaques informatique un motif légitime de traitement des communications électroniques.

A l'instar du dispositif prévu lors de la 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, la mise en place de ces dispositifs de détection, distincte des mesures de gestion de trafic, est justifiée par la nécessaire protection de la sécurité et l'intégrité des réseaux dans le but de prévenir les cyberattaques. Elle constituera donc une mesure proportionnée au regard des dispositions du règlement n° 2015/2120 établissant des mesures relatives à l'accès à un internet ouvert.

Le Conseil d'Etat lors d'un recours pour excès de pouvoir dirigé contre le décret d'application de l'article L. 33-14 du CPCE a écarté l'ensemble des moyens tirés de la méconnaissance du droit de l'Union européenne dirigés, par voie d'exception, à l'encontre de celle-ci (CE, 30 déc. 2021, La Quadrature du Net et autres, n° 428028). La constitutionnalité et la conventionnalité du dispositif prévu à l'article L. 33-14 précité sont donc désormais bien établies.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Si la loi obligeait les OCE à développer leurs capacités de détection, il serait souhaitable qu'émerge une offre industrielle européenne pour assurer la mise en œuvre de l'article L. 33-14, alinéa 2, du CPCE. Développer les capacités de détection des OCE peut permettre de diversifier l'offre technologique et de soutenir le tissu industriel français ou européen en la matière, ce qui renforcerait en retour la compétitivité des entreprises françaises et la souveraineté numérique. Néanmoins, à ce jour, tout type de capacité de supervision permettant d'injecter les marqueurs de l'ANSSI doit être envisagé.

4.2.2. Impacts sur les entreprises

Les dispositifs existants n'ont pas permis le développement, même progressif, des capacités de détection des OCE. Il importe qu'ils effectuent les investissements nécessaires pour répondre aux demandes de l'ANSSI.

Cette mesure induira donc des charges qui seront compensées au moyen d'une aide au financement en juste rémunération, comme le sont les dispositifs portés via le guichet unique du Commissariat aux Communications Electroniques de Défense (CCED). L'ANSSI a exprimé des besoins budgétaires nouveaux pour tenir compte de l'évolution.

4.2.3. Impacts budgétaires

Le développement des capacités de détection des OCE fera l'objet d'une compensation financière intégrale de la part de l'Etat.

Cette mesure pourrait engendrer des charges administratives supplémentaires au titre de l'aide au financement, avec l'intégration d'un nouveau dispositif au sein du guichet unique du CCED. Cette option permet toutefois de mutualiser la charge administrative avec d'autres dispositifs et évite la création d'un guichet redondant par l'ANSSI.

La compensation financière pour un tel dispositif a été estimée par l'ANSSI lors du déploiement de France Relance, qui ne permettait toutefois pas de financer de telles capacités. Au regard des besoins spécifiques et des échanges opérationnels nécessaires entre les opérateurs et l'ANSSI, elle devra s'étendre sur plusieurs années, même si des investissements initiaux rapides sont possibles. Le modèle proposé par l'ANSSI évalue le coût approximatif de la mesure à un million d'euros par an. Ces besoins budgétaires ont été exprimés par l'ANSSI lors des travaux budgétaires et des estimations de trajectoires financières pour la période 2023-2027.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette mesure devrait contribuer à renforcer la sécurité des systèmes d'information en France.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Ces capacités de détection permettront de mieux protéger l'ensemble des utilisateurs, non seulement les administrations, OIV et OSE, mais également les particuliers.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément à l'article L. 36-5 du code des postes et des communications électroniques, cette disposition a été présentée à l'ARCEP qui a rendu son avis le 9 mars 2023[392].

[392] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2024-2030.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

La présente disposition s'appliquera sur l'ensemble du territoire de la République.

Pour l'article L. 33-14 du CPCE, les conditions d'application outre-mer sont précisées à l'article L. 33-15 de ce code.

