N° 726

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 13 juin 2023

AVIS

PRÉSENTÉ

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la **programmation militaire** *pour les* **années 2024** *à* **2030** *et portant diverses dispositions intéressant la* **défense***,*

Par M. François-Noël BUFFET,

Sénateur

(1) Cette commission est composée de : M. François-Noël Buffet*, président ;* Mmes Catherine Di Folco, Marie-Pierre de La Gontrie, MM. Christophe-André Frassa, Jérôme Durain, Marc-Philippe Daubresse, Philippe Bonnecarrère, Mme Nathalie Goulet, M. Thani Mohamed Soilihi, Mmes Cécile Cukierman, Maryse Carrère, MM. Alain Marc, Guy Benarroche*, vice-présidents ;* M. André Reichardt, Mmes Laurence Harribey, Muriel Jourda, Agnès Canayer*, secrétaires ;* Mme Éliane Assassi, MM. Philippe Bas, Arnaud de Belenet, Mmes Nadine Bellurot, Catherine Belrhiti, Esther Benbassa, MM. François Bonhomme, Hussein Bourgi, Mme Valérie Boyer, M. Mathieu Darnaud, Mmes Françoise Dumont, Jacqueline Eustache-Brinio, M. Pierre Frogier, Mme Françoise Gatel, MM. Loïc Hervé, Patrick Kanner, Éric Kerrouche, Jean-Yves Leconte, Henri Leroy, Stéphane Le Rudulier, Mme Brigitte Lherbier, MM. Didier Marie, Hervé Marseille, Mme Marie Mercier, MM. Alain Richard, Jean-Yves Roux, Jean-Pierre Sueur, Mme Lana Tetuanui, M. Dominique Théophile, Mmes Claudine Thomas, Dominique Vérien, M. Dany Wattebled.

Voir les numéros :

Assemblée nationale (**16**ème législ.) : **1033**, **1234** rect. et T.A. **127**

Sénat : **712** (2022-2023)

SOMMAIRE

Pages

L'ESSENTIEL

Réunie le 13 juin 2023, la commission des lois a donné, sur le rapport de François-Noël Buffet, un avis favorable à l'adoption du projet de loi n° 712 relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.

La commission a souscrit aux évolutions proposées tant en matière de renseignement qu'en matière de sécurité des systèmes d'information dans un contexte budgétaire favorable aux recrutements et au développement des missions des services de renseignement.

Par ses amendements, elle s'est efforcée de remédier à certains manques et de sécuriser juridiquement les dispositifs proposés, potentiellement attentatoires aux libertés. Elle a adopté à cette fin des amendements aux articles 20, 27, 32, 33, 34 et 35 ainsi qu'un amendement portant sur le rapport annexé et que trois amendements portant articles additionnels relatifs aux pouvoirs de la délégation parlementaire au renseignement et de la commission nationale de contrôle des techniques de renseignement.

I. PRENDRE EN COMPTE LES BESOINS DES SERVICES DE RENSEIGNEMENT ET DE LA SECURITÉ DES SYSTÈMES D'INFORMATION

A. DES DISPOSITIONS UTILES MAIS PONCTUELLES POUR L'ATTRACTIVITÉ ET L'EFFICACITÉ DES SERVICES RELEVANT DU MINISTÈRE DES ARMÉES

Les services de renseignement font actuellement face à plusieurs enjeux dont le besoin de recrutements durables sinon pérennes et la nécessité d'investir dans des moyens ambitieux pour faire face aux nouveaux défis technologiques. Sur ces deux points, le projet de loi apporte aux services relevant du ministère des armées (la direction générale de la sécurité extérieure (DGSE), la direction du renseignement et de la sécurité de la défense (DRSD) et la direction du renseignement militaire (DRM) des moyens budgétaires sur la période de programmation qui paraissent à la hauteur des besoins.

La commission approuve cet engagement. Elle soutient également les mesures susceptibles de permettre aux services d'assurer plus efficacement leurs missions et de mieux protéger leurs agents. L'**article 19** autorise ainsi les services en charge des enquêtes administratives à consulter le bulletin n° 2 du casier judiciaire afin de mieux mesurer les vulnérabilités voire les risques posés par des personnes susceptibles d'être recrutées ou d'avoir accès à des lieux ou informations protégées. **L'article 21** permet la transmission d'informations figurant dans une procédure judiciaire ouverte pour crime contre l'humanité ou crime de guerre afin de renforcer la capacité des services à traiter l'évolution de la menace pesant sur la France et ses intérêts. L'**article 22** renforce la protection des anciens agents et membres des unités spéciales en leur garantissant l'anonymat lors de leur témoignage dans une procédure judiciaire, dans les mêmes conditions qu'à ceux actuellement en activité. Ces mesures, ponctuelles et techniques, viennent compléter celles déjà adoptées dans la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme et dans la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

L'**article 20** marque pour sa part la volonté de lutter contre les ingérences étrangères et de protéger les intérêts supérieurs de la France en mettant en place un mécanisme de contrôle des activités exercées par les militaires ou anciens militaires et par certains personnels civils ayant occupé des fonctions d'une sensibilité particulière et souhaitant, à l'issue de leurs fonctions, exercer une activité lucrative pour le compte d'un État étranger ou d'une entreprise étrangère ou sous contrôle étranger intervenant dans le domaine de la défense et de la sécurité.

B. DES POUVOIRS RENFORCÉS POUR L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

Les articles 32 à 35 renforcent la capacité de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à détecter, identifier et prévenir les attaques informatiques visant les systèmes d'information des autorités publiques, des opérateurs stratégiques et de leurs sous-traitants. En ce sens, **l'article 32** dote l'ANSSI de la possibilité d'enjoindre aux acteurs du numérique de filtrer ou de rediriger des noms de domaine utilisés par des cyberattaquants. **L'article 33** lui permet de recevoir communication des données de cache, non identifiantes, afin de mieux comprendre les modes opératoires des attaquants. Enfin, **l'article 35** étend à plusieurs titres les données pouvant être recueillies par l'ANSSI, rend obligatoire la mise en place de capacités de détection chez les opérateurs de communication électronique d'importance vitale, et supprime l'assermentation des agents de l'ANSSI habilités à analyser les données recueillies.

En outre, les dispositions prévoient de renforcer l'information des victimes des cyber-attaques. À cette fin, **l'article 34** oblige les éditeurs de logiciels à notifier à l'ANSSI et aux utilisateurs concernés les vulnérabilités significatives susceptibles de compromettre la sécurité de leurs produits, tandis que **l'article 35** élargit aux hébergeurs de données l'obligation de communiquer à l'ANSSI les informations concernant des utilisateurs ou détenteurs de systèmes d'informations vulnérables ou attaqués afin de les en informer.

C. DES POUVOIRS ETENDUS DANS LA LUTTE CONTRE LES DRONES MALVEILLANTS

L'article 27 du projet de loi vise à autoriser les services de l'État à utiliser divers moyens techniques pour neutraliser un drone qui présenterait une menace imminente pour l'ordre public, la défense et la sécurité nationales ou le service public de la justice. En élargissant le champ du dispositif « anti-brouillage », adopté dans le cadre de la loi du 30 juillet 2021 précitée, à tout type de dispositif pouvant aller jusqu'à la destruction du drone malveillant, il dote les services de l'État de la capacité de réagir sans délai face au survol d'une zone interdite (centrale nucléaire, établissement pénitentiaire, etc.) ou en cas de risque pour un évènement ou une manifestation sensible (G7, jeux Olympiques, *etc.*).

II. LA POSITION DE LA COMMISSION : FAIRE FACE AUX ENJEUX CONNUS EN MATIÈRE DE RENSEIGNEMENT ET SÉCURISER JURIDIQUEMENT LES DISPOSITIFS PROPOSÉS

A. UNE PRISE EN COMPTE INSUFFISANTE DES GARANTIES NÉCESSAIRES AU FONCTIONNEMENT DU RÉGIME LÉGAL DU RENSEIGNEMENT

1. Alerter sur la nécessité de réformer le cadre des échanges entre services français et étrangers sans attendre une éventuelle condamnation de la France par la Cour européenne des droits de l'homme

La commission déplore l'absence dans le projet de loi de mesure prévoyant la mise en conformité du cadre des échanges d'informations entre les services de renseignement français et étrangers. Les insuffisances du cadre actuel au regard des exigences découlant du respect de la Convention européenne des droits de l'homme sont connues depuis plusieurs années et la délégation parlementaire au renseignement a déploré la volonté de ne s'engager dans la mise en conformité du droit français que le plus tard possible, le cas échéant après une éventuelle condamnation de la France par la Cour européenne des droits de l'Homme.

La commission relève que cette mise en conformité a déjà été conduite par le Royaume-Uni sans entraver l'action de ses services de renseignement. Si, désireuse qu'une solution proportionnée et acceptable par tous puisse être trouvée, la commission, suivant la position du rapporteur, n'a pas souhaité proposer à ce stade de réforme du cadre légal, elle souhaite souligner qu'à défaut d'une initiative gouvernementale, un texte d'origine parlementaire deviendra nécessaire à brève échéance.

2. Maintenir l'équilibre entre les développements des moyens accordés aux services et ceux du contrôle

La commission a également souhaité que les prérogatives accordées aux services et l'évolution de leurs pratiques trouvent leur pendant nécessaire dans le renforcement des pouvoirs de contrôle de la délégation parlementaire au renseignement (DPR) et de la commission nationale de contrôle des techniques de renseignement (CNCTR). La commission des lois a accompagné, avec responsabilité, le développement des moyens techniques et légaux accordés aux services. Mais elle tient à rappeler que l'équilibre du dispositif et sa conformité au cadre tant constitutionnel qu'européen repose sur le développement parallèle des capacités de contrôle effectives. Ces mécanismes de contrôle reposent sur une délégation parlementaire commune aux deux assemblées, chargée de l'ensemble des questions relatives au renseignement, ainsi que sur la CNCTR, clef de voûte non seulement du contrôle des techniques du renseignement, mais également, depuis la loi du 30 juin 2021, de celui des échanges entre services.

À l'initiative du rapporteur, la commission a donc adopté quatre **amendements COM-127**, **COM-128**, **COM-129** et **COM-141** poursuivant les objectifs suivants :

- garantir, conformément à l'intention initiale de la loi du 30 juin 2021, que lorsque des sujets d'actualité concernant une action des services de renseignement revendiquée par le gouvernement font l'objet d'une publicité, ceux-ci pourront faire l'objet d'un suivi par la DPR ;

- renforcer les liens entre la DPR et la CNCTR en prévoyant la présentation à la délégation d'un bilan annuel des recommandations de la commission et son information sur les saisines du procureur de la République dans le cadre du dispositif de lanceur d'alerte ;

- permettre l'accès immédiat de la CNCTR aux éléments collectés par les services de renseignement lors de la mise en œuvre des techniques les plus intrusives afin de renforcer le contrôle du respect des autorisations accordées et la destruction des données ;

- supprimer, suivant la position constante du Sénat, la mention de la création d'une délégation au renseignement économique, qui aboutirait à un émiettement du contrôle en décalage avec les enjeux de la souveraineté nationale.

