Projet de loi actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (n° 2630)

Document faisant état de l'avancement des travaux de
Mme Sabine Thillaye, rapporteure pour avis

Mercredi 15 avril 2026

COMMENTAIRE DES ARTICLES DU PROJET DE LOI DÉLÉGUÉS AU FOND À LA COMMISSION DES LOIS

Article 17
(art. L. 861-4 du code de la sécurité intérieure [*nouveau*])
Procédure de déclaration préalable avant tout publication, diffusion et communication à un tiers

➢ Résumé du dispositif et effets principaux

L'article 17 crée une procédure de déclaration préalable avant toute publication, diffusion ou communication à un tiers d'une œuvre de l'esprit portant sur les activités d'un service de renseignement appartenant au premier cercle et dont l'auteur est un agent, ou ancien agent, de ce service. Le ministre responsable du service concerné, une fois l'œuvre transmise, peut, dans certains cas, demander à l'auteur d'y apporter des modifications. Si celui-ci les refuse, alors le ministre peut s'opposer à la publication, diffusion et communication de l'œuvre en question.

➢ Dernière modification législative intervenue

L'article 42 de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense a créé, aux articles L. 4122-11 et suivants du code de la défense, une procédure de déclaration préalable auprès du ministre pour les militaires et les anciens militaires ayant occupé des fonctions sensibles ou très techniques et qui souhaitent travailler pour un État étranger ou une entreprise étrangère.

I. LE DROIT EXISTANT

● Les services spécialisés de renseignement dits « du premier cercle » sont énumérés à l'article R. 811-1 du code de la sécurité intérieure (CSI). Il s'agit de :

– la direction générale de la sécurité extérieure (DGSE) ;

– la direction du renseignement et de la sécurité de la défense (DRSD) ;

– la direction du renseignement militaire (DRM) ;

– la direction générale de la sécurité intérieure (DGSI) ;

– la direction nationale du renseignement et des enquêtes douanières (DNRED) ;

– et du service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers » (TRACFIN).

● Les informations qui relèvent du secret de la défense nationale sont protégées par différents textes, notamment par les articles R. 2311-2 et suivants du code de la défense, qui précisent notamment les différents niveaux de classification et les enjeux attachés à la divulgation de ces informations.

Ainsi, comme le rappelle l'étude d'impact du présent projet de loi, il est possible aujourd'hui d'engager une procédure disciplinaire à l'égard d'un agent qui serait l'auteur d'un ouvrage qui divulguerait des informations protégées. L'article 9 du décret n° 2015-386 du 3 avril fixant le statut des fonctionnaires de la DGSE interdit ainsi à ces agents de *« communiquer, sous quelque forme que ce soit, sur des sujets en rapport avec les activités de la direction générale de la sécurité extérieure* ».

Les agents ou anciens agents qui portent atteinte au secret de la défense nationale sont également passibles de sanctions pénales, pour compromission. Les articles 413-9 à 413-12 du code pénal sanctionnent ainsi les atteintes au secret de la défense nationale de sept ans d'emprisonnement et de 100 000 euros d'amende, lorsque celles-ci sont le fait d'un agent ou d'un ancien agent.

Est également sanctionné le fait de révéler les identités protégées de certains agents, conformément aux articles 413-13 et 413-14 du code pénal.

Ces différentes sanctions pénales nécessiteraient néanmoins d'être complétées. Ainsi, l'étude d'impact indique que ces sanctions ne suffiraient pas à protéger le secret de la défense nationale, « *en ce qu'elles ne peuvent intervenir que postérieurement à la réalisation du dommage* » (1). Elle l'illustre en citant trois ouvrages écrits par des anciens employés de la DGSE et parus récemment, dont l'un qui décrit précisément les techniques et moyens employés, ainsi que la localisation de certaines entités du service.

L'article 17 propose donc d'instaurer une procédure en amont pour éviter la diffusion d'informations sensibles.

II. LES DISPOSITIONS DU PROJET DE LOI INITIAL

Le 2° de l'article 17 insère un nouvel article L. 861-4 au sein du chapitre I^er^ du titre VI du livre VIII du CSI, qui concerne la protection du secret de la défense

(1) Étude d'impact du présent projet de loi, p 247.

nationale et de l'anonymat des agents. Ce nouvel article crée une procédure de contrôle a priori de toute publication ou diffusion d'une œuvre de l'esprit (1) par un agent d'un service spécialisé de renseignement, dès lors qu'elle porte sur les activités de l'un de ces services.

● Le I précise que les agents concernés sont ceux qui appartiennent aux services spécialisés de renseignement mentionnés à l'article L. 811-2 du CSI, soit les six services cités *supra*.

Dès lors qu'un agent souhaite publier ou diffuser une œuvre de l'esprit dont il est l'auteur et qui porte sur les activités du service auquel il appartient ou a appartenu, il est soumis à une double obligation :

– le déclarer au ministre responsable du service concerné ;

– transmettre au même ministre l'œuvre ou les éléments d'information avant la publication ou la diffusion de l'œuvre, et avant tout communication à des tiers dans ce but.

Cette transmission doit intervenir avec un délai de préavis qui sera fixé par décret en Conseil d'État.

L'obligation de déclaration et de transmission préalable s'applique pendant une période de dix ans suivant la cessation des fonctions de l'agent. Cette durée se justifie, selon les services entendus par votre rapporteure, par le fait que certaines opérations se conduisent sur le temps long, et que certaines identités doivent rester protégées pendant plusieurs années.

● Le II précise la suite de la procédure.

Une fois l'œuvre transmise, le ministre peut demander à l'auteur de l'œuvre de la modifier avant toute communication à des tiers s'il estime que la publication ou la diffusion de celle-ci, ou toute communication à des tiers dans ce but, est de nature à :

– porter atteinte au secret de la défense nationale ;

– porter atteinte à certains services ou unités spécialisés ;

– conduire à une révélation des procédures opérationnelles ou des capacités techniques des services spécialisés de renseignement de nature à nuire à leur efficacité opérationnelle ou à compromettre la sécurité de leurs agents.

Si l'agent refuse de procéder à ces modifications, alors le ministre peut s'opposer à la communication de l'œuvre. Cette décision d'opposition peut intervenir

(1) Au sens des articles L. 112-1, L. 112-2 et L. 112-3 du code de la propriété intellectuelle.

à l'issue d'une phase contradictoire : la personne intéressée doit avoir eu la possibilité de présenter des observations écrites et, sur sa demande, orales.

● La méconnaissance de l'obligation de déclaration préalable ou de l'opposition à la communication de l'œuvre concernée est passible d'un an d'emprisonnement et de 3 750 euros d'amende (III du nouvel article L. 861-4). Cette infraction pourra se cumuler avec les infractions déjà existantes en matière de compromission.

● Le IV renvoie à un décret en Conseil d'État la détermination des modalités d'application de l'article. Celui-ci devra préciser les modalités de communication au ministre de la version amendée de l'œuvre et les délais de notification de la décision d'opposition.

Enfin, le 1° du présent article 17 complète le titre du chapitre I^er^ du titre VI du livre VIII du CSI afin qu'il englobe le nouvel article L. 861-4 relatif à la protection de l'action des services spécialisés de renseignement.