Pour l'article L. 2321-3 du code de la défense, les conditions d'application en Outre-Mer sont prévues à l'article L. 1 : *« Le code de la défense est applicable de plein droit sur l'ensemble du territoire de la République, à moins qu'il n'en dispose autrement ».*

5.2.3. Textes d'application

Les conditions d'application du dispositif proposé, et notamment la juste rémunération liée à l'obligation à la charge des OCE désignés OIV de mettre en œuvre les dispositifs de détection, seront définies par décret en Conseil d'Etat.

C- Elargir aux hébergeurs de données l'obligation de communication à des fins exclusives d'alerte d'utilisateurs de systèmes vulnérables ou attaqués, élargir la communication à celles des données techniques des sous-traitants des autorités publiques, OIV et OSE et rationaliser ladite procédure en supprimant l'assermentation des agents de l'autorité nationale de sécurité des systèmes d'information

1. ÉTAT DES LIEUX

1.1. CONTEXTE

Le monde numérique, en mutation constante, recourt à des technologies innovantes ou à de nouveaux types d'architectures ou d'organisations visant à rationaliser la gestion de la masse des données numériques et à mutualiser les coûts d'hébergement et d'opération ou à promouvoir des modèles économiques dynamiques comme celui de la sous-traitance.

L'exemple du *cloud computing* est particulièrement topique à cet égard. Il offre des avantages aux utilisateurs en termes d'économies de coûts, de flexibilité, d'efficacité, de sécurité et d'adaptabilité[393]. De nombreuses offres de services sont désormais disponibles sur le marché, que ce soit pour l'hébergement d'infrastructures (IaaS – *Infrastructure as a Service*), la fourniture de plateformes de développement (PaaS – *Platform as a Service*) ou celle de logiciels en ligne (SaaS – *Software as a Service*). Ces offres sont proposées dans des *clouds* publics (service partagé et mutualisé entre de nombreux clients), privés (*cloud* dédié à un client) ou hybrides (combinaison des modèles public et privé)[394].

Devenu un objet juridique[395], le *cloud* est surtout une réalité économique et commerciale[396] qui concerne tout autant les entreprises que les autorités publiques. L'informatique nuagique est même désormais au cœur de la stratégie numérique de l'Etat. Avec l'adoption de la doctrine *cloud* au centre, le Gouvernement a fait du *cloud* « *un prérequis pour tout nouveau projet numérique au sein de l'Etat ou refonte substantielle de l'architecture applicative existante* »[397].

---

[393] Code de Conduite des Fournisseurs d'Infrastructures *Cloud* relatif à la Protection des Données 9 Février 202 ;

[394] Le *cloud computing* ; Recommandations pour les entreprises qui envisagent de souscrire à des services de *cloud computing*, CNIL ;

[395] « Le numérique, et en particulier le *cloud*, témoigne de l'une de ces accélérations de l'histoire qui, selon le doyen Savatier, force le juriste à une adaptation continue du droit à la réalité sociale », Discours de Jean-Marc Sauvé, Vice-Président du Conseil d'Etat, le 18 octobre 2018;

[396] Par exemple, le marché mondial du *cloud* public est passé de 196,7 à 354,6 milliards de dollars de 2020 à 2022, Sophy Caulier, « Numérique : le *cloud*, enjeu de souveraineté », *Le Monde*, 16 février 2020 ; Selon le Gartner Group, d'ici 2025, 51 % du budget des entreprises françaises va être consacré aux solutions de *cloud computing* plutôt qu'en informatique traditionnelle ; si 58 % de ces entreprises se tournent vers le *cloud* pour leurs logiciels applicatifs en 2022, ce chiffre dépasserait 66 %, soit deux entreprises sur trois, en 2025.

[397] Stratégie nationale pour le Cloud, dossier Presse, 17 mai 2021.