La commission a également adopté les **amendements COM-134**, **COM-136** et **COM-139** tendant à ce que la CNCTR puisse donner un avis avant la prise des décrets renforçant les pouvoirs de l'ANSSI. En effet, si l'ANSSI n'est pas un service de renseignement, ses liens avec ceux-ci sont étroits et la nature de son intervention appelle le regard particulièrement informé de la CNCTR sur les pratiques de ces services.

B. DES AJUSTEMENTS DESTINÉS À RENFORCER LE CARACTÈRE OPÉRATIONNEL ET LA SÉCURITÉ JURIDIQUE DES DISPOSITIFS PROPOSÉS

1. Des ajustements destinés à donner leur pleine effectivité aux dispositifs relatifs à l'ANSSI

Suivant l'avis de son rapporteur, la commission des lois a largement approuvé les articles 32 à 35 destinés à doter l'ANSSI de la capacité à mieux lutter contre les cyber-attaques et à mieux en informer les victimes, tels qu'ils ont été précisés par l'Assemblée nationale.

Aux articles 32, 33 et 35, elle a adopté les **amendements COM-131**, **COM-132**, **COM-133**, **COM-135** et **COM-138** visant à clarifier la rédaction retenue et à ajuster les dispositifs afin de les rendre pleinement opérationnels. À l'article 34, elle a adopté l'amendement COM-137 afin de prévoir que l'ensemble des utilisateurs d'un logiciel présentant une vulnérabilité critique devront être informés par l'éditeur de cette dernière, et pas uniquement les seuls utilisateurs professionnels comme l'ont prévu les députés de façon injustifiée. Elle a également adopté l'**amendement COM-140** visant à supprimer l'obligation d'assermentation, qu'elle estime superflue, pour les agents de l'ANSSI habilités à analyser les données recueillies.

2. Des précisions destinées à sécuriser les dispositifs « anti-drones » et « anti-ingérences »

Si la commission partage sans réserve les finalités poursuivies par l'article 27, qui vise à doter les services de l'État des moyens de parer sans délai à une menace représentée par un drone, elle relève que, dans certaines conditions, ces moyens pourront être mis en œuvre dans des zones où la circulation du drone est par principe légale. Elle a adopté l'**amendement COM-130** visant à renvoyer au décret au Conseil d'État la définition des conditions dans lesquelles, en cas de menace imminente, les moyens de neutralisation seront mis en œuvre, dans le respect des principes et des finalités édictés par cet article.

Enfin, à l'article 20, qui vise à soumettre certains militaires et anciens militaires à déclarer au ministre de la défense leurs projets de reconversion professionnelle au service d'un État ou d'une société étrangère, la commission des lois a adopté l'**amendement COM-126** prévoyant que les conditions d'application du dispositif à certains civils relevant du ministère de la défense devront être précisées par décret en Conseil d'État.

*

* *

La commission a émis un avis favorable à l'adoption du projet de loi sous réserve des amendements qu'elle a adoptés.

EXAMEN DES ARTICLES

Article 19

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

L'article 19 propose de permettre aux services de renseignement en charge des enquêtes administratives de consulter le bulletin n° 2 du casier judiciaire.

La commission a émis un avis favorable à l'adoption de cet article sans modification.

1. L'enquête administrative est la première et la plus importante phase de maitrise des risques

Les enquêtes administratives, anciennes enquêtes de moralité, sont une pratique ancienne qui recouvre, historiquement et souvent conjointement, deux finalités.

La première est l'enjeu de réputation. La nécessité de garantir les « bonnes vie et mœurs » du futur conjoint d'une personne investie d'une responsabilité publique fondait notamment l'obligation d'obtenir une autorisation préalable du ministre pour le mariage des militaires[1]. Cette autorisation, dont le champ s'est progressivement réduit, a finalement disparu du statut général des militaires en 2005. La seconde, qui s'est au contraire plutôt développée, est liée à la prévention des risques en matière de sécurité, que ce soit la sécurité nationale ou celle des personnes.

Les modalités et le périmètre de ces enquêtes ont été redéfinis au début des années 2000. La loi du 18 mars 2003 pour la sécurité intérieure[2] a autorisé (article 21) la création de fichiers automatisés de traitement des antécédents judiciaires et permis (article 25) leur consultation dans le cadre des *« décisions administratives de recrutement, d'affectation, 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'État, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées*

[1] *La loi n° 2005-270 du 24 mars 2005 portant statut général des militaires a supprimé cette obligation, qui ne demeure que pour les militaires servant à titre étranger pendant les cinq premières années de leur service actif.*

[2] *Loi n° 2003-239.*

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 (…) » pour « *vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées* ».

L'article 25 de la loi du 18 mars 2003 est désormais codifié à l'article L. 114-1 du code de la sécurité intérieure.

Le régime des fichiers d'antécédents judiciaires a été complété par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure[1], qui a inséré dans le code de procédure pénale une nouvelle section relative aux fichiers d'antécédents[2] et a renforcé les garanties qui leur sont liées[3], notamment celles offertes aux personnes en matière de rectification.

C'est sur le fondement de la loi du 14 mars 2011 qu'a été créé le traitement d'antécédents judiciaires[4] (TAJ), fusion de deux fichiers antérieurs. Ainsi que l'indique la Commission nationale de l'informatique et des libertés (Cnil)[5] :

« *Commun à la police et à la gendarmerie, le TAJ regroupe des informations concernant les personnes mises en cause ou victimes d'infractions pénales.*

« *Ce fichier comporte des données issues des comptes rendus d'enquête établis par les forces de police et de gendarmerie, pour des crimes (par ex. : homicide involontaire), délits (par ex. : dégradations de biens publics ou privés) ou certaines contraventions de 5e classe (par ex. : conduite sous l'empire d'un état alcoolique, détention de stupéfiants).*

« *Le TAJ est totalement différent du casier judiciaire national, qui comprend uniquement les faits ayant fait l'objet d'une condamnation pénale prononcée par les tribunaux français.* »

Les enquêtes administratives font l'objet du chapitre IV au sein du titre Ier du livre Ier de la partie réglementaire du code de la sécurité intérieure.

L'article L. 114-1 dispose que la liste des décisions pouvant donner lieu, en application de l'article L. 114-1, à des enquêtes administratives est fixée aux articles R. 114-2 à R. 114-5. L'article R. 114-2 vise notamment les autorisations et habilitations en lien avec l'accès à des informations couvertes par le secret de la défense nationale, mais aussi celles des personnels appelés à la mise en œuvre des missions de vérification de traitements de données à

---

[1] *Loi n° 2011-267.*
[2] *Articles 230-6 à 230-11 du code de procédure pénale.*
[3] *Comme l'indique le Conseil constitutionnel dans sa décision n° 2011-625 DC du 10 mars 2011.*
[4] *Décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires.*
[5] *https://www.cnil.fr/fr/les-refus-dembauche-un-poste-dagent-de-securite-la-suite-dune-enquete-administrative*

caractère personnel ou des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par la voie des communications électroniques. L'article R. 114-4 concerne les enquêtes préalables à l'octroi des autorisations d'accès aux lieux protégés. Enfin l'article R. 114-5 concerne les enquêtes relatives aux matériels, produits ou activités présentant un danger pour la sécurité publique, parmi lesquels la fabrication de matériels de guerre, d'armes et de munitions.

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[1].

Le rapport du Président Christian Cambon relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020[2] a dressé un bilan de l'activité de la DRSD, de la DGSI et de la DGSE en 2020.

---

[1] *Leur champ de compétence des différents services en matière d'habilitation diffère. Ainsi la DGSI, la DRSD et la DGSE ont parmi leurs attributions les enquêtes liées au secret de la défense nationale ; il convient d'y ajouter la direction du renseignement de la préfecture de police de Paris (DRPP), qui participe aux enquêtes administratives sur la base d'un protocole signé avec la DGSI.*
Le SNEAS pour sa part « réalise [...] des enquêtes administratives destinées à vérifier, au regard de l'objectif de prévention du terrorisme et des atteintes à la sécurité et à l'ordre public et à la sûreté de l'État, que le comportement de personnes physiques ou morales n'est pas incompatible avec l'autorisation d'accès à des sites sensibles ou l'exercice de missions ou fonctions sensibles dont elles sont titulaires ou auxquelles elles prétendent. » (décret n° 2017-668 du 27 avril 2017).

[2] *Rapport n° 506 du 11 juin 2020.*

	Structure interne chargée des enquêtes	Ressources humaines	Missions	Populations concernées	Statistiques
DRSD	Centre national des habilitations de défense (CNDH), rattaché à la sous-direction des centres nationaux d'expertises (SDCNE). *NB : les enquêtes sur le personnel du service sont assurées par le « bureau enquêtes personnel service » (BEPS), qui relève du CNDH. Les enquêtes sur le personnel du BEPS sont réalisées par un autre bureau du CNDH.*	*Effectifs* : 135 personnes au CNDH, dont 6 au BEPS habilités « secret défense » (un officier, deux sous-officiers, 2 personnels civils de catégorie B et un militaire du rang). *Ancienneté moyenne* : 4 ans à la DRSD, 2 ans au sein du BEPS. Les agents du BEPS sont choisis parmi les personnels affectés au CNHD.	Enquêtes administratives pour le renseignement et la sûreté (EARS) au profit de l'ensemble de la sphère défense.	- Ensemble de la sphère défense : forces armées, directions et services du ministère, base industrielle et technologique de défense, division des applications militaires du CEA (commissariat à l'énergie atomique et aux énergies alternatives) et entreprises contractant avec la DAM (direction des applications militaires ; - personnel de la DRSD (y compris les stagiaires).	- *Nombre d'organismes étatiques ou industriels concernés par les EARS* : 6 800. - *Nombre d'avis restrictifs* : 130 agents du service font l'objet d'un avis restrictif au niveau « secret défense ».