Ce dispositif est similaire à celui prévu pour les départs à l'étranger de militaires et anciens militaires ayant exercé des fonctions sensibles. L'article L. 4122-11 du code de la défense les oblige ainsi à déclarer ce changement d'activité au ministre de la défense, qui peut s'y opposer lorsqu'il estime que l'exercice de cette activité comporte un risque de divulgation de savoir-faire nécessaires à la préparation et à la conduite d'opérations militaires et que cette divulgation est susceptible de porter atteinte aux intérêts fondamentaux de la Nation.

● Dans son avis sur le présent projet de loi, le Conseil d'État estime que l'atteinte à la liberté d'expression prévue par le présent article « *répond à de fortes considérations d'intérêt général, en lien avec les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux* » (1). Il précise également que les sanctions pénales prévues en cas de non-respect des diverses obligations sont adéquates et proportionnées. Il en déduit que les dispositions de l'article ne présentent pas d'obstacle d'ordre constitutionnel ou conventionnel.

Le Conseil constitutionnel a d'ailleurs déjà admis que le législateur pouvait assurer une conciliation entre la liberté d'expression et de communication et la sauvegarde des intérêts fondamentaux de la Nation, le secret de la défense nationale participant à ce dernier principe (2).

Selon l'étude d'impact, ce dispositif permettra d'instaurer « *un dialogue préalable entre l'auteur et le ministère de tutelle* » de nature à préserver l'efficacité

---

(1) Avis du Conseil d'État sur un projet de loi actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, séance du 25 mars 2025, n° 410563, point 39.

(2) Voir notamment la décision n° 2016-738 DC du 10 novembre 2016 sur la loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias.

opérationnelle des services et la possibilité pour les agents de produire des témoignages [(1)].

*

* *

Article 18

(art. L. 851-3 du code de la sécurité intérieure et art. 6 et 9 de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France)

Restaurer l'usage des URL dans les traitements algorithmiques utilisés par les services de renseignement et élargir les finalités d'utilisation de ces traitements

➢ **Résumé du dispositif et effets principaux**

L'article 18 du projet de loi réécrit l'article L. 851-3 du code de la sécurité intérieure (CSI), qui prévoit le recours par les services spécialisés de renseignement aux traitements algorithmiques pour certaines finalités.

Il étend le dispositif en ajoutant une finalité : la technique de renseignement pourra viser à détecter les menaces en lien avec la criminalité et la délinquance organisées.

Il tire également les conséquences de la décision du Conseil constitutionnel du 12 juin 2025 sur la loi visant à sortir la France du piège du narcotrafic : il réintroduit la possibilité pour les services spécialisés de renseignement d'utiliser des adresses complètes de ressources utilisées sur internet (aussi dites « URL » pour *Uniform Resource Locator*), tout en l'assortissant de garanties supplémentaires.

➢ **Dernière modification législative intervenue**

L'article 6 de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a étendu les finalités pour lesquelles les services spécialisés de renseignement peuvent recourir aux traitements algorithmiques sur les données transitant par les réseaux des opérateurs et des fournisseurs de services internet, pour y inclure la prévention des ingérences étrangères et des menaces contre la défense nationale. Cette extension est bornée dans le temps, au 1er juillet 2028.

(1) Étude d'impact précitée, p 254.

I. LE DROIT EXISTANT

A. L'ENCADREMENT JURIDIQUE DU RECOURS AUX TECHNIQUES DE RENSEIGNEMENT PAR LES SERVICES SPÉCIALISÉS

L'article L. 811-3 du CSI autorise les services spécialisés de renseignement à recourir aux techniques mentionnées au titre V du livre VIII du même code pour le recueil des renseignements relatifs, notamment, à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :

– l'indépendance nationale, l'intégrité du territoire et la défense nationale (1°) ;

– 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 (2°) ;

– la prévention du terrorisme (4°) ;

– la prévention de la criminalité et de la délinquance organisées (6°).

L'accès administratif des services de renseignement aux données de connexion est encadré par le chapitre Ier du titre V du livre VIII du CSI.

L'article L. 851-1 du CSI énumère ainsi les données de connexion qui peuvent être recueillies par les services spécialisés de renseignement sous réserve d'une autorisation délivrée par le Premier ministre.

Il s'agit « des *informations ou documents traités ou conservés* » par les réseaux ou services de communications électroniques des opérateurs, « *y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ».

Le CSI distingue ainsi les données de connexion, qui permettent l'acheminement d'une communication électronique, des données de contenu, qui visent le contenu de correspondances échangées ou encore d'informations consultées (1).

L'autorisation de recueillir ces données doit être délivrée dans les conditions prévues au chapitre Ier du titre II du livre VIII du CSI, c'est-à-dire par le Premier ministre après avis non contraignant de la commission nationale de contrôle des techniques de renseignement (CNCTR).

---

(1) Comme le précise également l'article L. 34-1 du code des postes et des communications électroniques.

La procédure d'autorisation par la CNCTR (chapitre Ier du titre II du livre VIII du code de la sécurité intérieure)

La mise en œuvre des techniques de recueil de renseignement est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (article L. 821-1).

Toute demande doit être motivée et préciser les éléments énumérés à l'article L. 821-2, notamment les techniques à mettre en œuvre, les finalités poursuivies et la durée de validité de l'autorisation.

Toute demande de renouvellement d'une autorisation doit préciser les raisons qui la justifient au regard des finalités poursuivies (article L. 821-2).

La commission rend un avis au Premier ministre dans un délai de vingt-quatre heures, sauf lorsque la demande est examinée par la formation restreinte ou par la formation plénière, auquel cas l'avis doit être rendu dans un délai de 72 heures. En l'absence d'avis transmis, il est réputé rendu (article L. 821-3).

Si la commission émet un avis défavorable et que l'autorisation est néanmoins délivrée, le Conseil d'État est saisi et doit statuer dans un délai de vingt-quatre heures. La décision d'autorisation ne peut être exécutée avant que le Conseil d'État ait statué, sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné une mise en œuvre immédiate (article L. 821-1).

L'autorisation est délivrée par le Premier ministre pour une durée maximale de quatre mois (article L. 821-4). Lorsqu'elle est délivrée après un avis défavorable de la CNCTR, elle précise les motifs pour lesquels l'avis n'a pas été suivi.

Il est explicitement exclu qu'un parlementaire, un magistrat, un avocat ou un journaliste fasse l'objet d'une demande à raison de l'exercice de son mandat ou de sa profession (article L. 821-7).

Toute autorisation est renouvelable dans les mêmes conditions que celles énoncées précédemment, conformément au premier alinéa de l'article L. 821-4.

Ainsi, les services peuvent mettre en œuvre diverses techniques de renseignement sous le contrôle de la CNCTR, dont l'analyse de données par des traitements algorithmiques.

B. LE RECOURS AUX TRAITEMENTS ALGORITHMIQUES PRÉVU PAR L'ARTICLE L. 851-3 A ÉTÉ PROGRESSIVEMENT ÉLARGI, JUSQU'À LA CENSURE CONSTITUTIONNELLE INTERVENUE EN JUIN 2025

L'article L. 851-3 du CSI autorise les services spécialisés de renseignement dits « du premier cercle » (1) à recourir à des traitements automatisés sur les données transitant par les réseaux des opérateurs et des services de communication en ligne, pour détecter certaines menaces en lien avec les finalités autorisées.