Assez logiquement, les cyberattaquants se saisissent de cette nouvelle réalité. Celle-ci doit donc être appréhendée en son entier par les moyens d'action de l'ANSSI. L'Agence s'appuie sur la contribution d'opérateurs en mesure de lui fournir des données lui permettant d'identifier ces victimes aux fins de les alerter. Les hébergeurs de données sont des acteurs névralgiques disposant d'une visibilité unique sur leurs clients. Cette visibilité permet de mettre au jour des victimes en plus grand nombre, mais également des pans entiers d'infrastructures d'attaques.

Enfin, les sous-traitants des autorités publiques, des OIV et des OSE sont détenteurs de données tout aussi sensibles que leurs donneurs d'ordre. Les cyberattaquants les ont immédiatement identifiés comme pouvant servir de relais aux attaques visant *in fine* les autorités publiques et opérateurs précités. Ils doivent, alors, bénéficier de la même protection que ces derniers.

1.2. CADRE GENERAL

La loi n° 2013-1168 du 18 décembre 2013 précitée[398] a créé un dispositif pour assurer la cybersécurité des activités d'importance vitale. Des mesures de sécurité s'appliquent tant aux opérateurs d'importance vitale (OIV) ou opérateurs de services essentiels (OSE) qu'aux opérateurs publics ou privés qui participent à ces systèmes[399].

En particulier, cette loi a créé l'article L. 2321-3 du code de la défense, lequel a été complété par la loi n° 2018-607 du 13 juillet 2018[400], qui précise dans quels cas l'Agence nationale de la sécurité des systèmes d'information (ANSSI) peut demander des informations aux opérateurs de communications électroniques (OCE) :

- l'alinéa premier prévoit que, pour les besoins de la sécurité des SI d'un OIV, d'un OSE ou d'une autorité publique, l'ANSSI peut demander à l'OCE l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information (SI) vulnérables, menacés ou attaqués. Le but est de les alerter sur la vulnérabilité ou l'atteinte de leur système ;
- le deuxième alinéa prévoit que, lorsque l'ANSSI est informée, en application de l'article L. 33-14 du CPCE, de l'existence d'un événement affectant la sécurité des SI d'un OIV, d'un OSE ou d'une autorité publique, ses agents habilités et assermentés peuvent obtenir de la part des OCE les données techniques strictement nécessaires à l'analyse de cet événement, ces données ne pouvant être exploitées qu'aux seules fins de caractériser la menace affectant la sécurité de ces systèmes, à l'exclusion de toute autre exploitation.

[398] 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.

[399] Article L. 1332-6-1 du code de la défense pour les OIV et article 7 du décret n° 2018-384 du 23 mai 2018 pour les OSE.

[400] 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.

1.3. CADRE CONSTITUTIONNEL ET INTERPRETATION DU CONSEIL D'ETAT

1.3.1. La communication des données par les hébergeurs

Les données mentionnées au premier alinéa de l'article L. 2321-3 du code de la défense sont celles que les hébergeurs collectent déjà, conformément au décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Ce décret a abrogé le décret n° 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Cette abrogation avait été rendue nécessaire par la décision d'Assemblée du Conseil d'Etat du 21 avril 2021[401], qui tirait lui-même les conséquences, en droit interne, des décisions de la Cour de justice de l'Union européenne (CJUE) interdisant la conservation généralisée des données[402], et plus particulièrement de celle rendue sur sa question préjudicielle, *La Quadrature du Net*, du 6 octobre 2020. En particulier, le Conseil d'Etat a estimé que la conservation généralisée aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, comme cela est requis par la CJUE. Conformément aux exigences de la Cour, il a imposé au Gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace et jugé illégale l'obligation de conservation généralisée des données (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins autres que ceux de la sécurité nationale, notamment la poursuite des infractions pénales, raison pour laquelle le décret n° 2011-219 a été abrogé et remplacé par le décret du 20 octobre 2021.