	Structure interne chargée des enquêtes	Ressources humaines	Missions	Populations concernées	Statistiques
DGSI	- Un service en charge des enquêtes ***** ; - *****.	*****	Enquêtes sur le personnel de la DGSI et contrôles après habilitation.	Personnel de la DGSI, y compris les enquêteurs.	- *Nombre d'enquêtes menées de janvier à novembre 2019* : 787, dont 564 pour des premières demandes (557 au niveau « secret défense » et 7 au niveau « très secret défense ») et 223 pour des renouvellements (222 au niveau « secret défense » et 1 au niveau « très secret défense »). *NB : quelque 1 000 enquêtes sont menées chaque année.* - *Résultat des enquêtes (de janvier à novembre 2019)* : 645 avis sans objection, 88 mises en éveil et 6 avis défavorables. - *Durée moyenne des enquêtes* : 3 mois ½.
	*****	*****	*****	*****	*****

	Structure interne chargée des enquêtes	Ressources humaines	Missions	Populations concernées	Statistiques
DGSE	Service de la sécurité du personnel, rattaché au service de sécurité, lui-même dirigé par le directeur de cabinet (n° 2 du service). *NB : une cellule est dédiée aux enquêtes sur la population des enquêteurs et de l'encadrement supérieur du service. En outre, un bureau est spécialement chargé des échanges avec les autres services de sécurité de la communauté du renseignement.*	*Effectifs* : 50 personnes environ. *Ancienneté moyenne* : 10 ans à la DGSE, 5 ans dans le poste.	- Enquêtes sur les candidats au recrutement ; - suivi du personnel de la DGSE ; - émission des avis de sécurité, des avis d'habilitation et des avis d'opportunité ; - conseil en matière de sécurité ; - liaison avec les services nationaux ; - octroi des badges d'accès ; - avis sur l'encadrement supérieur et les désignations à l'étranger ; - avis sur les congés à l'étranger ; - enquêtes sur les personnes morales de droit privé et les personnes physiques passant des marchés publics avec la DGSE ; - émission d'avis techniques d'aptitude à détenir des informations classifiées au sein des entreprises.	- Personnel de la DGSE ; - entreprises intervenant sur les sites de la DGSE ; - vacataires linguistes accédant au site. *NB : les agents des services du premier cercle placés pour emploi bénéficient d'un accès à la DGSE octroyé sur la base de leur habilitation de sécurité fournie par leur service d'origine. Cet accès est révocable sur décision du service de sécurité.*	- *Recrutements* : 1 831 enquêtes réalisées en 2018 (contre 1 677 en 2017). - *Suivi des agents* : 972 enquêtes réalisées en 2018 (contre 1 521 en 2017). - *Durée moyenne des enquêtes* : de 1 à 3 mois suivant la complexité du dossier.

Source : Délégation parlementaire au renseignement, 2020 à partir des réponses des services à son questionnaire écrit.

2. Le dispositif proposé par le projet de loi

Afin de renforcer l'efficacité des contrôles exercés lors des enquêtes administratives, le projet de loi propose de donner aux services en charge des enquêtes administratives, au-delà des fichiers auxquels ils peuvent avoir accès comme le TAJ, l'accès au bulletin n° 2 du casier judiciaire (B2), qui comporte l'ensemble des condamnations judiciaires et des sanctions administratives[1], sous réserve de certaines exceptions[2]. Plus restrictif que le TAJ, le B2 permettra de mieux cibler les enquêtes des services sur les vulnérabilités des personnes ou les risques qu'elles sont susceptibles de poser.

Cette disposition n'a pas fait l'objet de modifications autres que rédactionnelles à l'Assemblée nationale.

3. La position de la commission : une disposition utile dans un contexte de forte pression sur les services menant les enquêtes

La commission est particulièrement consciente de l'ampleur de travail demandé aux services en matière d'enquêtes administratives et particulièrement, dans le champ de la défense, à la DRSD. Elle note d'ailleurs que ces enquêtes sont conduites non seulement *a priori*, mais également, de plus en plus, en cours d'exercice pour permettre de détecter une éventuelle évolution des risques.

Le nombre de demandes et la nécessité de mener des investigations adéquates mobilisent fortement les personnels. L'importance d'un contrôle de l'accès aux données, aux technologies ou aux lieux les plus sensibles justifie pleinement ce travail qui, en matière de défense, aboutit dans environ 15 % des cas à des restrictions ou à des refus. Mais il a une conséquence sur la possibilité pour des personnels d'accéder aux fonctions pour lesquelles ils ont été pressentis ou recrutés, et les délais d'enquête avant avis par les services sont un facteur de découragement des candidats et potentiellement de blocage des recrutements.

---

[1] *S'agissant des sanctions administratives l'article 768 du code de procédure pénale dispose que figurent au casier judiciaire : 'Les décisions disciplinaires prononcées par l'autorité judiciaire ou par une autorité administrative lorsqu'elles entraînent ou édictent des incapacités ».*

[2] *Ces exceptions sont les suivantes : décisions à l'encontre des mineurs (par exemple travail d'intérêt général, placement dans un centre éducatif fermé), condamnations prononcées pour contraventions (par exemple amende), condamnations assorties d'une dispense de peine ou d'un ajournement du prononcé de la peine, décisions prononçant la déchéance de l'autorité parentale, condamnations avec sursis, lorsque le délai d'épreuve a pris fin sans exécution de la totalité de la peine (sauf si un suivi socio-judiciaire, une interdiction d'exercer une activité avec des mineurs ou une peine d'inéligibilité a été prononcée pour une durée plus longue que celle de la peine), arrêtés d'expulsion abrogés, compositions pénales, condamnations pour une infraction portant sur les prix ou la concurrence entre commerçants (sauf si le tribunal en a décidé autrement), condamnations désignées par une décision spécifique du tribunal lors du jugement, condamnations prononcées par une juridiction étrangère à l'égard d'un mineur, condamnations prononcées par une juridiction étrangère qui a expressément interdit toute utilisation en dehors du cadre d'une procédure pénale.*

Toute mesure permettant de mieux cibler les enquêtes est donc nécessaire. L'accès au B2 permet d'aller en ce sens et suscite donc l'adhésion de la commission.

La commission a donné un avis favorable à l'adoption de l'article 19 **sans modification.**

Article 20

Soumission de certains militaires et personnels civils disposant de compétences particulières dans le domaine de la défense à l'obligation de déclarer leurs projets de reconversion professionnelle au service d'un État étranger ou d'une entreprise ou organisation sous contrôle étranger au ministre de la défense

L'article 20 vise à soumettre certains militaires et personnels civils disposant de compétences particulières dans le domaine de la défense à l'obligation de déclarer leurs projets de reconversion au service d'un État étranger ou d'une entreprise ou organisation sous contrôle étranger au ministre de la défense, lequel pourra s'y opposer en cas de risque pour les intérêts fondamentaux de la Nation.

La commission a donné un avis favorable à l'adoption de cet article après avoir proposé de le préciser.

1. Un angle mort de la prévention des ingérences étrangères

De par ses caractéristiques opérationnelles, le service dans les forces armées implique la plupart du temps un temps de carrière court, qui soulève l'enjeu de la reconversion des personnels concernés à l'issue de cette période. À l'heure actuelle, la moyenne d'âge de la population militaire est de 33 ans, et plus de 25 000 militaires[1] quittent chaque année le ministère des armées pour poursuivre une activité professionnelle dans un autre secteur[2].

Or, certains de ces personnels ont acquis au cours de l'exercice de leurs fonctions un savoir-faire et des compétences très spécifiques que des puissances étrangères peuvent être tentées d'attirer. Il y a quelques mois, la presse s'est faite l'écho du recrutement d'anciens pilotes de chasse

[1] *Sur un peu plus de 200 000 personnels militaires relevant du ministère des Armées. Parmi eux, 16 % sont des officiers, 44 % des sous-officiers et 39 % des militaires de rang (source : bilan social du ministère des Armées, 2020).*

[2] *Source : ministère des armées.*

américains, britanniques et français par des sociétés contrôlées par la Chine. Mais, comme le souligne l'étude d'impact, certains emplois sensibles dans les domaines des sous-marins, de la cyberdéfense et du nucléaire sont également susceptibles d'intéresser des États étrangers souhaitant bénéficier de l'expertise et du savoir-faire des armées françaises.

Il n'existe pourtant à l'heure actuelle aucun dispositif permettant de prévenir ou de contrôler ce risque de « captation » de compétences par une puissance étrangère. S'il existe en effet depuis 1996 une commission de déontologie des militaires, celle-ci n'est compétente qu'en matière de prévention des conflits d'intérêts, qui relève d'une logique bien différente.

En outre, si les articles 411-5 à 411-8 du code pénal punissent de peines sévères le fait d'entretenir des intelligences avec une puissance étrangère ou de livrer des informations ou des documents au mépris des intérêts fondamentaux de la Nation, non seulement leur mise en œuvre suppose de pouvoir constituer des preuves, ce qui peut s'avérer en pratique impossible lorsque les nouvelles fonctions sont exercées en dehors du territoire national, mais surtout, à supposer que des éléments utiles aient pu être réunis, l'éventuel engagement de poursuites intervient par définition « trop tard », lorsque le transfert de compétences ou d'informations a déjà eu lieu.

Enfin, comme le souligne l'étude d'impact, l'emploi d'un ancien militaire français par un État étranger n'est pas systématiquement problématique, par exemple lorsque cet État est partie à une alliance militaire avec la France impliquant des coopérations techniques régulières dans le domaine considéré.

2. Le dispositif proposé par le projet de loi

Afin de remédier à ce vide juridique sans pour autant entraver les possibilités de reconversion d'anciens militaires dans des situations qui ne soulèveraient pas de difficulté au regard de la protection des intérêts fondamentaux de la Nation, l'article 20 du projet de loi crée **une obligation de déclaration** à destination des militaires ou anciens militaires ayant exercé certaines fonctions spécifiques au sein des armées (lesquelles seront précisées par voie réglementaire) et qui envisageraient d'exercer une activité dans le domaine de la défense ou de la sécurité au bénéfice d'un État étranger ou d'une entreprise ou d'une organisation sous contrôle étranger. Il complète à cette fin le chapitre du code de la défense consacré aux obligations et responsabilités des militaires de deux nouveaux articles L. 4122-11 et L. 4122-12.

Cette obligation s'appliquerait non seulement aux militaires concernés en exercice, mais également pendant **un délai de dix ans** après la cessation de leurs fonctions[1]. Les militaires soumis à cette obligation en seraient individuellement informés, dès lors que, pour des raisons de confidentialité, l'arrêté listant précisément les fonctions concernées ne ferait pas l'objet d'une publication.

Le ministre de la défense pourrait s'opposer à l'exercice de l'activité envisagée par l'intéressé s'il estime :

- d'une part, que cet exercice comporte le risque d'une divulgation par l'intéressé de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires auxquels il a eu accès dans le cadre de ses fonctions ;

- et, d'autre part, que cette divulgation est de nature à porter atteinte aux intérêts fondamentaux de la Nation.

En cas de méconnaissance de son obligation de déclaration, ou s'il passe outre l'opposition du ministre, le militaire concerné encourrait des **sanctions administratives et pénales** :

- au titre des sanctions administratives, des retenues sur pension et le retrait de décorations ;

- au titre des sanctions pénales, cinq ans d'emprisonnement et 75 000 euros d'amende ;

- en outre, le contrat conclu en vue de l'exercice de l'activité envisagée serait nul de plein droit – sanction en partie symbolique lorsque l'activité est exercée à l'étranger mais qui permettrait de faire obstacle à son exécution sur le territoire national.

L'ensemble de ce dispositif est inspiré d'une disposition applicable aux magistrats de l'ordre judiciaire (voir encadré).