(1) Qui sont ceux mentionnés à l'article R. 811-1 du CSI : direction générale de la sécurité extérieure, direction du renseignement et de la sécurité de la défense, direction du renseignement militaire, direction générale de la sécurité intérieure, direction nationale du renseignement et des enquêtes douanières et le service de traitement du renseignement et de l'action contre les circuits financiers clandestins ».

● Cette possibilité a été introduite par l'article 5 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, pour une durée initialement limitée : l'article 25 de la même loi prévoyait une application jusqu'au 31 décembre 2018.

Périmètre de l'article L. 851-3 dans la version de la loi du 24 juillet 2015

La mise en œuvre de traitements automatisés sur les données des opérateurs de communications électroniques et des fournisseurs de service Internet est autorisée pour les seuls besoins de la prévention du terrorisme. L'objectif est de détecter des connexions susceptibles de révéler une menace terroriste. La mise en œuvre de ces traitements doit être autorisée par le Premier ministre.

La CNCTR émet un avis sur la demande d'autorisation et exerce un contrôle permanent sur la mise en œuvre des traitements. Les traitements automatisés peuvent uniquement utiliser les informations ou documents mentionnés à l'article L. 851-1 du CSI, et ne doivent pas permettre l'identification des personnes auxquels se rapportent ces informations et documents.

L'anonymat est levé uniquement lorsque les traitements détectent des données qui sont susceptibles de caractériser l'existence d'une menace à caractère terroriste. Lorsque c'est le cas, le Premier ministre doit explicitement autoriser l'identification de la personne concernée et l'exploitation des données recueillies. Cette autorisation est donnée après avis de la CNCTR. Les données concernées doivent être exploitées dans un délai de soixante jours et être détruites à l'issue de ce délai, sauf si la menace terroriste est confirmée.

Le recours à un algorithme doit être autorisé par le Premier ministre après avis de la CNCTR. L'autorisation précise le champ technique de la mise en œuvre de l'algorithme. Une fois l'autorisation délivrée, l'algorithme est conçu par le groupement interministériel de contrôle pour correspondre aux besoins exprimés par les services de renseignement. Il est donc développé sur mesure, de manière souveraine, pour répondre à la fois aux besoins opérationnels et aux critères arrêtés par le Premier ministre.

Comme l'indique la CNCTR dans son rapport d'activité de 2024, « *l'objectif poursuivi était donc de recouper et analyser un grand nombre d'éléments techniques en vue de détecter des signaux de faible intensité suggérant une menace terroriste* », en limitant l'identification des personnes à celles à l'origine de ces signaux faibles (1). En effet, le recours aux techniques de renseignement algorithmique permet d'analyser un volume très important de données de connexion. Comme le précise la CNCTR dans le rapport précité, les données sur lesquelles les algorithmes tournent ne sont pas mises à disposition des services : ce sont bien uniquement celles qui sont associées aux résultats positifs auxquelles ils ont accès (2).

Le Conseil constitutionnel a validé le recours à cette technique, considérant que l'article ne portait pas une atteinte manifestement disproportionnée au droit au

(1) Commission nationale de contrôle des techniques de renseignement, 9ème rapport d'activité, 2024, p 152.

(2) Ibid, p 153.

respect de la vie privée. À l'appui de sa décision, il souligne que la mise en œuvre de celle-ci est subordonnée à plusieurs garanties :

– le recours à la technique, comme les paramètres du traitement automatisé, sont autorisés par la CNCTR ;

– la première autorisation d'utilisation est délivrée pour une durée limitée à deux mois ;

– la demande de renouvellement doit comporter un relevé du nombre d'identifiants signalés par le traitement automatisé ainsi qu'une analyse de la pertinence de ces signalements ;

– les traitements automatisés utilisent uniquement les informations et documents mentionnés à l'article L. 851-1 et ne doivent pas permettre d'identifier les personnes auxquels ces éléments se rapportent ;

– lorsqu'une donnée est détectée par le traitement comme étant susceptible de caractériser l'existence d'une menace terroriste, une nouvelle autorisation du Premier ministre, sur avis de la CNCTR, est nécessaire pour exploiter les données et identifier les personnes concernées ;

– les données sont exploitées pour une durée limitée et détruites à l'issue ;

– il est exclu d'utiliser la procédure d'urgence pour autoriser le recours à cette technique de renseignement ;

– la technique ne peut être mise en œuvre qu'aux fins de prévention du terrorisme.

La première autorisation de mise en œuvre d'un algorithme a été délivrée le 12 octobre 2017, en raison des contraintes techniques liées à l'élaboration des traitements (1).

● L'expérimentation a été pérennisée par l'article 15 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Dans une délibération datée du 7 avril 2021, la CNCTR a admis le principe d'une pérennisation de l'expérimentation, considérant que la menace terroriste était toujours présente et que « *les impératifs de sécurité nationale* » justifiaient que le dispositif soit conservé (2).

Cet article a également élargi la liste des données pouvant faire l'objet d'un traitement automatisé aux adresses complètes de ressources utilisées sur internet, communément appelées « URL ».

---

(1) Rapport d'activité de l'année 2024 de la CNCTTR précité, p 155.

(2) Délibération de la CNCTR n° 2/2021 du 7 avril 2021.

Comme le rappelle l'étude d'impact du présent projet de loi, ces URL sont des données mixtes, puisqu'elles « *sont certes nécessaires à l'acheminement des communications mais comprennent également des mots faisant référence au contenu de correspondances échangées ou aux informations consultées* » (1). Il en découle qu'elles ne peuvent être assimilées à des données de connexion et doivent être mentionnées explicitement dans le dispositif pour que les services de renseignement puissent les utiliser lorsqu'ils mettent en œuvre les traitements automatisés.

L'étude d'impact du présent projet de loi souligne que le dispositif « *s'avère indispensable pour permettre de détecter des individus inconnus des services de renseignement ou que leurs comportements antérieurs n'avaient jusqu'ici pas permis d'identifier comme menaçants, dans un contexte de persistance de la menace terroriste* ». Elle ajoute que le dispositif a permis à la fois d'identifier des individus porteurs de menace et d'améliorer la connaissance des services sur la manière de procéder de certains individus de la mouvance terroriste (2).

L'article 15, outre la pérennisation de l'expérimentation et l'élargissement des données utilisées aux URL :

– restreint aux services spécialisés du renseignement du premier cercle l'utilisation de la technique ;

– prévoit que les données qui n'ont pas généré d'alerte sont détruites immédiatement ;

– supprime la possibilité de conserver les données ayant généré des alertes dans un délai supérieur à soixante jours ;

– désigne explicitement le groupement interministériel de contrôle comme étant le seul habilité à exécuter les traitements.

Le Conseil constitutionnel, dans sa décision sur la loi du 30 juillet 2021 (3), ne s'est pas prononcé sur les dispositions de l'article 15 qui modifiaient l'article L. 851-3 du CSI.

● L'article 6 de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a élargi le dispositif en ajoutant deux finalités à celle de prévention du terrorisme, pour lesquelles les services de renseignement peuvent avoir recours aux traitements automatisés :

– l'indépendance nationale, l'intégrité du territoire et la défense nationale (1° de l'article L. 811-3 du CSI) ;

---

(1) Étude d'impact du présent projet de loi, p 260.

(2) Étude d'impact du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, p 178.