En tout état de cause, les données qui sont recueillies par l'ANSSI dans les conditions du II *bis* de l'article L. 34-1 modifié du code des postes et des communications électroniques ne sont pas toutes les données conservées par les hébergeurs, mais seulement les données mentionnées aux articles 2 et 5 (s'agissant de l'article 5, seulement les adresses IP source et port associé) du décret n° 2021-1362 précité. Ces données ont été considérées comme les moins sensibles puisqu'elles sont conservées par les OCE et les hébergeurs de manière généralisée et indifférenciée pendant une période de temps limitée et définie par les textes. Il n'y a donc pas d'atteinte supplémentaire à une liberté ou un droit constitutionnellement protégé.

1.3.2. L'assermentation des agents

Les agents de l'ANSSI à qui les OCE communiquent les informations demandées au titre de l'article L. 2321-3 du code de la défense sont spécialement habilités et assermentés.

---

[401] *French data Network et a.*, n° 393099, 394922, 397844, 397851, 424717, 424718.

[402] CJUE, 21 déc. 2016, *Télé2 Sverige AB*, n° C-203/15 et C-698/15 ; CJUE 2 oct. 2018, *Ministerio fiscal*, n° C-207/16 et CJUE 6 oct. 2020, *La Quadrature du Net et a.*, n° C-511/18, C-512/18 et C-520/18.

L'assermentation est une garantie exigée par le Conseil constitutionnel dans le seul cas où les agents concernés ont pour mission **la recherche ou la poursuite d'infractions pénales**, dans la mesure où les actes qu'ils prennent ont le caractère de constatations et peuvent aboutir à des sanctions[403].

De la même manière, le rapport du Conseil d'Etat sur les pouvoirs d'enquête de l'administration datant d'avril 2021 précise le rôle de l'assermentation (pages 84 à 86) : « *[…] la loi prévoit que les agents habilités, commissionnés ou agréés doivent être assermentés pour pouvoir rechercher et constater des infractions pénales. La prestation de serment constitue l'engagement solennel de l'agent, généralement pris devant le président du tribunal judiciaire du ressort de son affectation, ce qui est une manifestation du caractère judiciaire des fonctions qu'il exerce, de bien remplir ses fonctions et de respecter les règles déontologiques inhérentes à leur exercice. […] Ce serment est une condition de la régularité des actes que l'agent effectuera ensuite. Selon une jurisprudence fort ancienne de la Cour de cassation, les procès-verbaux établis par un agent non assermenté sont entachés de nullité* »[404]. Le Conseil d'Etat a étendu cette exigence aux contrôles administratifs[405].

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le dispositif actuel de l'article L. 2321-3 du code de la défense nécessite d'être amélioré pour des raisons organisationnelles, opérationnelles et procédurales.

2.1.1. Sur le plan organisationnel

L'ANSSI ne peut, à ce jour, utiliser le dispositif de l'article L. 2321-3 alinéa 2 que lorsqu'il s'agit directement des autorités publiques, des opérateurs d'importance vitale ou des opérateurs de services essentiels, même lorsqu'elles ont confié l'exploitation de leurs systèmes à un tiers. La pratique démontre que ce dispositif devrait être étendu aux opérateurs publics ou privés qui participent aux systèmes d'information des autorités publiques, des OIV et des OSE.

En effet, ces sous-traitants, lorsqu'ils travaillent au profit des autorités publiques, des OIV et des OSE, ont accès à des informations qui sont aussi critiques que celles manipulées par leurs donneurs d'ordres. L'ANSSI a alors constaté que les opérateurs publics ou privés qui participent en tant que sous-traitants aux systèmes des autorités publiques, OIV et OSE, représentent une porte d'entrée de prédilection pour les cyber-attaquants qui visent, par rebonds, les systèmes d'informations des entités plus critiques (autorités publiques, OIV, OSE, etc.).