---

[1] *L'étude d'impact précise à cet égard que les anciens militaires ayant déjà commencé, à 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, l'exercice d'un emploi dans le domaine de la défense et de la sécurité pour le compte d'un État 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.*

Article 9-2 de l'ordonnance n° 58-1270 du 22 décembre 1958 portant loi organique relative au statut de la magistrature

« Le magistrat en disponibilité ou qui demande à être placé dans cette position doit, lorsqu'il se propose d'exercer une activité privée, en informer préalablement le garde des sceaux, ministre de la justice. La même obligation s'applique pendant cinq ans au magistrat ayant définitivement cessé ses fonctions.

« Le garde des sceaux, ministre de la justice, peut s'opposer à l'exercice de cette activité lorsqu'il estime qu'elle est contraire à l'honneur ou à la probité, ou que, par sa nature ou ses conditions d'exercice, cette activité compromettrait le fonctionnement normal de la justice ou porterait le discrédit sur les fonctions de magistrat.

« En cas de violation d'une interdiction prévue au présent article, le magistrat mis en disponibilité est passible de sanctions disciplinaires dans les conditions prévues au chapitre VII. Le magistrat retraité peut faire l'objet, dans les formes prévues au chapitre VII, du retrait de son honorariat, et, le cas échéant, de retenues sur pension.

« Les modalités d'application du présent article sont déterminées par un décret en Conseil d'État ».

Le principe de ce dispositif a fait l'objet d'une approbation unanime lors de son examen par les députés, qui ont adopté plusieurs amendements destinés à le compléter. Outre des amendements rédactionnels, ils ont notamment :

- étendu le champ de l'obligation de déclaration aux activités exercées au bénéfice, non seulement d'États, d'entreprises et d'organisations étrangers, mais également de **collectivités territoriales étrangères** (amendement de Charles Sitzenstuhl adopté en séance publique) ;

- précisé que l'activité envisagée pourrait être exercée au profit de l'un de ces derniers **« *directement ou indirectement* »** (amendement d'Isabelle Santiago adopté en commission), afin de prévoir l'hypothèse d'une embauche par une société « fantôme », établie en France mais en réalité contrôlée par une puissance étrangère ;

- exempté du respect de l'obligation de déclaration les projets de reconversion au service d'une entreprise de la base industrielle et technologique de défense (BITD) française, titulaire de l'autorisation prévue à l'article L. 2332-1 du code de la défense (amendement de Jean-Michel Jacques, rapporteur, adopté en commission) ;

- enfin, **étendu à certains agents civils de l'État et de ses établissements publics participant au développement de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires le champ de cette obligation de déclaration** (amendement du Gouvernement adopté en séance publique).

3. La position de la commission : approuver ce dispositif qui vient combler un vide juridique préjudiciable aux intérêts de la France

L'article 20 du projet de loi vient combler un vide juridique particulièrement dommageable aux intérêts fondamentaux de la Nation. En instaurant un régime déclaratif ciblé sur les fonctions les plus stratégiques, il permet à la fois d'exercer un contrôle sur des tentatives de recrutement d'anciens militaires par des puissances étrangères sans pour autant entraver de façon excessive les possibilités de reconversion professionnelle des militaires français. Le dispositif proposé paraît à cet égard à la fois **adapté** et **proportionné** à l'objectif poursuivi de sauvegarde des intérêts fondamentaux de la Nation.

Lors de l'examen du projet de loi à l'Assemblée nationale, les députés ont souhaité que puissent également être inclus dans le champ de cette obligation certains **personnels civils du ministère des armées ayant accès à des informations stratégiques**. L'amendement du Gouvernement qu'ils ont adopté se borne ainsi, de façon non codifiée, à prévoir l'application des dispositions introduites par l'article 20 « *aux agents civils de l'État ou de ses établissements publics participant au développement de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires* », sans davantage de précisions, bien que l'exposé des motifs de l'amendement précise que les agents civils œuvrant au développement des capacités militaires au sein de la direction générale de l'armement ou de la division des applications militaires du Commissariat à l'énergie atomique et aux énergies alternatives pourront être concernés.

Toutefois, si cette rédaction permet d'appliquer aux intéressés l'ensemble du régime introduit par les nouveaux articles L. 4122-11 et L. 4122-12 du code de la défense (obligation de déclarer le projet d'activité au ministre de la défense en respectant un préavis, soumission à cette obligation pendant un délai de dix ans, précision des fonctions concernées par un décret en Conseil d'État et un arrêté non publié du ministre de la défense, information individuelle des personnes concernées), des précisions et adaptations seront probablement nécessaires en raison des différences de statut entre militaires, d'une part, et fonctionnaires et agents contractuels de droit public, d'autre part. Compte tenu de l'incidence de ces dispositions sur la situation des intéressés, la commission a souhaité qu'elles soient précisées **par un décret en Conseil d'État** et a proposé de compléter le texte en ce sens (**amendement n°COM-126** du rapporteur).

La commission a donné un avis favorable à l'adoption de l'article 20 **ainsi modifié.**

Article 21

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

L'article 21 tend à compléter les possibilités d'échange d'informations entre la justice et les services de renseignement en autorisant le parquet anti-terroriste à leur transmettre les informations qu'il aurait découvertes dans le cadre des procédures ouvertes pour crimes ou délits de guerre ou pour crimes contre l'humanité

La commission a émis un avis favorable à l'adoption sans modification de cet article.

1. Des dérogations encadrées au secret de l'enquête pour permettre l'action des services de renseignement

L'article 706-25-2 du code de procédure pénale permet au procureur de la République de communiquer aux services dits du premier cercle des informations issues des procédures ouvertes en matière de terrorisme.

Cette disposition est issue d'un amendement du rapporteur du Sénat, alors François Grosdidier, adopté par la commission des lois lors de l'examen de la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique. Le rapporteur expliquait cette dérogation au secret de l'enquête par les considérations suivantes :

« *La lutte contre le terrorisme, à laquelle concourent l'autorité judiciaire et les services spécialisés de renseignement, nécessite une coordination efficace entre la police administrative et la police judiciaire. Dans cette perspective, les services de renseignement alimentent les procédures judiciaires en application du deuxième alinéa de l'article 40 du code de procédure pénale, auquel il est fait une référence explicite au troisième alinéa de l'article L. 811-2 du code de la sécurité intérieure, et à l'occasion des réponses aux réquisitions judiciaires dont ces services sont saisis. À l'inverse, il apparaît indispensable que les services de renseignement puissent avoir accès à certains éléments figurant dans les procédures judiciaires lorsque leur connaissance est nécessaire à l'exercice de leurs missions en matière de prévention des actes terroristes.* »

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

L'une, dans le prolongement de la loi du 28 février 2017, permet aux services de renseignement de se voir transmettre, à l'initiative du procureur ou, selon le cas, du juge d'instruction, ou à leur demande, les informations issues des procédures et relatives à la prévention de la criminalité et de la

délinquance organisées. Cette extension particulièrement large bénéficie tant aux services du premier cercle qu'à ceux du second.

L'autre permet au procureur de la République de Paris, pour les procédures d'enquête et d'instruction en matière de cybercriminalité, de communiquer des éléments de toute nature figurant dans ces procédures.

La commission des lois avait admis ces nouvelles exceptions pour faire face au risque émergent de la cybercriminalité et pour mieux faire face au risque lié à la criminalité organisée dont le pouvoir de corruption et donc de déstabilisation des institutions a été souligné par la délégation parlementaire au renseignement[1].

Elle avait cependant posé deux conditions. La première était que les dérogations au secret de l'enquête ne deviennent pas trop nombreuses, au risque de priver à terme ce principe de toute effectivité. La seconde était la préservation de l'appréciation des magistrats sur les informations à communiquer, même en cas de demande formulée par les services. Ce deuxième point a semble-t-il été garanti par les protocoles établis entre les services et la Chancellerie pour définir les procédures de transmission.

2. Le dispositif proposé par le projet de loi

Le projet de loi propose d'introduire dans le code de procédure pénale un article 628-8-1 prévoyant une nouvelle possibilité de transmission d'information aux services de renseignement, celle-ci en matière de crimes contre l'humanité, de crimes et délits de guerre, ainsi que les infractions qui leur sont connexes. Cette exception serait justifiée par la situation au Sahel, au Levant et en Ukraine, selon l'étude d'impact :

« *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.* »

L'exception proposée comporte plusieurs limites. Tout d'abord, la transmission d'informations ne sera possible qu'avec les services du premier cercle. Ensuite, elle ne pourra être justifiée que pour certaines des finalités prévues à l'article L. 811-13 du code de la sécurité intérieure :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale ;

[1] *Rapport n° 547 (2021-2022) du 24 février 2022 de François-Noël Buffet.*

- 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 ;

- la prévention du terrorisme ;

- la prévention de la criminalité et de la délinquance organisées ;

- la prévention de la prolifération des armes de destruction massive.

Enfin, comme c'est le cas pour les autres exceptions prévues par le code de procédure pénale, les informations transmises ne pourront faire l'objet d'un échange avec des services étrangers. Elles sont couvertes par le secret professionnel, sauf pour les condamnations publiques.

3. La position de la commission : un complément légitime aux exceptions déjà prévues en matière de secret de l'enquête

La commission des lois considère que cet article s'inscrit dans le prolongement de la loi du 28 février 2017 et apporte une dérogation suffisamment limitée et légitime au secret de l'enquête.

La justification de la nécessité et de l'ampleur de la délégation repose sur l'existence « *d'une certaine porosité entre les différents faits criminels* [contre l'humanité, de guerres et connexes] *et (…) la diversification de certains individus ou groupes déterminés dans leurs activités* ». La commission reconnaît l'existence de cette porosité mais constate son caractère limité qui ne devrait conduire qu'à des transferts d'informations peu nombreux. Elle souligne cependant que, spécialement dans le cadre du développement de la compétence universelle des juridictions françaises (articles 689 et suivants du code de procédure pénale), la finalité de l'action des services tenant 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* » pourrait être invoquée plus fréquemment par les services pour susciter des échanges.

La commission des lois sera donc attentive au bilan qui pourra être tiré des échanges entre la justice et les services de renseignement dans le cadre autorisé par ce nouvel article.

La commission a donné un avis favorable à l'adoption de l'article 21 **sans modification.**

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

L'article 22 tend à permettre de protéger l'identité des anciens agents des services de renseignement ou unités des forces spéciales dans les affaires dans lesquelles ils sont appelés à témoigner du fait de leur participation à une mission intéressant la défense et la sécurité nationales, au même titre qu'est protégée l'identité des agents en fonction.

La commission a émis un avis favorable à l'adoption de cet article sans modification.

1. L'identité des agents des services de renseignement et des unités spéciales

La divulgation de l'identité des agents des services de renseignement et des membres des unités des forces spéciales est réprimée par les articles 413-13 et 413-14 du code pénal.