(3) Conseil constitutionnel, décision n° 2021-822 DC du 30 juillet 2021 sur la loi relative à la prévention d'actes de terrorisme et au renseignement.

– 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 (2° du même article).

Le traitement doit maintenant pouvoir détecter également les connexions susceptibles de révéler des ingérences étrangères et des menaces pour la défense nationale.

L'article 6 consacrait le caractère expérimental de cet élargissement en en bornant son application au 1er juillet 2028 et prévoyait que le Gouvernement doit remettre au Parlement un rapport sur l'application dudit article avant le 1er juillet 2026. L'objectif était que le législateur puisse disposer d'éléments utiles pour décider ou non de pérenniser le recours à ces deux finalités supplémentaires.

Si le Conseil constitutionnel a été saisi sur cette extension, il ne s'est finalement pas prononcé sur la conformité du dispositif à la Constitution : la dissolution de l'Assemblée nationale étant intervenue entretemps, le mandat des députés l'ayant saisi avait pris fin (1).

● En dernier lieu, l'article 15 de la loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic a modifié l'article L. 851-3 du CSI :

– il a élargi les finalités à la prévention de la criminalité et de la délinquance organisées (6° de l'article L. 811-3) ;

– en conséquence, les menaces pouvant être détectées grâce aux traitements sont étendues aux menaces relatives à la criminalité organisée et à la délinquance organisée portant sur des délits punis de dix ans d'emprisonnement en tant qu'elles concernent le trafic de stupéfiants, le trafic d'armes et de produits explosifs, l'importation et l'exportation de ces marchandises prohibées commises en bande organisée ainsi que le blanchiment des produits qui en sont issus ;

– il repousse également la date de fin de l'expérimentation des nouvelles finalités pour l'établir au 31 décembre 2028.

Le Conseil constitutionnel, saisi, a censuré l'intégralité de l'article 15 de la loi du 13 juin 2025 (2).

Il n'a pas exclu le recours au traitement automatisé alimenté par des URL, mais a souligné que des garanties particulières devaient être apportées :

« *l'analyse systématique et automatisée de donnée se rapportant à un nombre très important de personnes est de nature à augmenter considérablement le nombre et la précision des informations qui en sont extraites. Dès lors, la mise en*

(1) Conseil constitutionnel, décision n° 2024-870 DC du 10 juillet 2024 sur la loi visant à prévenir les ingérences étrangères en France.

(2) Conseil constitutionnel, décision n° 2025-885 DC du 12 juin 2025 sur la loi visant à sortir la France du piège du narcotrafic.

œuvre de tels systèmes de surveillance doit être assortie de garanties particulières afin de sauvegarder le droit au respect de la vie privée » (1).

Or, au cas d'espèce, si le Conseil a reconnu qu'un certain nombre de garanties sont attachées au recours à cette technique de renseignement – notamment le contrôle permanent de la CNCTR et l'exclusion de toute donnée permettant d'identifier les personnes – il a souligné que les traitements utilisés, en incluant les URL, « *permettent ainsi de procéder à grande échelle à l'analyse systématique et automatisée de données qui sont susceptibles de porter sur le contenu des correspondances échangées ou des informations consultées dans le cadre de ces communications* ». Le législateur, « *en autorisant de manière générale et indifférenciée* […] *le recours à de tels traitements algorithmiques pour la détection des connexions susceptibles de révéler certaines menaces relatives à la criminalité et à la délinquance organisées, sans autre condition tenant notamment à la nature des données révélées par les adresses complètes de ressources utilisées sur internet* » n'a pas assuré une conciliation équilibrée entre les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de prévention des infractions, et le droit au respect de la vie privée.

Le Conseil a examiné en parallèle la conformité à la Constitution de certaines dispositions de l'article L. 851-3 du CSI, qui étaient complétées par l'article 15. Suivant le même raisonnement, il a considéré que la possibilité d'inclure les adresses URL dans les traitements automatisés n'était pas conforme à la Constitution.

Dans son commentaire sur la décision, le Conseil a précisé que c'était « *l'indétermination des données susceptibles d'être analysées par les traitements algorithmiques – en l'absence de tout critère fixé par le législateur – qui, rapportée à l'ampleur potentielle de tels traitements* », expliquait la censure de l'article 15 (2). Il a confirmé par ailleurs que cette censure ne signifiait pas une interdiction définitive du recours aux traitements algorithmiques pour traiter des URL, mais que celui-ci devait être subordonné à « *un encadrement nettement plus précis des types de données susceptibles d'être recueillies, par le législateur lui-même (et non en reportant les garanties sur la seule effectivité du contrôle confié à la CNCTR)* ».

Finalement, l'article L. 851-3 du CSI, compte tenu de la censure intervenue en juin 2025, permet aux services de renseignement de recourir aux traitements automatisés sur les données de connexion mentionnées à l'article L. 851-1, sans les URL, pour les finalités de prévention du terrorisme, des ingérences étrangères et des menaces pour la défense nationale.

Alors qu'ils avaient l'autorisation d'inclure les URL dans les traitements automatisés depuis 2021, les services de renseignement n'en ont plus la possibilité depuis juin 2025.

---

(1) Conseil constitutionnel, décision précitée, paragraphe 119.

(2) Conseil constitutionnel, commentaire de la décision n° 2025-885 DC du 12 juin 2025 sur la loi visant à sortir la France du piège du narcotrafic, p 16.

II. LES DISPOSITIONS DU PROJET DE LOI INITIAL

L'article 18 du présent projet de loi réécrit l'article L. 851-3 du CSI.

A. LA RÉÉCRITURE DE L'ARTICLE L. 851-3 POUR RÉINTÉGRER LES URL ET ÉTENDRE LES FINALITÉS À LA PRÉVENTION DE LA CRIMINALITÉ ET DE LA DÉLINQUANCE ORGANISÉES

● L'extension des finalités

Le I de l'article L. 851-3 dans la rédaction proposée par l'article 18 du présent texte, sur le modèle actuel, énumère les finalités pour lesquelles les services spécialisés de renseignement peuvent être autorisés à recourir à des traitements algorithmiques pour analyser les données transitant par les opérateurs et les services de communication en ligne.

Aux finalités déjà prévues aujourd'hui (1), il ajoute celle prévue au 6° de l'article L. 811-3 du CSI, soit la prévention de la criminalité et de la délinquance organisées.

Cette finalité ne recoupe pas complètement l'intégralité des infractions susceptibles d'entrer dans le champ de la procédure applicable à la criminalité organisée et à la délinquance organisée au sens du code de procédure pénale, comme le rappelle la CNCTR dans son rapport d'activité de l'année 2023 (2). Elle précise, dans ce même rapport, sa doctrine permettant de délimiter les contours de cette finalité : est ainsi retenu « *un double critère matériel tenant, d'une part, à la réalité d'une action en 'bande organisée'* […] *et, d'autre part, au degré de gravité ou de dangerosité de la menace qu'il s'agit de prévenir, justifiant le recours à des techniques de surveillance en amont d'une éventuelle procédure judiciaire* ». Elle s'intéresse également à l'aspect procédural, en recherchant si *« des techniques spéciales d'enquêtes, assimilables aux techniques relevant du code de la sécurité intérieure, sont susceptibles d'être mises en œuvre pour la recherche, la constatation et la poursuite de ces infractions* » (3). Elle considère par ailleurs que des infractions relevant de la « *grande délinquance organisée* » peuvent être concernées.