---

[403] Cf., par exemple, la décision n° 2020-841 QPC du 20 mai 2020, *La Quadrature du Net et autres*, relative aux agents de la HADOPI pour la constatation d'actes de contrefaçon, points 9 et 10.

[404] Les pouvoirs d'enquête de l'administration, rapport du Conseil d'Etat d'avril 2021.

[405] CE, 17 nov. 2017, n° 400976.

Ces sous-traitants sont d'ailleurs déjà soumis au respect des règles de sécurité prévues par les articles L. 1332-6-1 et R. 1332-41-2 du code de la défense pour ce qui concerne les prestataires d'OIV et par les articles 7 et 17 du décret n° 2018-384 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique pour ce qui concerne les OSE.

2.1.2. Sur le plan opérationnel

L'ANSSI est confrontée à deux changements majeurs : d'une part, les pratiques de conception des réseaux évoluent rapidement ; d'autre part, le recours aux technologies en nuage (*cloud*) est exponentiel.

Ces évolutions changent les usages des utilisateurs et des potentielles victimes. Aujourd'hui, les clients d'OCE ne sont plus les seules victimes d'activités malveillantes. Désormais, les services fournis par des hébergeurs de données (gestion de serveurs, machines virtuelles, etc.) font aussi l'objet de cyberattaques ; leurs clients doivent être considérés comme des victimes, à l'instar des abonnés d'OCE[406].

Dans sa rédaction actuelle, l'article L. 2321-3 alinéa 1er du code de la défense renvoie au CPCE pour son application et limite donc l'applicabilité du dispositif aux OCE. Pour tenir compte de l'évolution des pratiques, il est donc proposé d'étendre aux hébergeurs de données le dispositif prévu pour les OCE. L'ANSSI doit pouvoir obtenir les mêmes informations des hébergeurs de données que des OCE. Ainsi, il est nécessaire d'inclure dans le dispositif prévu par l'article L. 2321-3 alinéa 1er les hébergeurs de données visés au 2 du I de l'article 6 de la LCEN.

Les données de connexion conservées par les hébergeurs de données sont énumérées dans un décret d'application spécifique[407]. Il s'agit tant de données d'identification que de données de paiement. L'ANSSI n'accédera toutefois qu'aux seules données permettant l'identification de la victime (article 2 du décret n° 2021-1362) à partir d'adresses IP source avec port associé (article 5 du décret n° 2021-1362). Comme pour le dispositif en place avec les OCE, il s'agit de poursuivre un objectif de protection, en permettant d'alerter la victime.

L'ajout des hébergeurs au premier alinéa de l'article L. 2321-3 du code de la défense nécessite de prévoir une compensation des surcoûts identifiables et spécifiques des prestations qu'ils vont assurer.

Par ailleurs, pour assurer une cohérence, en ce qui concerne la compensation des OCE, entre le dispositif prévu au premier alinéa de l'article L. 2321-3 et celui prévu à son deuxième alinéa, il convient également de prévoir que les surcoûts identifiables et spécifiques des prestations assurées par les opérateurs de communications électroniques à la demande de l'ANSSI en application du deuxième alinéa seront compensés selon des modalités prévues par décret en Conseil d'État.

[406] Panorama de la cybermenace 2022.

[407] Décret n° 2021-1362 du 20 octobre 2021 précité.

2.1.3. Sur le plan procédural

L'assermentation des agents ayant accès aux informations issues de ces dispositifs implique une obligation de secret professionnel dont le non-respect est puni par le code pénal (article R. 2321-5 du code de la défense) pour ces agents assermentés. Tel qu'appliqué aujourd'hui, ce dispositif n'est pas adapté.

L'assermentation est une garantie exigée pour les agents dont la mission est la recherche ou la poursuite d'infractions pénales, dans la mesure où les actes qu'ils prennent ont le caractère de constatations et peuvent aboutir à des sanctions. Or, ces missions ne sont pas celles des agents de l'ANSSI, qui exploitent les informations collectées auprès des OCE aux seules fins d'identifier et d'alerter les victimes d'attaques informatiques.