Cette protection s'applique également dans le cadre de la procédure pénale, l'article 651-1 du code de procédure pénale dispose que l'« *identité réelle* [d'un agent des services de renseignements ou d'un membre d'une unité spéciale] *ne doit jamais apparaître au cours de la procédure judiciaire* », lorsque son témoignage « *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* ».

2. Le dispositif proposé par le projet de loi

L'article 22 tend à compléter l'article 651-1 du code de procédure pénale pour prévoir que l'interdiction de faire apparaître l'identité d'un agent ou membre d'une unité spéciale s'applique également aux anciens agents et membres des unités.

Cette précision, nécessaire du fait du principe d'interprétation stricte de la loi pénale, permet de répondre aux situations dans lesquelles une personne est appelée à témoigner de faits qu'elle a connus dans le cadre de l'exercice de ses missions en tant qu'agent ou au sein d'une unité spéciale.

Elle souligne le fait que ce sont les personnes elles-mêmes qu'il convient de protéger et non pas uniquement le fonctionnement des services ou unités auxquelles elles appartiennent ou ont appartenu.

L'Assemblée nationale n'a pas adopté de modifications autres que rédactionnelles à cet article.

3. La position de la commission : un complément pragmatique aux dispositions protégeant l'identité des agents et membres des unités spéciales.

La commission des lois considère que les dispositions proposées par l'article 22 sont proportionnées, les garanties prévues devant légitimement s'appliquer aux personnes qu'elles soient encore en fonction ou non.

Elle a émis un avis favorable à l'adoption de cet article sans modification.

La commission a donné un avis favorable à l'adoption de l'article 22 **sans modification.**

Article additionnel après l'article 22

Conditions d'accès la Commission nationale de contrôle des techniques de renseignement aux éléments recueillis par les services dans le cadre de certaines techniques

L'amendement adopté à l'initiative du rapporteur tend à donner à la Commission nationale de contrôle des techniques de renseignement (CNCTR) un accès immédiat aux éléments collectés par les services de renseignement afin d'assurer son contrôle de la mise en œuvre des techniques de renseignement les plus intrusives.

Le dispositif proposé

La Commission nationale de contrôle des techniques de renseignement (CNCTR) est l'autorité administrative indépendante en charge du contrôle de l'utilisation des techniques de renseignement.

Elle apprécie la proportionnalité des atteintes portées à la vie privée par une technique de renseignement au regard de finalités prévues par l'article L.811-3 du code de la sécurité intérieure.

Le contrôle de la CNCTR s'exerce *a priori*, puisqu'elle émet un avis sur toutes les demandes de mise en œuvre d'une technique de renseignement soumises par les services au Premier ministre.

Il s'exerce également *a posteriori* pour contrôler que la mise en œuvre de la technique de renseignement respecte les conditions posées lors de son autorisation et notamment les conditions de conservation et de destruction des données, renseignements ou documents collectés.

Matériellement, le contrôle de la CNCTR *a posteriori* prend deux formes. Lorsque les données sont centralisées au Groupement interministériel de contrôle, elle les contrôle depuis ses propres locaux ; lorsque les éléments collectés sont stockés au sein des services de renseignement, elle s'y déplace. La centralisation ou non des éléments collectés varie selon le type de technique.

La nécessité pour les agents de la CNCTR de se déplacer pose deux principales difficultés.

D'une part, cela impose un déplacement physique, généralement avec prise de rendez-vous, ce qui est une contrainte matérielle sur le contrôle. D'autre part, le fait que les éléments collectés soient stockés dans les services et non immédiatement accessibles à la CNCTR pose le risque d'éclatement des données collectées, c'est-à-dire que certaines soient stockées par exemple sur un poste de travail et échappent ainsi au tri et au contrôle.

Cette situation est particulièrement inadaptée pour les trois techniques les plus intrusives, qui sont en outre sans doute appelées à devenir les plus utilisées en matière de renseignement :

- la captation de paroles prononcées à titre privé (article L. 853-1 du code de la sécurité intérieure) ;

- la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;

- le recueil ou la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure).

L'amendement portant article additionnel adopté par la commission à l'initiative du rapporteur **(COM-127)** tend donc à prévoir l'accès direct et immédiat de la CNCTR aux éléments collectés par l'intermédiaire de ces trois techniques. Ceci facilitera matériellement le travail de la CNCTR. Surtout cette disposition renforcera le caractère exhaustif du contrôle sur les masses d'éléments collectés grâce à ces techniques. Elle s'inscrit dans la continuité des échanges entre la CNCTR et la coordination nationale du renseignement tendant à la centralisation des éléments collectés par les différentes techniques de renseignement et permettra les progrès nécessaires en ce domaine.

La commission a donné un avis favorable à l'adoption de cet article additionnel ainsi **rédigé.**

Article additionnel après l'article 22

Information de la délégation parlementaire au renseignement

L'amendement adopté par la commission, adopté à l'initiative du rapporteur, tend à compléter l'information de la délégation parlementaire au renseignement en prévoyant explicitement qu'elle a connaissance des sujets d'actualité et qu'un bilan annuel des recommandations présentées par la Commission nationale de contrôle des techniques de renseignement au Premier ministre lui est adressé.

Le dispositif proposé par la commission

La loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a renforcé les prérogatives de la délégation parlementaire au renseignement (DPR) en lui reconnaissant explicitement la possibilité de traiter des enjeux d'actualité liés au renseignement. Il s'agissait, sans interférer avec les opérations en cours, de souligner l'intérêt pour la délégation de mener des travaux en prise avec l'actualité, en usant d'un droit d'accès à des informations classifiées, ce qui n'est permis à aucun autre organe parlementaire. Or, la DPR s'est vu refuser par le Gouvernement des auditions relatives aux affaires « Pegasus » et « Sirli » dont les médias s'étaient pourtant fait l'écho. Ce point a fait l'objet d'une analyse dans le dernier rapport annuel de la DPR[1].

Afin d'écarter toute divergence d'interprétation, il est proposé par l'**amendement COM-128** du rapporteur de remplacer le terme d'enjeux d'actualité, aux contours flous, par les termes « enjeux et sujets d'actualité ».

L'amendement tend par ailleurs à ce que soit communiqué à la DPR un bilan annuel des recommandations présentées par la Commission nationale de contrôle des techniques de renseignement au Premier ministre.

Il modifie en conséquence l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires qui détermine les pouvoirs de la DPR.

La commission a donné un avis favorable à l'adoption d'un article additionnel ainsi **rédigé.**

[1] *Rapport n° 547 (2021-2022) du 24 février 2022 de François-Noël Buffet.*

Article additionnel après l'article 22

Missions de la Commission nationale de contrôle des techniques de renseignement pour l'information de la délégation parlementaire au renseignement

L'amendement adopté par la commission, à l'initiative du rapporteur, tend à compléter les missions de la Commission nationale de contrôle des techniques de renseignement pour prévoir qu'elle transmet à la délégation parlementaire au renseignement un bilan annuel des recommandation qu'elle adresse au Premier ministre et l'informe de ses saisines du procureur de la République sur le fondement de l'article L. 861-3 du code de la sécurité intérieure.

Le dispositif proposé par la commission

Dans son rapport 2019-2020, la délégation parlementaire au renseignement (DPR) a formulé une recommandation visant à lui permettre d'être informée des recommandations adressées au gouvernement par la commission nationale de contrôle des techniques de renseignement (CNCTR) et tendant à l'interruption de la mise en œuvre d'une technique de renseignement et à la destruction des renseignements collectés, en cas d'irrégularité constatée.

Il est essentiel pour la délégation de disposer, chaque année, d'un bilan des recommandations adressées par l'autorité administrative indépendante afin de savoir si des techniques de renseignement ont été accordées, mises en œuvre ou exploitées en méconnaissance du livre VIII du code de la sécurité intérieure. Les membres de la DPR pourront ainsi disposer de ces éléments pour savoir si des contournements au cadre juridique qu'ils ont posé ont été constatés pour, le cas échéant, apporter les modifications législatives nécessaires. Dans ce bilan, il ne sera fait mention d'aucun élément permettant aux membres de la délégation de connaître d'une opération en cours ou d'une méthode opérationnelle.

Dans ce même rapport, la DPR a émis une recommandation visant à ce qu'elle soit informée des saisines du procureur de la République par la commission nationale de contrôle des techniques de renseignement (CNCTR), sur le fondement de l'article L. 861-3 du code de la sécurité intérieure – il s'agit d'un dispositif de lanceur d'alerte limité aux seules techniques de renseignement, introduit par la loi de 2015. Cette information est destinée à orienter la délégation dans ses travaux de contrôle de la politique publique de renseignement, lesquels n'ont pas vocation à se substituer au travail de la justice.

Par coordination avec l'amendement précédent adopté par la commission, cet amendement inscrit la transmission d'un bilan annuel des recommandations parmi les missions de la CNCTR à l'article L. 833-6 du

code de la sécurité intérieure. Il inscrit par ailleurs l'information la transmission à la DPR des saisines du procureur à l'article L. 861-3 du même code.

La commission a donné un avis favorable à l'adoption d'un article additionnel **ainsi rédigé.**

Article 27

Renforcement du régime légal de lutte contre les aéronefs circulant sans personne à bord présentant une menace

L'article 27 a pour objet d'étendre les moyens techniques dont disposent les services de l'État pour prévenir les menaces résultant de l'utilisation malveillante d'un drone civil.

La commission a donné un avis favorable à l'adoption de cet article, après l'avoir complété pour préciser que les conditions de mise en œuvre des moyens de neutralisation du drone devraient être précisées par décret en Conseil d'État.

1. La nécessité de doter les services de l'État des moyens de prévenir les menaces résultant de l'utilisation malveillante d'un drone

Issus de la technologie militaire, les drones civils se sont considérablement développés au cours des dix dernières années – leur nombre en circulation sur le territoire national serait ainsi passé de 400 000 en 2017 à 2,5 millions en 2021, dont plus de 40 000 drones de plus de 800 grammes, d'après un récent rapport de la commission des affaires étrangères, de la défense et des forces armées[1].

Porteurs d'opportunités de développement technologique variées et prometteuses (en matière de protection civile, de surveillance de l'environnement, d'information, d'agriculture ou encore de transport de colis notamment), ils peuvent également présenter des risques pour la sécurité des personnes et des biens, du fait de risques de collision et de chute, mais également, par les dispositifs de captation d'image et de son à l'insu des personnes dont ils peuvent être dotés, un défi pour la protection de la vie privée et le respect des données personnelles.