En conséquence, l'article 18 élargit également la liste des menaces pouvant être détectées grâce aux traitements automatisés. Outre les ingérences étrangères, les menaces pour la défense nationale et les menaces terroristes, les traitements pourront détecter **les menaces relatives à la criminalité organisée et à la délinquance organisée portant sur des délits punis de dix ans d'emprisonnement** en ce qu'elles concernent :

– le trafic de stupéfiants ;

---

(1) Pour rappel, les finalités prévues sont celles prévues aux 1°, 2° et 4° de l'article L. 811-3 du CSI.

(2) Commission nationale de contrôle des techniques de renseignement, 8ème rapport d'activité, 2023.

(3) Ibid, p 101-102.

– le trafic d'armes et de produits explosifs ;

– l'importation et l'exportation de ces marchandises prohibées ;

– le blanchiment et le recel du produit, des revenus et des choses provenant de ces infractions.

Le périmètre retenu est très similaire à celui que prévoyait l'article 15 de la loi du 13 juin 2025 : celui-ci visait uniquement l'importation et l'exportation en bande organisée et ne précisait pas que le recel du produit de l'infraction était couvert, mais mentionnait explicitement le reste.

Dans son avis sur le présent projet de loi, le Conseil d'État souligne que « *les nouvelles finalités décrites* […] *sont définies de manière suffisamment précise* […] *pour permettre un contrôle de la proportionnalité des atteintes aux droits et libertés mises en cause* ». Il précise également que l'utilisation massive de données personnelles par le traitement « *résulte de la technique elle-même et non du nombre de finalités qui lui sont assignées* ». Il conclut donc que l'extension à de nouvelles finalités ne présente pas de difficulté d'ordre constitutionnelle (1).

● La réintégration des URL dans les données pouvant être utilisées par les algorithmes

Est reprise la garantie déjà existante selon laquelle les traitements automatisés doivent utiliser exclusivement les informations ou documents mentionnés à l'article L. 851-1 du CSI.

Le texte précise également que les traitements peuvent utiliser les adresses complètes de ressources utilisées sur internet, **lorsqu'elles sont nécessaires pour détecter des connexions susceptibles de révéler une ingérence ou une menace**.

Selon l'étude d'impact, le choix du Gouvernement de réintégrer les URL s'explique car cela constitue « *la seule technique de renseignement domestique visant à permettre la détection de nouvelles menaces* » et répond donc à un besoin essentiel en permettant de détecter précocement les menaces issues d'auteurs qui ne sont pas encore connus des services de renseignement (2).

● La procédure de délivrance de l'autorisation de recours aux traitements

L'article 18 prévoit des spécificités à la procédure de délivrance de l'autorisation pour permettre à la CNCTR de mieux contrôler les demandes de recours aux traitements automatisés.

---

(1) Avis du Conseil d'État sur un projet de loi actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, séance du 25 mars 2025, n° 410563, point 44.

(2) Étude d'impact du présent projet de loi, p 267.

Alors qu'elle doit normalement rendre son avis dans un délai compris entre vingt-quatre et soixante-douze heures (conformément à l'article L. 821-3), le IV du nouvel article L. 851-3 prévoit que pour la première demande d'autorisation relative à un traitement automatisé, la commission peut par dérogation rendre son avis dans un délai de trente jours. Il est également précisé que c'est la formation plénière de la CNCTR qui examine la demande.

Pour les demandes de renouvellement d'autorisation relative à des traitements automatisées, la commission dispose de soixante-douze heures pour rendre son avis.

À l'inverse, au VII de l'article L. 851-3, l'article 18 conserve, s'agissant de la durée de validité d'une première autorisation de mise en œuvre des traitements, celle de deux mois qui existe déjà à cet article.

L'article 18 introduit par ailleurs des garanties spécifiques lorsque les traitements incluent les adresses complètes de ressources utilisées sur Internet.

Au préalable, ces traitements ne peuvent uniquement utiliser des URL que lorsque celles-ci sont nécessaires, conformément au II de l'article L. 851-3 dans la nouvelle rédaction proposée par le présent texte.

Ensuite, si ces traitements utilisent des URL, alors le III de l'article L. 851-3 dans sa nouvelle version circonscrit le périmètre des URL qui peuvent être retenues dans les paramètres des traitements. Celles-ci doivent :

– soit diriger vers des ressources dont l'objet est en rapport avec les ingérences ou les menaces mentionnées au I (défense nationale, terrorisme, criminalité organisée), par exemple les pages du site internet d'un groupe terroriste [(1)] ;

– soit diriger vers des ressources dont il existe des raisons sérieuses de penser qu'elles sont utilisées à des fins d'ingérence ou de menaces mentionnées au I, par exemple l'URL d'un groupe de discussion dont il est établi qu'il est utilisé par des terroristes [(2)] ;

– soit présenter des caractéristiques techniques de nature à révéler des ingérences ou des menaces mentionnées au I.

À cela s'ajoute un délai spécifique pour la CNCTR : celle-ci dispose de 45 jours pour rendre son avis sur une première demande d'autorisation lorsque celle-ci inclut des URL, contre 30 jours pour les traitements automatisés n'incluant pas d'URL et vingt-quatre à soixante-douze heures pour les autres techniques de recueil de renseignement.

---

(1) Exemple mentionné à l'article 268 de l'étude d'impact annexée au présent projet de loi.

(2) Exemple également mentionné par l'étude d'impact, p 269.

Autre garantie : si la commission n'a pas transmis son avis dans le délai imparti, alors le Conseil d'État doit être saisi et avoir statué avant que la décision du Premier ministre ne soit exécutée. Pour les autres techniques de renseignement, un avis non transmis est réputé rendu (article L. 821-3).

● L'encadrement du recours aux traitements une fois l'autorisation délivrée

Le V de l'article L. 851-3 dans la version proposée par le présent projet de loi reprend les garanties prévues par l'article dans sa version actuelle, une fois que l'autorisation de recourir aux traitements a été délivrée :

– l'exécution des traitements ne doit pas permettre de recueillir des données autres que celles prévues par les paramètres, ni d'identifier les personnes auxquelles ces données se rapportent (à l'exception des données ayant déclenché une alerte) ;

– les données non détectées par les traitements comme susceptibles de révéler une ingérence ou une menace sont immédiatement détruites ;

– la CNCTR dispose d'un accès permanent, complet et direct aux traitements ainsi qu'aux données utilisées, et est informée de toute modification apportée aux traitements et paramètres.

Le V précise que seul un service du Premier ministre est habilité à exécuter lesdits traitements : comme actuellement, c'est le groupement interministériel de contrôle qui en sera chargé.

Le V introduit également une précision absente de la procédure actuelle, selon laquelle aucun service spécialisé de renseignement ne peut accéder aux données utilisées par les traitements (à l'exception de celles ayant déclenché une alerte).

● Procédure en cas d'alerte

Si la mise en œuvre des traitements automatisés a permis la détection de données susceptibles de révéler l'existence d'une ingérence ou d'une menace, alors le Premier ministre peut autoriser l'identification de la personne concernée et le recueil des données afférentes, après avoir recueilli l'avis de la CNCTR. Les données doivent être exploitées dans un délai de soixante jours à compter de leur recueil et sont détruites à l'issue de ce délai.