Parce qu'il suppose un déplacement de l'agent au Tribunal judiciaire de Paris pour la prestation de serment, le dispositif actuel est extrêmement lourd à mettre en place, au regard du nombre d'agents susceptibles de manipuler les données pour les analyser et les qualifier (analystes en charge de la connaissance de la menace, liaisons avec les opérateurs, liaisons avec les victimes, administrateurs d'outils, *etc*.), ainsi que du renouvellement régulier des agents au sein des services concernés de l'ANSSI. La totalité des agents des bureaux effecteurs de la SDO sont susceptibles d'appartenir à cette catégorie soit, dans l'état actuel des effectifs, près de 200 agents sur un total de 280.

En outre, les données reçues des OCE ne suffisent pas toujours pour identifier une victime et aboutir à un signalement pertinent. Dans certaines situations, les analystes de l'ANSSI doivent donc réaliser des recherches complémentaires, sur des services en ligne et hors ligne, pour compléter les éléments obtenus et orienter leurs travaux (en confirmant que la victime n'est pas française, en cherchant à mieux comprendre le statut de l'entreprise, *etc*.). La simple transmission en interne à d'autres analystes de l'ANSSI des données reçues par les OCE, même spécialement habilités et sensibilisés sur le statut particulier de ces données, expose les agents assermentés, alors même que cette transmission est nécessaire pour qualifier l'information et assurer un signalement de qualité.

Enfin, il faut relever que, par rapport au régime d'habilitation générale mis en place par l'ANSSI pour l'ensemble de ses dispositifs opérationnels, ce dispositif d'assermentation n'apporte aucune garantie complémentaire.

2.2. OBJECTIFS POURSUIVIS

L'objectif poursuivi par cette mesure est d'étendre la couverture des moyens d'action de l'ANSSI pour pouvoir approfondir la connaissance des modes opératoires des cyberattaquants et identifier et alerter de façon étendue les victimes de cyberattaques, grâce à l'élargissement du périmètre des opérateurs pouvant fournir des éléments d'identification de ces victimes, à l'extension de l'action de l'agence aux sous-traitants des autorités publiques, des OIV et des OSE pour approfondir celle menée à l'égard des donneurs d'ordre et contrer l'effet rebond des cyberattaques.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

- **Concernant l'extension du dispositif aux sous-traitants** des autorités publiques, OIV et OSE, il est nécessaire de compléter l'article L. 2321-3 alinéa 2 du code de la défense.
- **Concernant l'extension du dispositif aux hébergeurs de données**, l'ajout de la possibilité de l'ANSSI de requérir les informations nécessaires à l'identification de la victime auprès de cette catégorie d'acteurs définie par la LCEN est nécessaire.
- **Concernant la modification relative à l'assermentation**, une option possible consistait à supprimer la sanction pénale au niveau réglementaire, dans la mesure où les agents de l'ANSSI, du fait de leurs statuts, sont déjà soumis à une obligation de secret professionnel et de discrétion professionnelle. Ces obligations sont prévues dans les textes suivants :
    - articles L. 121-6 et L. 121-7 du code général de la fonction publique pour tout agent public ;
    - article L. 4121-2 du code de la défense pour les militaires.

  Il est toutefois nécessaire de garantir aux OCE que sera préservé le secret des informations qu'ils communiquent à l'ANSSI, d'autant plus qu'il s'agit de données à caractère personnel.

  Une autre option aurait consisté à assermenter l'ensemble des analystes susceptibles de traiter les données, y compris la chaîne hiérarchique. Toutefois, l'assermentation implique une organisation lourde peu compatible avec le nombre d'agents pouvant intervenir au sein de la sous-direction des opérations (SDO) de l'ANSSI. Qui plus est, la forte rotation des effectifs de SDO risquerait d'en altérer les capacités et représenterait une véritable contrainte.