Surtout, la prévention de leur utilisation à des fins malveillantes constitue un véritable enjeu pour les pouvoirs publics, comme l'a par

[1] *« Se préparer à la « guerre des drones » : un enjeu stratégique », rapport d'information n° 711 (2020-2021) fait au nom de la commission des affaires étrangères, de la défense et des forces armées par MM. Cédric Perrin, Gilbert Roger, Bruno Sido et François Bonneau, déposé le 23 juin 2021 : https://www.senat.fr/rap/r20-711/r20-711.html*

exemple montré l'incident de l'aéroport de Londres Gatwick en décembre 2018, lorsque le survol illégal de ce dernier par plusieurs drones a entraîné la paralysie totale du trafic aérien pendant plusieurs jours et le blocage de 140 000 personnes. La protection des sites et évènements sensibles (centrales nucléaires, sommets internationaux, manifestations sportives, *etc.*) et la prévention de la menace terroriste et des trafics criminels nécessitent à cet égard de pouvoir agir vite.

Afin de prévenir ces différents risques sans entraver le développement d'un secteur économique en expansion, la France s'est dotée à partir de 2012 d'une réglementation complète, progressivement inscrite dans un cadre communautaire, qui soumet les drones aux normes internationales et nationales du droit aérien en les assimilant à des aéronefs et définit leurs conditions d'utilisation et de navigation en fonction, notamment, de la masse de l'engin et du type de zones survolées (voir encadré).

Réglementation applicable au vol de drones

Les usages de drones, récréatifs ou professionnels, font l'objet des règlements européens (UE) 2019/945 relatif aux systèmes d'aéronefs sans équipage à bord et 2019/947 concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord. Ceux-ci posent un ensemble de conditions pour l'exploitation des drones et leur circulation dans l'espace aérien en fonction du niveau de risque de l'opération entreprise. Ainsi, à titre d'exemple, tout drone doit voler à moins de 120 mètres de hauteur et de façon à ne pas survoler de rassemblement de personnes au sol. Les États membres peuvent fixer des exigences complémentaires pour leur circulation. La plupart des activités professionnelles sont déclaratives et nécessitent de respecter un ensemble de conditions relatives aux opérations, à la formation du pilote et aux équipements du drone. Les usages les plus complexes nécessitent toutefois une autorisation de la direction générale de l'aviation civile. Au niveau national, diverses interdictions et restrictions de vol sont imposées pour protéger des activités et sites spécifiques, notamment les abords d'aérodromes, des zones militaires, des installations industrielles ou nucléaires, des parcs et réserves naturelles nationaux. En milieu urbain, pour les vols en espace public, il est requis une déclaration à la préfecture, qui peut opposer un refus. Une notification aux autorités militaires est exigée dans certaines zones. En outre, des zones réservables pour l'utilisation de drones peuvent être créées dans l'espace aérien à titre permanent ou temporaire pour des expérimentations, par exemple pour des opérations sur de longues distances. Il en a été créé un nombre limité en France, en fonction des besoins. L'ensemble de la réglementation concernant les drones est présenté de façon didactique et détaillée sur le site internet du ministère de la transition écologique et de la cohésion des territoires à l'adresse https://www.ecologie.gouv.fr/politiques/drones-aeronefs-telepilotes. […]

Source : extrait de la réponse du Ministère auprès du ministre de la transition écologique et de la cohésion des territoires, chargé des transports publics, à une question de Jean-Louis Masson, publiée au JO Sénat le 6 octobre 2022.

En outre, afin de parer aux menaces imminentes, la loi n° 2021-998 du 30 juillet 2021 relative à la prévention des actes de terrorisme et au renseignement a inséré à l'article L. 33-3-1 du code des postes et des communications électroniques une disposition autorisant les services de l'État à recourir **à des dispositifs de « brouillage » des drones**, « *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* » – cette dernière mention ayant vocation à désigner pour l'essentiel les établissements pénitentiaires –, ou afin d'empêcher le survol d'une zone interdite[1].

Comme l'expliquait l'étude d'impact annexée à cette loi, la neutralisation de l'équipement radioélectrique de ce type d'aéronef a pour effet de l'empêcher de recevoir et d'émettre des ondes lui permettant de se localiser dans l'espace et de perturber ainsi son itinéraire et, le cas échéant, la transmission immédiate de données captées pendant le vol au télépilote ou à un tiers. Cette neutralisation de l'équipement radioélectrique par brouillage ne permet pas à l'aéronef de continuer son vol tel que programmé initialement ou tel que prévu par le télépilote. Dans certains cas, sa mise en œuvre peut avoir pour conséquence la chute et la destruction du drone.

La mise en œuvre de ce dispositif a été précisée par un récent décret n° 2023-204 du 27 mars 2023 relatif au brouillage des aéronefs circulant sans personne à bord, lequel donne compétence au Premier ministre, au ministre de la défense et au représentant de l'État dans le département, dans le champ de leurs attributions respectives, pour autoriser l'utilisation de matériels de brouillage, décrit la procédure d'autorisation du brouillage, qu'il subordonne à la réalisation d'une étude d'impact coordonnée par l'Agence nationale des fréquences afin d'évaluer l'impact du brouillage sur les affectataires de fréquences, et recense, enfin, les agents de l'État autorisés à utiliser les brouilleurs.

2. Le dispositif proposé par le projet de loi

Bien qu'il ne soit opérationnel que depuis peu de temps, le Gouvernement fait valoir que le dispositif introduit par la loi du 30 juillet 2021 ne répond que partiellement au besoin de protection contre les drones malveillants, dès lors que les développements technologiques rendent progressivement une partie des drones autonomes[2] et donc insensibles au brouillage.

---

[1] *Aux termes de l'article L. 6211-4 du code des transports, « le survol de certaines zones du territoire français peut être interdit pour des raisons d'ordre militaire ou de sécurité publique dans des conditions fixées par décret en Conseil d'État. L'emplacement et l'étendue des zones interdites sont définis par l'autorité administrative. […] ».*

[2] *Par « autonomes », on entend le fait que leur navigation ne repose pas 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.*

L'article 27 du projet de loi vise donc à **élargir le dispositif adopté en 2021 à un plus large ensemble de moyens techniques, qui seront désignés par arrêté, permettant de « rendre inopérant ou de neutraliser » un drone** présentant une menace imminente pour l'ordre public, la défense ou la sécurité nationales, le service public de la justice ou survolant une zone interdite de survol. Concrètement, il s'agit d'autoriser les services de l'État à utiliser non seulement des systèmes de brouillage, mais également **des armes à effet dirigé électromagnétiques** ou des **drones intercepteurs**, lesquels pourront notamment **capturer le drone par filet ou le percuter afin de le faire chuter**. Compte tenu de cet élargissement des dispositifs autorisés, l'article transfère la disposition **dans le code de la sécurité intérieure** et abroge concomitamment celle qui avait été introduite dans le code des postes et des communications électroniques en 2021. Ses modalités d'application outre-mer sont réglées à l'article 36 du projet de loi.

Cet article a suscité peu de débats lors de son examen à l'Assemblée nationale, qui a adopté en séance publique un amendement du Gouvernement tendant à permettre également **aux services de certains établissements publics concourant à la défense nationale**, tels que le Commissariat à l'énergie atomique, de recourir le cas échéant à ces dispositifs de brouillage ou de neutralisation de drones représentant une menace.

3. La position de la commission : approuver le dispositif de l'article 27 tout en appelant à une vigilance particulière sur les conditions dans lesquelles il sera mis en œuvre

Cet article appelle plusieurs observations de la part de la commission des lois.

En premier lieu, au regard du nombre important de survols de zones interdites constatés chaque année[1] et des risques qu'ils présentent pour la sécurité nationale, de la capacité croissante des drones à transporter des substances dangereuses (explosifs, armes, dispositifs de piratage) ou interdites (produits stupéfiants), et à l'approche de grandes manifestations sportives (coupe du monde de rugby, jeux Olympiques) qui vont poser des enjeux de sécurité inédits, les finalités poursuivies par cet article ne souffrent guère de contestation : il paraît en effet **indispensable de doter les services de l'État des moyens de réagir rapidement à toute menace** que pourrait représenter l'incursion d'un drone dans un périmètre sensible.

En second lieu, la rédaction proposée par le projet de loi est **particulièrement épurée**, tant en ce qui concerne les conditions de mise en œuvre du dispositif – l'existence d'une menace imminente – qu'en ce qui concerne les finalités poursuivies – les besoins de l'ordre public, de la

[1] *En 2019, 335 survols illicites ont été relevés par le ministère de l'intérieur et 54 par le ministère de la justice.*

défense et de la sécurité nationales ou du service public de la justice (lequel ne semble viser, d'après l'étude d'impact, que la protection des établissements pénitentiaires), ou encore le survol d'une zone interdite.

D'après les précisions apportées par les services du ministère des armées, la référence aux « *besoins de la défense nationale* » vise en particulier à assurer la sécurité des convois militaires et des convois transportant des matières nucléaires, tandis que celle des « *besoins de la sécurité nationale* » traduit la nécessité, pour les services de renseignement, d'assurer la protection de leurs emprises qui ne seraient pas nécessairement des zones interdites de survol. Quant aux « *besoins de l'ordre public* », ils peuvent viser notamment la nécessité d'assurer la protection de certains évènements sportifs (par exemple le Tour de France cycliste).

Il ressort surtout des explications fournies que le dispositif proposé par cet article **sera, la plupart du temps, mis en œuvre dans des zones faisant l'objet d'une interdiction de survol édictée à titre permanent ou temporaire**. En effet, les grands évènements ou manifestations sont la plupart du temps organisés dans des agglomérations ou des zones où le vol est déjà très réglementé, voire interdit. Les drones qui s'y trouveraient sont alors en principe titulaires d'une autorisation permettant aux forces de sécurité de les identifier facilement et de les différencier des drones non autorisés. En présence d'un drone non autorisé, les mesures sont mises en œuvre par les forces de l'ordre de façon graduelle, allant de l'invitation faite au télépilote de faire sortir son drone de la zone concernée à, en dernier ressort, la « neutralisation » de ce dernier, si les mesures d'effarouchement, d'immobilisation, de perturbation ou de capture du drone n'ont précédemment eu aucun effet.

La commission admet sans difficultés que le dispositif de neutralisation du drone puisse être mis en œuvre dans de telles circonstances.

Elle s'interroge en revanche sur **la possibilité, que laisse ouverte le dispositif, de les mettre en œuvre également dans des zones qui ne feraient pas l'objet d'une interdiction de survol permanente ou temporaire**. En pareille hypothèse, la circulation des drones est alors non seulement, par principe, légale (sous réserve du respect par ailleurs de la réglementation générale applicable aux drones), mais elle peut en outre poursuivre une finalité légitime – par exemple lorsque le drone est utilisé par des journalistes aux fins d'informer le public sur un évènement ou une manifestation. Il pourrait en résulter une atteinte excessive à des droits ou libertés constitutionnellement garantis (droit de propriété, liberté de communication, liberté d'informer, notamment). Or, au regard de ce risque, le texte proposé par le projet de loi se contente de rappeler les principes de la jurisprudence constitutionnelle aux termes de laquelle les mesures prises doivent être « *adaptées, nécessaires et proportionnées au regard des finalités poursuivies* ».