Cette procédure en cas d'alerte est identique à celle prévue par l'article L. 851-3 dans sa rédaction actuelle. L'article 18 y ajoute néanmoins deux éléments qui n'y figurent pas :

– la précision selon laquelle seul un service du Premier ministre est habilité à exécuter les opérations d'identification et de recueil des données ;

– l'accès permanent, complet direct et immédiat de la CNCTR aux données recueillies qui sont susceptibles de révéler l'existence d'une ingérence ou d'une menace.

● Renouvellement de l'autorisation

Le VII prévoit que toute demande de renouvellement doit se faire dans les conditions prévues par le chapitre Ier du titre II du livre VIII. S'agissant des éléments que doit préciser la demande de renouvellement, il reprend ceux prévus à l'actuel article L. 851-3, en prévoyant que celle-ci doit comporter :

– un relevé du nombre de détections par le traitement automatisé ;

– et une analyse de la pertinence de ces détections.

Il ajoute une garantie supplémentaire lorsque le traitement utilise des URL : la demande doit également comporter une actualisation de la nécessité et de la proportionnalité du recours à ces adresses.

Le VIII de l'article L. 851-3 dans la version proposée par le présent projet de loi reprend la formulation prévue au III de l'article L. 851-3 dans sa version actuelle s'agissant des modalités de réquisition des opérateurs.

Le IX de l'article L. 851-3 dans la version proposée par le présent projet de loi écarte la possibilité d'utiliser la procédure d'urgence prévue à la dernière phrase du deuxième alinéa de l'article L. 821-1 du CSI, qui permet une mise en œuvre immédiate, sans attendre la décision du Conseil d'État. L'impossibilité d'utiliser cette procédure d'urgence est déjà prévue au V de l'article L. 851-3 dans sa version actuelle.

● L'avis du Conseil d'État sur la réintroduction du traitement des URL

Le Conseil souligne que des garanties supplémentaires sont introduites par le présent projet de loi :

– des garanties spécifiques au traitement des URL qui conduisent à limiter le champ des URL recueillies par le traitement à ce qui est strictement nécessaire (1) ;

– des garanties procédurales nouvelles, notamment sur les délais dans lesquels la CNCTR est appelée à se prononcer.

Il émet cependant deux réserves : il estime nécessaire que la CNCTR puisse avoir 30 jours pour examiner la première demande d'autorisation d'un traitement automatisé et 45 jours lorsque des URL sont incluses. Cette recommandation a été prise en compte puisque l'article 18 prévoit justement ces deux délais. Le

(1) Au point 45 de son avis, le Conseil d'État rappelle ainsi que l'utilisation des URL devra être subordonnée à une exigence de nécessité et que le champ des URL retenues dans les paramètres de conception est explicitement restreint par le projet de loi.

Gouvernement n'a cependant pas souhaité que le délai d'examen par la CNCTR d'une demande de renouvellement de l'autorisation d'un traitement soit porté à 7 jours, comme le souhaitait le Conseil d'État.

L'avis préconise également que les premières demandes d'autorisation soient examinées en formation plénière en formation plénière de la CNCTR, qu'elles incluent des URL ou non. Cette précision est bien prévue par l'article 18.

B. LA RESTRICTION DU DISPOSITIF À LA FINALITÉ DE PRÉVENTION DU TERRORISME À COMPTER DU 1ER JUILLET 2029

Le II du présent article 18 prévoit qu'à compter du 1er juillet 2029, les traitements automatisés ne puissent uniquement être mis en œuvre que pour la finalité de prévention du terrorisme en procédant aux coordinations nécessaires à l'article L. 851-3.

Le IV du présent article 18 prévoit la remise par le Gouvernement au Parlement de deux rapports :

– le premier sur l'application du présent article s'agissant des finalités de prévention des ingérences étrangères et des menaces pour la défense nationale, avec une temporalité très rapprochée, la remise étant prévue au 1er juillet 2026 ;

– le deuxième sur l'application du présent article s'agissant de l'extension aux nouvelles finalités prévue par la loi du 24 juillet 2024 et par l'actuel projet de loi, avant le 1er juillet 2029.

Le III du présent article abroge, en conséquence, le II et le III de l'article 6 et le III de l'article 9 de la loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France. Ces dispositions n'ont plus lieu d'être puisque l'article 18 fixe une nouvelle borne temporelle et prévoit la remise des rapports qui étaient prévus à l'article 6.

*

* *

Article 19

Procédure d'autorisation préalable à l'exercice d'une activité pour le compte d'une entité étrangère

➢ **Résumé du dispositif et effets principaux**

L'article 19 du projet de loi initial instaure une procédure d'autorisation préalable pour toute personne exerçant au sein de certaines zones à régime restrictif et souhaitant exercer une activité lucrative pour le compte d'une entité étrangère.

➢ **Dernière modification législative intervenue**

L'article 42 de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense a créé, aux articles L. 4122-11 et suivants du code de la défense, une procédure de déclaration préalable auprès du ministre pour les militaires et certains agents civils ayant occupé des fonctions sensibles ou très techniques et qui souhaitent travailler pour un État étranger ou une entreprise étrangère.

I. LE DROIT EXISTANT

● Le potentiel scientifique et technique est défini comme « *l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée et au développement technologique* » (1). Il constitue l'un des intérêts fondamentaux de la Nation, conformément à l'article 410-1 du code pénal.

Il revient à l'État d'identifier et de protéger les activités scientifiques et techniques les plus sensibles. C'est dans cette perspective que s'inscrit la politique publique de protection du potentiel scientifique et technique de la Nation (PPST), qui vise à « *limiter la captation d'informations dans le domaine scientifique et technique pouvant affecter les intérêts de la Nation* » (2).

La PPST s'organise autour de quatre risques différents :

– le risque 1 (R1), « intérêts économiques de la Nation » : il vise les atteintes au potentiel scientifique et technique susceptibles de porter préjudice aux intérêts et à la compétitivité économiques et scientifiques de la France ;

– le risque 2 (R2), « arsenal militaire » : il vise le détournement du potentiel scientifique et technique susceptible de renforcer les capacités militaires conventionnelles d'un autre pays ou d'affaiblir les capacités de défense françaises ;

---

(1) Instruction interministérielle relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation datée du 28 avril 2025, NOR : PRMD2505309C.

(2) Présentation du dispositif de PPST sur le site de l'Agence nationale de la sécurité des systèmes d'information, accessible ici : https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/protection-information-sensible-diffusion-restreinte/protection-du-potentiel-scientifique-et-technique-de-la-nation-ppst/.

– le risque 3 (R3), « prolifération » : il concerne le détournement de savoirs et savoir-faire susceptibles de contribuer à la prolifération des armes de destruction massive et de leurs vecteurs, dans les domaines nucléaire, balistique, chimique ou biologique ;

– le risque 4 (R4), « terrorisme » : il concerne le détournement de savoir et de savoir-faire susceptibles d'être utilisés pour commettre des actes terroristes, sur le territoire National ou à l'étranger, ainsi que le risque radiologique.