  Il est donc proposé de supprimer l'assermentation tout en maintenant l'habilitation spéciale pour les agents amenés à manipuler les données fournies par les OCE. En effet, l'objectif poursuivi par l'article L. 2321-3 du CODEF consiste à prévenir les utilisateurs ou les détenteurs de SI vulnérables, menacés ou attaqués, afin de les alerter de la vulnérabilité ou de l'atteinte de leur système. Il ne s'agit pas de la recherche ou de la poursuite d'infractions pénales, pour lesquelles une assermentation s'avèrerait nécessaire au regard de la jurisprudence du Conseil constitutionnel ou du Conseil d'Etat.

La suppression de l'assermentation et le maintien de l'habilitation spéciale des agents de l'ANSSI permettent de garantir un niveau plus élevé de protection des données communiquées par les OCE à l'ANSSI, puisque cela conduit à responsabiliser pénalement, non plus les seuls agents en contact avec les OCE, mais bien l'ensemble de la chaîne de traitement des données au sein de l'ANSSI.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La présente disposition modifie l'article L. 2321-3 du code de la défense.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les modifications envisagées de l'article L. 2321-3 n'ont pas d'effet supplémentaire au regard du droit international et du droit de l'Union européenne que lorsque le dispositif a été adopté en vertu de la 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.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les hébergeurs de données se verront imposer de nouvelles obligations pour contribuer à la cybersécurité et à l'identification des victimes de cyberattaques. Comme dans le cadre des autres dispositifs impliquant des hébergeurs et comme les OCE dans le cadre du dispositif existant, ils pourront être compensés pour leurs actions. En outre, les données d'identification des utilisateurs sont déjà conservées par les hébergeurs pour leur propre facturation ou dans le cadre d'obligations légales préexistantes. Ainsi, aucun nouvel investissement financier n'est à prévoir de leur part avant de pouvoir répondre aux demandes de l'ANSSI.

4.2.3. Impacts budgétaires

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

4.4.1. Impacts sur l'ANSSI

Les évolutions proposées du cadre législatif visent avant tout à mieux répondre à des besoins opérationnels. Il s'agit d'un ajustement qui favorisera, d'une part, la connaissance et le suivi des modes opératoires des attaquants et limitera, d'autre part, la pression exercée sur le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) en matière de signalement sur des entités ne relevant pas directement du périmètre critique de l'ANSSI.

4.4.2. Impacts sur l'ARCEP

L'ARCEP dispose déjà d'un accès complet et permanent aux données recueillies ou obtenues en application des articles L. 2321-2-1 et de l'alinéa 2 de L. 2321-3 du code de la défense, ainsi qu'aux dispositifs de traçabilité des données collectées. En outre, elle peut solliciter de l'ANSSI tous les éléments nécessaires à l'accomplissement de sa mission (article L. 36-14 du CPCE). Concernant le contrôle de l'ARCEP sur l'application de l'article L. 2321-3 alinéa 2 du CODEF, l'ANSSI fournira la liste des agents spécialement habilités lui permettant de s'assurer que seuls ces agents ont accès aux données communiquées. Cette mesure devrait avoir un impact limité sur les moyens de l'ARCEP.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette mesure contribuera à renforcer la sécurité des systèmes d'information en France.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Cette mesure permettra d'identifier plus efficacement les victimes d'attaques informatiques, et donc de mieux lutter contre les attaques informatiques.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. MODALITES D'APPLICATION ET CONSULTATIONS MENEEES

5.1. CONSULTATIONS MENEES

Conformément à l'article L. 36-5 du Code des postes et des communications électroniques, cette disposition a été présentée à l'ARCEP qui a rendu son avis le 9 mars 2023[408].

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées par les hébergeurs à la demande de l'ANSSI seront définies dans un décret en Conseil d'Etat.

[408] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années2024-2030