En réponse à ces interrogations, les services du ministère des armées ont précisé que, dans de telles circonstances, les forces de l'ordre caractérisent l'existence d'une menace imminente en prenant en compte le « comportement » du drone, par exemple si celui-ci demeure de façon prolongée en surplomb d'une zone ou d'un évènement sensible, s'il projette des matières, explosives ou pas, ou s'il paraît suivre une trajectoire destinée à toucher une infrastructure, un bien ou une personne. Dans tous les cas, les mesures ne sont mises en œuvre qu'afin de répondre à l'une des finalités prévues par le texte.

La commission estime néanmoins qu'au regard des risques d'atteinte à certains droits et libertés constitutionnellement garantis que pourrait présenter la neutralisation du drone, en particulier dans une zone dans laquelle la circulation de ce dernier n'a pas été préalablement interdite, les conditions de mise en œuvre du dispositif mériteraient d'être précisées de façon explicite. À l'initiative du rapporteur, elle a donc adopté un **amendement n° COM-130** tendant à prévoir qu'elles le seront **par décret en Conseil d'État**, dans le respect des principes et finalités édictés par cet article.

La commission a donné un avis favorable à l'adoption de l'article 27 **ainsi modifié.**

Article 32

Possibilité pour l'ANSSI de prescrire des mesures de filtrage de noms de domaine en cas de menace sur la sécurité nationale

L'article 32 vise à doter l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de la possibilité de prescrire des mesures de filtrage ou de redirection de noms de domaine utilisés ou instrumentalisés par des cyber-attaquants en cas de menace pour la sécurité nationale.

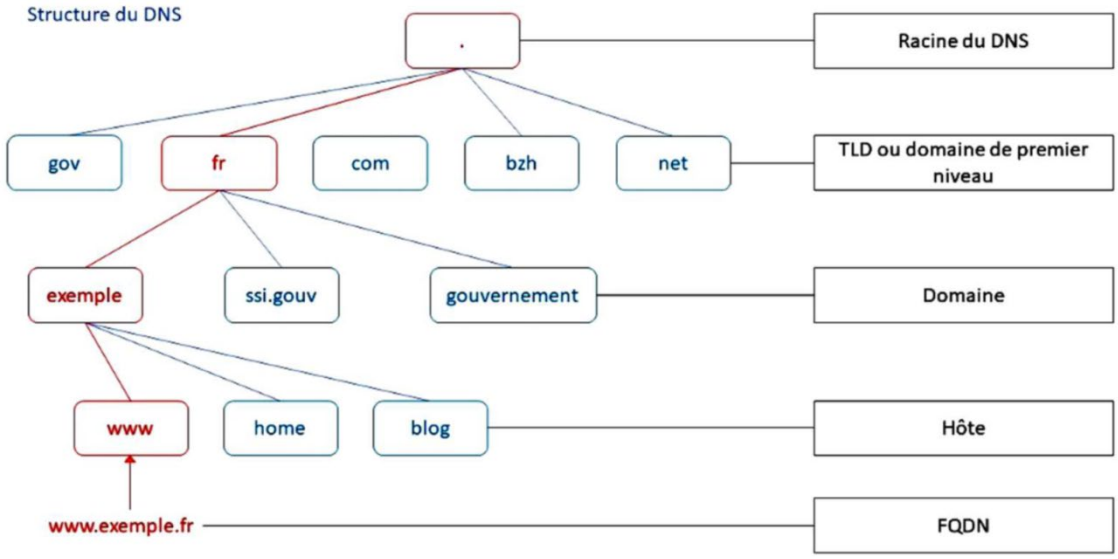
La commission propose d'adopter cet article sous réserve de deux modifications tendant à en simplifier et préciser le dispositif.

1. L'exploitation frauduleuse du système DNS, une menace informatique pouvant porter atteinte à la sécurité nationale

Infrastructure essentielle d'Internet, le système DNS (pour « *Domain Name System* » ou « système de nom de domaine ») est, à ce titre, sujet à de nombreuses exploitations frauduleuses et attaques informatiques qui menacent la sécurité des systèmes d'information et peuvent par ce biais porter atteinte à la sécurité nationale.

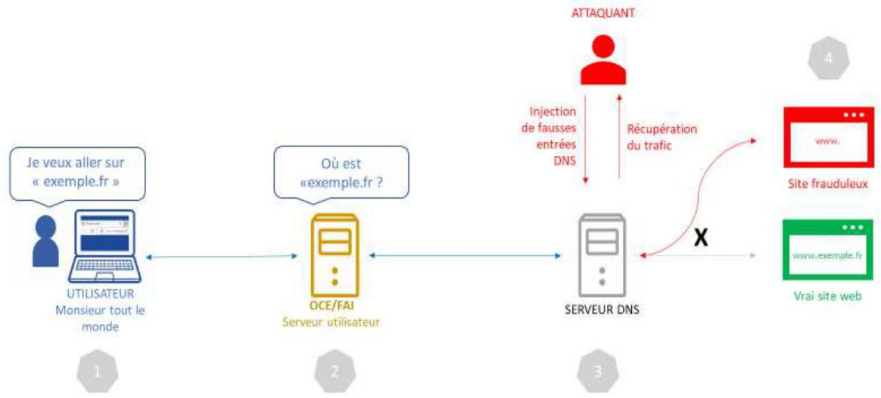
Concrètement, le système DNS est un service informatique permettant de faire correspondre une adresse IP (pour *Internet Protocol*) avec un identifiant alphanumérique (appelé *Fully Qualified Domain Name*). Les adresses IP, qui prennent la forme d'une suite de numéros, permettent d'identifier l'ensemble des périphériques connectés au réseau internet. Le nom de domaine, plus simple à retenir que cette suite de numéros, permet quant à lui de faciliter l'usage et les recherches des utilisateurs du réseau IP.

Cet identifiant alphanumérique est créé selon un système hiérarchique, permettant de garantir l'unicité d'un nom, et rassemblant des domaines successifs séparés par un point : généralement, le premier niveau, appelé « *Top Level Domain* », correspond à une identification nationale (« .fr » par exemple), le second à la dénomination du site (« senat.fr » par exemple), et le troisième à l'hôte (www.senat.fr. par exemple).



Source : étude d'impact du projet de loi

Afin d'établir la correspondance entre le nom de domaine et l'adresse IP, il est nécessaire d'interroger différents serveurs de nom de domaine, selon le système hiérarchique du DNS. La grande majorité des attaques informatiques utilisent ce mécanisme d'association, appelé « résolution du nom de domaine ». Comme expliqué par l'étude d'impact du projet de loi, elles peuvent par exemple rediriger le flux d'un des domaines composant l'ensemble du nom vers un site malveillant.



Exemple d'une vulnérabilité du DNS

Source : étude d'impact du projet de loi

En vue de renforcer la sécurisation des systèmes d'information, certains pouvoirs ont déjà été conférés à l'ANSSI, notamment par l'article L. 2321-2-1 du code de la défense qui lui permet de mettre en œuvre des dispositifs de détection sur le serveur d'un hébergeur, d'un fournisseur d'accès à Internet, ou d'un opérateur de communication électronique lorsqu'elle a connaissance d'une menace susceptible d'affecter la sécurité des systèmes d'exploitation. Toutefois, si elle dispose de **pouvoirs de détection des attaques informatiques, aucune capacité de neutralisation des menaces graves et avérées ne lui est encore attribuée**.

2. Le dispositif proposé par le projet de loi : conférer à l'ANSSI un pouvoir d'injonction de mesures de filtrage afin de sécuriser le système DNS en cas de menaces susceptibles de porter atteinte à la sécurité nationale

S'il existe déjà des dispositions législatives permettant la mise en œuvre ou l'injonction de mettre en œuvre des mesures de filtrages, afin de supprimer des contenus et de bloquer des adresses IP sur Internet, aucune des mesures préexistantes ne sont utilisées aux fins de bloquer une utilisation malveillante du système DNS, ni aux fins de protéger la sécurité nationale. Elles sont principalement utilisées pour la lutte contre le terrorisme, la pédopornographie, ou encore les pratiques commerciales trompeuses.

L'article 32 du projet de loi, qui crée un nouvel article L. 2321-2-3 du code de la défense, vise à fournir à l'ANSSI des moyens d'action afin que, **lorsqu'elle identifie une menace, elle puisse prendre des mesures graduelles pour neutraliser** l'utilisation dévoyée d'un nom de domaine. Ces possibilités d'injonction ne lui sont toutefois octroyées que lorsqu'il existe une **menace susceptible de porter atteinte à la défense et à la sécurité nationale.** L'appréciation de cette atteinte dépend généralement de l'identité de l'attaquant et de la victime, et de la complexité des moyens employés. Les mesures d'injonction prises par l'ANSSI, ainsi que la conservation des

données recueillies au cours des procédures de redirection de noms de domaine, **sont contrôlées par l'ARCEP.**

Concrètement, le dispositif **distingue selon que le propriétaire du nom de domaine malveillant a été enregistré de bonne foi ou non**. Lorsque le titulaire du nom de domaine n'est pas à l'origine de son exploitation malveillante, l'ANSSI enjoint des mesures de filtrage graduelles :

- dans un premier temps, elle demande au **titulaire du nom de domaine** de prendre les mesures adaptées pour neutraliser la menace, dans un délai imparti qui tient compte de la nature du titulaire et de ses contraintes opérationnelles ;

- en l'absence de neutralisation dans le délai imparti, l'ANSSI peut alors enjoindre à un **fournisseur de système de résolution de noms de domaine** de bloquer le nom de domaine, ou enjoindre à **un office ou bureau d'enregistrement** la suspension de ce nom de domaine.

En revanche, lorsque le propriétaire du nom de domaine l'a enregistré dans le seul but de commettre des actes malveillants, l'ANSSI peut alors **directement enjoindre** aux acteurs du numérique des mesures de filtrage, afin d'agir dans les plus brefs délais :

- elle peut enjoindre à un fournisseur de système de résolution de noms de domaine de procéder au blocage ou à la redirection du nom de domaine vers un serveur sécurisé ou un serveur neutre ;

- elle peut demander à l'office ou au bureau d'enregistrement d'enregistrer, de renouveler, de suspendre ou de transférer le nom de domaine, afin de s'assurer que le blocage ne puisse être contourné.

Une redirection vers un serveur sécurisé et maîtrisé par l'ANSSI doit lui permettre d'observer le mode opératoire de l'attaquant, pendant une durée de deux mois maximum, renouvelable une fois après avis conforme de l'Autorité de régulations des communications électroniques, des postes et de la distribution de la presse (ARCEP). La redirection vers un serveur neutre d'un nom de domaine permet d'informer les usagers de la suspension d'un nom de domaine. En ce sens, l'article 32 prévoit également de doter l'ANSSI d'un **pouvoir d'information des utilisateurs ou des détenteurs des systèmes d'information menacés.**

3. La position de la commission : un dispositif utile et pertinent face à une menace cyber croissante pesant sur la sécurité nationale

Au regard de l'objectif poursuivi de protection de la défense et de la sécurité nationale, et de la nécessité de renforcer les moyens d'action face aux risques de cyber-attaques, toujours plus complexes et nombreuses, la commission souscrit sans réserves au dispositif proposé par l'article 32, qui lui paraît à la fois **adapté** et **proportionné**. Elle relève qu'au-delà de mesures

de détection des attaques informatiques, la capacité de neutraliser les menaces graves est une prérogative essentielle, qu'il convient évidemment d'encadrer afin d'éviter toute atteinte disproportionnée aux libertés d'entreprendre et de communiquer, ainsi qu'à la neutralité d'Internet.