Les secteurs scientifiques et techniques les plus susceptibles d'être concernés par ces quatre risques sont définis en annexe I de l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la Nation, étant identifiés comme des secteurs protégés. Parmi ces secteurs, certains sont identifiés comme étant particulièrement à risque de détournement à des fins de terrorisme ou de prolifération des armes de destruction massive et de leurs vecteurs : ce sont des spécialités dites « sensibles » qui sont listées par un arrêté classifié du Premier ministre, non publié au Journal officiel.

Dès lors qu'une unité de recherche ou de développement relève d'un ou plusieurs secteurs protégés, son besoin de protection est évalué par le ministre compétent. Comme le rappelle l'instruction interministérielle datée du 28 avril 2025, le ministre compétent pour déterminer le besoin de protection est celui qui est « *le plus à même d'apprécier la sensibilité des activités en cause* » (1), que ce soit par son lien de tutelle, par son expertise sectorielle ou par un lien contractuel avec l'unité concernée.

Si le besoin de protection est avéré, alors cette unité est considérée comme une « unité protégée ».

L'un des axes de cette politique de protection du potentiel scientifique et technique est la création de zones à régime restrictif (ZRR) au sein des unités protégées identifiées comme étant les plus sensibles. Ces zones sont définies à l'article R. 413-5-1 du code pénal. Des mesures de protection particulières y sont appliquées en raison des risques élevés de détournement ou de captation des informations, données, technologies et matériels qui s'y trouvent. Ainsi, l'accès et la circulation des personnes y sont strictement régulés : tout accès doit faire l'objet d'une autorisation de la part du chef de service, d'établissement ou d'entreprise. Dans certains cas, cette autorisation ne peut intervenir qu'après avis favorable du ministre ayant déterminé le besoin de protection (2). Le périmètre d'une ZRR ne recouvre pas nécessairement celui de l'unité protégée.

L'intrusion sans autorisation dans une ZRR est ainsi passible de six mois d'emprisonnement et de 7 500 euros d'amende, conformément à l'article L. 413-7 du code pénal.

---

(1) Instruction interministérielle précitée, p 10.

(2) Voir le II de l'article R. 413-5-1 du code pénal.

● Dans un contexte de résurgence des tensions internationales, les tentatives étrangères pour capter le potentiel scientifique et technique de la France se multiplient. L'un des moyens utilisés est le débauchage des personnels ayant des savoir-faire reconnus et des compétences techniques précieuses.

Ce constat a justifié l'introduction d'un dispositif visant à faire obstacle au départ de militaires vers des structures étrangères par l'article 42 de la loi du 1er août 2023. L'étude d'impact faisait ainsi état de la nécessité de créer un dispositif pour prévenir le risque des militaires soient recrutés par une puissance étrangère pour l'exploitation de leur savoir-faire opérationnel. Elle mentionnait qu'une dizaine de pilotes français avaient ainsi été approchés par des États tiers au cours des dernières années (1).

L'article 42 a inséré au sein du code de la défense trois articles L. 4122-11 à L. 4122-13 qui ont créé une procédure de déclaration préalable pour tout militaire qui exerce des fonctions présentant une sensibilité particulière ou requérant des compétences techniques spécialisées et qui souhaite exercer une activité lucrative dans le domaine de la défense ou de la sécurité au bénéfice d'une entité étrangère.

Les domaines d'activité concernés sont énumérés à l'article R. 4122-33-1 du code de la défense. La même obligation s'applique dans un délai de dix ans suivant la cessation des fonctions.

La déclaration est faite auprès du ministre de la Défense, qui peut s'opposer à l'exercice de l'activité envisagée. Des sanctions administratives et pénales sont prévues en cas de méconnaissance de l'obligation de déclaration ou de la décision d'opposition (2). Conformément à l'article L. 4122-13, certains agents civils de l'État et de ses établissements publics sont également concernés.

Sollicitée par la commission de la Défense de l'Assemblée nationale dans le cadre d'une mission *flash* sur l'application de la loi de programmation militaire du 1er août 2023, la direction du renseignement et de la sécurité de la défense (DRSD) indiquait avoir été saisie uniquement de quatre demandes d'avis depuis l'entrée en vigueur du dispositif (3).

Si le caractère dissuasif du dispositif est mis en avant par le Gouvernement dans l'étude d'impact, celui-ci insiste sur son périmètre réduit, puisqu'en l'état, il

---

(1) Étude d'impact du projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, datée du 5 avril 2023, p 146.

(2) Outre la nullité du contrat de plein droit, l'autorité administrative peut prononcer des retenues sur la pension de la personne concernée (jusqu'à 50 % de son montant pour la durée d'exercice de l'activité illicite, dans la limite de dix ans) et le retrait des décorations. La personne s'expose également à une sanction pénale pouvant aller jusqu'à cinq ans d'emprisonnement et 75 000 euros d'amende.

(3) Rapport d'information par la commission de la défense nationale et des forces armées en conclusion des travaux d'une mission d'information flash sur l'application de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, n° 1890, déposé le mardi 30 septembre 2025, présenté par M. Jean-Michel Jacques, M. Yannick Chenevard et M. Sébastien Saint-Pasteur, députés.

concerne uniquement des militaires et certaines catégories limitées d'agents civils de la direction générale de l'armement et de la direction des applications militaires du Commissariat à l'énergie atomique.

S'agissant des autres personnels, les outils juridiques déjà existants, comme le contrôle déontologique auxquels sont soumis les agents et les dispositifs visant à encadrer la cessation temporaire d'activité ou l'exercice d'une activité accessoire ne suffisent ainsi pas, selon l'étude d'impact, à protéger les compétences critiques stratégiques. Elle souligne ainsi l'absence de motif d'opposition aux demandes de cessation temporaire ou de cumul d'activité qui serait fondé sur la protection des intérêts fondamentaux de la Nation.

Suivant la même logique que pour l'article 17 qui instaure une procédure d'autorisation préalable à la publication pour les agents de services de renseignement, l'étude d'impact souligne que les sanctions pénales n'interviennent qu'une fois que le dommage s'est matérialisé et souligne la nécessité de créer un dispositif préventif.

II. LES DISPOSITIONS DU PROJET DE LOI INITIAL

L'article crée une procédure d'autorisation préalable similaire à celle déjà existante pour les militaires et anciens militaires, sans la codifier.

● Les personnes concernées par ce dispositif

Le dispositif s'applique aux personnes qui réunissent deux conditions :

– exercer au sein d'une ZRR mise en place pour empêcher le détournement d'éléments scientifiques ou techniques à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs (1) ;

– disposer d'une expérience significative et d'un savoir-faire technique ou de connaissances présentant un niveau d'importance critique.

Selon l'étude d'impact, la notion d'expérience significative « *s'entend notamment comme l'exercice effectif de responsabilités scientifiques ou techniques dans des activités de recherche, de développement, d'essais ou d'expertise portant sur des technologies, systèmes ou procédés sensibles* » (2).

Ce dispositif sera donc applicable aux agents publics mais également aux personnels de droit privé. En sont exclus :

---

(1) Soient les risques 3 et 4 dans la nomenclature présentée supra.

(2) Étude d'impact du présent projet de loi, p 294.

– les agents qui font déjà l'objet d'un dispositif équivalent, soit les militaires et agents civils mentionnés aux articles L. 4122-11 et L. 4122-13 du code de la défense ;

– les personnes ayant accès aux locaux et terrains dans le cadre d'un contrat doctoral, d'un contrat postdoctoral ou d'un contrat d'attaché temporaire d'enseignement et de recherche. Les chercheurs en début de carrière ne sont donc pas concernés. Selon l'étude d'impact, il serait disproportionné d'inclure ces personnes alors même que « *les tentatives de débauchages concernent en priorité des chercheurs expérimentés* » (1).

● Responsabilité de l'employeur pour élaborer la liste des personnes concernées

Le II précise que c'est l'employeur qui doit identifier, à titre préliminaire, les personnes qui peuvent relever du dispositif d'autorisation prévu au I, et transmettre une liste au ministre concerné (2). Celui-ci n'est néanmoins pas tenu par la proposition de l'employeur et c'est à lui que revient la responsabilité d'identifier définitivement les personnes concernées par le dispositif. Le défaut de transmission de cette liste par l'employeur est passible d'une amende de 45 000 euros.

Une fois identifiées, les personnes concernées seront informées individuellement. Cette obligation d'information individuelle découle à la fois de la nécessité de ne pas rendre publique l'identité des personnes mais également du fait que toutes n'ont pas forcément conscience d'exercer au sein d'une ZRR.

L'étude d'impact précise que seront concernées et devront donc être informées les personnes qui ont cessé leur activité depuis moins de cinq ans.

● Champ des activités nécessitant une déclaration

Le III délimite le périmètre des activités dont l'exercice doit être préalablement autorisé. Celle-ci répond à trois critères : elle doit être lucrative, dans certains domaines définis, et être au bénéfice d'une entité étrangère.

Les domaines concernés sont ceux qui relèvent d'un secteur scientifique et technique protégé, c'est-à-dire l'un des secteurs mentionnés à l'annexe I de l'arrêté du 3 juillet 2012 du Premier ministre relatif à la protection de la PPST.

Les entités étrangères visées sont, plus précisément :

– un État étranger ;

---

(1) Étude d'impact du présent projet de loi, p 297.

(2) Le ministre concerné est celui qui évalue le besoin de protection au titre de la PPST, c'est-à-dire, en pratique, le ministre qui dispose d'un lien de tutelle, d'une expertise sectorielle, ou d'un lien contractuel avec l'entreprise, l'organisme ou le laboratoire français concerné. Comme l'indique l'étude d'impact, l'option selon laquelle le ministre de la défense aurait centralisé le traitement des déclarations a été écartée, pour garantir une plus grande efficacité du dispositif.

– une collectivité étrangère ;

– une entreprise ou une organisation ayant son siège en dehors du territoire national ou sous contrôle étranger.

Le VIII de l'article 19 précise que ces dispositions ne s'appliquent pas :

– lorsque l'activité est réalisée au bénéfice direct d'un État ou d'une collectivité situés au sein d'États membres de l'Union européenne ou de l'Association européenne de libre-échange, ou d'une entreprise ou d'une organisation ayant son siège dans l'un de ces États-membres, sous réserve qu'elle ne soit pas sous le contrôle d'une personne étrangère à l'un de ces États ;

– lorsque l'activité envisagée intervient dans le cadre d'un détachement auprès d'une organisation internationale à laquelle la France est partie.

● Procédure d'autorisation préalable à l'exercice d'une activité lucrative au bénéfice d'une entité étrangère, dans certains domaines définis en cas de cessation définitive d'activité professionnelle

Dès lors qu'une personne mentionnée au I souhaite exercer une activité relevant du champ défini au III, elle doit le déclarer auprès du ministre chargé des éléments essentiels du potentiel scientifique et technique à protéger. Cette obligation de déclaration s'applique pendant une période de cinq ans à compter de la cessation des fonctions. Cette durée est considérée comme suffisante au regard notamment « *du caractère rapidement obsolète des compétences critiques de niche susceptibles d'être détournées* » [(1)].

Le ministre saisi de la déclaration peut s'opposer à l'exercice de l'activité envisagée lorsqu'il estime que deux conditions cumulatives sont remplies :

– cet exercice comporte le risque sérieux d'une divulgation par l'intéressé de savoir-faire ou de connaissances dont il dispose et susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs ;

– cette divulgation est de nature à porter atteinte aux intérêts fondamentaux de la Nation.

Pour instruire le bien-fondé de la demande préalable, une enquête administrative peut être réalisée (V).

La personne concernée doit être en mesure de présenter des observations écrites et, à sa demande, orales avant que la décision d'opposition ne lui soit notifiée.

(1) Étude d'impact du présent projet de loi, p 300.

● Cas particulier des demandes d'exercice d'activité à titre accessoire et de cessation temporaire d'activité

Le IV ajoute un motif de refus d'exercice d'activité à titre accessoire ou de cessation temporaire d'activité plutôt que créer une procédure *ad hoc* pour les agents concernés.

Ainsi, si un agent public appartenant à la catégorie établie par le I souhaite exercer une activité mentionnée au III à titre accessoire, ou une activité soumise à autorisation de l'autorité hiérarchique, alors celle-ci se prononce après avis conforme du ministre, qui peut formuler un avis défavorable pour les mêmes motifs que ceux énoncés au III.

Si un agent public souhaite cesser temporairement ses fonctions pour exercer l'une des activités mentionnées au III, la même procédure s'applique (avis conforme du ministre). Pendant cette période de cessation temporaire d'activité, l'agent reste soumis aux dispositions du présent article.

L'instruction de ces demandes peut donner lieu à la réalisation d'une enquête administrative (V).

● Sanctions administratives et pénales

En cas de méconnaissance de l'obligation de déclaration ou de la décision d'opposition du ministre en vue d'une cessation définitive de fonctions, plusieurs sanctions s'appliquent :

– le contrat conclu en vue de l'exercice de l'activité est nul de plein droit (VI) ;

– l'autorité administrative peut prononcer des retenues sur pension, dans la limite de 25 % du montant de celle-ci, pour la durée de l'exercice de l'activité illicite, dans la limite de cinq ans (VI) ;

– elle peut également prononcer le retrait des décorations obtenues par la personne (VI) ;

– en matière pénale, une telle méconnaissance est passible de trois ans d'emprisonnement et de 45 000 euros d'amende (VII).

Toute méconnaissance de la décision de refus de l'autorité hiérarchique d'exercer une activité à titre accessoire ou dans le cadre d'une cessation temporaire de fonctions est également passible de trois ans d'emprisonnement et de 45 000 euros d'amende (VII).

Ces sanctions sont du même ordre que celles prévues pour les militaires et les agents civils qui méconnaissent leurs obligations de déclaration ou la décision

d’opposition du ministère de la Défense, bien que fixées à des seuils légèrement inférieurs.

L’entrée en vigueur de l’article est fixée au 1er janvier 2027 (X).

Le Conseil d’État, dans son avis sur le projet de loi, souligne que ce contrôle exercé par l’administration « *répond à de fortes considérations d’intérêt général, en lien avec les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* ». Il estime qu’une telle mesure apparaît proportionnée aux buts poursuivis, dans la mesure où :

– le contrôle est limité à une période de cinq ans après la cessation des fonctions ;

– le champ du contrôle est précisément délimité :

– les activités exercées au bénéfice direct de certains États, entreprises ou organisations sont explicitement exclues du dispositif (1).

*

* *

(1) Avis du Conseil d’État sur le présent projet de loi précité, point 48.