Elle souligne ainsi que, d'une part, ces mesures sont strictement réservées aux menaces graves, susceptibles de porter atteinte à la sécurité nationale, et que, d'autre part, elles sont proportionnées en prévoyant un dispositif différencié selon que le propriétaire est de bonne foi ou non.

Toutefois, au regard de la masse de données que l'ANSSI peut recueillir au cours de la redirection d'un nom de domaine, des garanties suffisantes doivent entourer les délais de conservation de ces données. C'est pourquoi la commission des lois **a accueilli favorablement la réduction du délai de conservation des données pertinentes de 10 à 5 ans** par l'Assemblée nationale. Elle a cependant considéré, au même titre que l'ARCEP, que la mention d'une **suppression « sans délai » des données non pertinentes était trop imprécise** et que la définition d'un délai fixe était nécessaire pour permettre à l'ARCEP d'effectuer un contrôle utile sur la mise en œuvre de ces dispositions par l'ANSSI. Elle a ainsi complété le projet de loi pour prévoir que ce délai, qui sera nécessairement bref, sera précisé par voie réglementaire (**amendement COM-133 du rapporteur**).

La commission a également adopté un **amendement du rapporteur (COM-134)**, identique à ceux apportés aux articles 33 et 35, **afin de prévoir que le projet de décret en Conseil d'État définissant les modalités d'application de cet article devra être soumis pour avis à la Commission nationale de contrôle des techniques de renseignement (CNCTR)**, en complément des avis de la Commission nationale de l'informatique et des libertés (CNIL) et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), aucune de ces deux autorités n'étant compétente pour apprécier l'état d'une menace sur la défense et la sécurité nationales

Enfin, à l'initiative du rapporteur, elle a **supprimé la mention de la concertation entre les fournisseurs de systèmes de résolution et l'ANSSI** pour fixer le délai dans lequel les mesures de filtrage doivent être prises (**amendement COM-132**), cette disposition n'étant pas nécessaire et incomplète, et a adopté un **amendement rédactionnel** (**COM-131**).

La commission a donné un avis favorable à l'adoption de l'article 32 **ainsi modifié**.

Article 33

Communication à l'ANSSI de données techniques de cache par les fournisseurs de systèmes de résolution de noms de domaine

L'article 33 vise à permettre à l'ANSSI d'améliorer sa connaissance des modes opératoires des cyber-attaquants en lui permettant de recueillir certaines données techniques non identifiantes.

La commission a donné un avis favorable à l'adoption de cet article, après avoir notamment précisé que les modalités de son application devraient être définies après avis, notamment, de la CNCTR.

1. La transmission de données de cache à l'ANSSI, une mesure permettant de renforcer la sécurité des systèmes d'information

L'article 33 du projet de loi entend permettre à l'ANSSI de se voir communiquer certaines données techniques dites « données de cache », non identifiantes, à des fins d'analyse et de recherche sur les modes opératoires des cyber-attaquants utilisant le système DNS (sur ce sujet, voir *supra* le commentaire de l'article 32). Ces données seront transmises aux seules fins de **garantir la défense et la sécurité nationales**, de répondre aux besoins de la **sécurité des systèmes d'information** ainsi que **de détecter et caractériser les attaques informatiques.**

Les données de cache correspondent **aux données conservées à la suite de la résolution du nom de domaine**, c'est-à-dire la correspondance entre une adresse IP et un nom de domaine. Pour permettre un gain de temps lors de recherches ultérieures, ces données sont enregistrées, de manière temporaire, par les serveurs de système de résolution de noms de domaine. Elles permettent ainsi, lorsqu'une demande identique est formulée, de ne pas interroger l'ensemble des serveurs pour établir la correspondance entre l'adresse IP et le nom de domaine. Ces données de cache comprennent :

- l'adresse IP source du périphérique de l'utilisateur ayant effectué la recherche ;

- le nom de domaine demandé ;

- la date de la recherche ;

- les adresses IP des différentes machines interrogées, qui contrairement aux adresse IP sources, ne sont pas identifiantes.

Le présent article vise à permettre la transmission régulière, par les fournisseurs de systèmes de résolution de noms de domaine, de ces données techniques, qui permettront à l'ANSSI de connaître les requêtes DNS qui ont été effectuées, afin de pouvoir identifier la structure de l'attaquant et de suivre son activité.

2. La position de la commission : de nouveaux moyens utiles et bienvenus

La commission souligne qu'en accroissant les capacités d'analyse et de compréhension des attaques par l'ANSSI, l'article proposé répond à un véritable besoin de renforcement de la sécurité des systèmes d'information.

Elle relève en outre qu'aucune atteinte n'est portée à l'identité de la personne ou au respect de sa vie privée, puisque le dispositif prévoit, d'une part, l'interdiction de **transmettre à l'ANSSI des données directement ou indirectement identifiantes,** et, d'autre part, **la stricte exploitation de ces données** à des fins de protection de la sécurité nationale, des systèmes d'information, et de caractérisation des attaques informatiques. Les fournisseurs de services de résolution devront procéder à l'anonymisation de l'ensemble des données transférées à l'ANSSI, qui ne pourra ainsi procéder à une quelconque identification.

Par conséquent, la commission des lois a considéré que **le dispositif retenu ne soulevait pas de difficulté au regard du droit des personnes au respect de leur vie privée**.

Lors de l'examen du projet de loi à l'Assemblée nationale, l'ensemble des garanties d'anonymisation et d'interdiction de transmission de certaines données identifiantes, qui n'étaient jusqu'alors qu'exposées dans l'étude d'impact, ont été explicitées dans le texte de loi. La commission des lois a adopté un amendement de clarification du rapporteur (**COM-135**) afin de coordonner ces nouvelles dispositions.

Elle a également adopté un amendement afin que le décret d'application en Conseil d'État soit pris après un avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR) (**amendement COM-136 du rapporteur**).

La commission a donné un avis favorable à l'adoption de l'article 33 **ainsi modifié.**

Article 34

Obligation pour les éditeurs de logiciels victimes d'un incident informatique ou d'une vulnérabilité critique d'en informer l'ANSSI et les utilisateurs du produit affecté

L'article 34 vise à obliger les éditeurs de logiciels à notifier à l'Autorité nationale de sécurité des systèmes d'information (ANSSI) les incidents ou vulnérabilités critiques affectant un de leurs produits et à en informer les utilisateurs recourant à ce dernier.

La commission a donné un avis favorable à l'adoption de cet article, sous réserve que soit précisé que l'ensemble des utilisateurs du logiciel concerné, et pas uniquement les utilisateurs professionnels, devraient être informés de l'existence de l'incident ou de la vulnérabilité en cause.

1. L'obligation d'information des éditeurs en cas d'incident ou de vulnérabilité sur leurs logiciels, une mesure visant à renforcer la bonne gouvernance informatique vis-à-vis des utilisateurs

L'article 34 s'inscrit dans la continuité de dispositions du droit européen et du droit français qui visent à inciter ou à obliger les acteurs du numérique à notifier des incidents portant tant sur les réseaux ou systèmes d'information que sur une violation de données personnelles. En ce sens, l'ANSSI bénéficie d'ores et déjà de prérogatives en la matière :

- elle doit se voir notifier tout incident touchant un système d'information d'importance vitale des opérateurs d'importance vitale (OIV), et tout incident significatif sur un système d'information des opérateurs de services essentiels (OSE) ou des fournisseurs de services numériques (FSN) ;

- elle peut également prendre des mesures d'information du public lorsqu'un incident vise les OSE ou les FNS.

Si certains éditeurs de logiciel procèdent déjà à des notifications à leurs utilisateurs en cas d'incident, il n'existe en revanche aucune obligation légale contraignant l'ensemble des éditeurs de logiciel à déclarer un incident à une autorité ou aux utilisateurs concernés. Pourtant, comme le souligne l'étude d'impact, certains éditeurs sous-estiment les conséquences des incidents ou des vulnérabilités sur leur système, ou « sur-anticipent » les réactions des marchés financiers ou des investisseurs, et préfèrent ainsi omettre d'en informer leurs utilisateurs.

2. Le dispositif proposé par le projet de loi

D'une part, afin de remédier à cette absence d'obligation légale et de renforcer les pratiques de bonne gouvernance des éditeurs vis-à-vis de leurs clients, **le présent article contraint les éditeurs de logiciels à informer les utilisateurs recourant au produit affecté par un incident ou une vulnérabilité sur le territoire français**. Ces dispositions permettront de garantir la bonne information des victimes potentielles parmi les utilisateurs du produit, afin qu'elles prennent toute mesure qu'elles jugent pertinente pour en limiter les effets.

Les éditeurs de logiciels sont spécifiquement définis par le présent article, en tant que personnes physiques ou morales qui conçoivent ou développent un produit logiciel, ou font concevoir ou développer un produit logiciel et le mettent à disposition d'utilisateurs, à titre onéreux ou non.

Lors de l'examen du projet de loi à l'Assemblée nationale, la notion d'incident informatique a également été précisée. Reprenant la définition inscrite dans la directive européenne dite « NIS 2 »[1], elle cible de façon plus précise les incidents informatiques compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement ou des services que les réseaux et les systèmes d'information offrent ou rendent accessibles. En outre, l'appréciation de la vulnérabilité d'un système d'information devrait être détaillée par décret.

D'autre part, **l'article prévoit également une information de l'ANSSI.** La nécessité d'intégrer l'ANSSI à ce processus de notification d'incidents ou de vulnérabilités sur un système d'information est justifiée :

- d'une part, par l'appui technique qu'elle peut apporter aux éditeurs, qui ne disposent pas nécessairement des capacités techniques leur permettant d'identifier les utilisateurs et de les informer ;

- d'autre part, par la réticence potentielle des éditeurs à se conforter à cette nouvelle obligation, d'autant que celle-ci n'est, en l'état du texte, assortie d'aucune sanction. Ainsi, les pouvoirs conférés à l'ANSSI d'enjoindre à l'éditeur de se conformer à son obligation d'information, ou d'informer elle-même l'utilisateur, voire de rendre public le manquement de l'éditeur, représentent des garanties d'efficacité du dispositif.

En outre, cette mesure concourra également à la sauvegarde de la sécurité nationale, dans la mesure où la notification des incidents et des vulnérabilités à l'ANSSI lui permettra d'assurer sa mission de sécurité et de défense des systèmes d'information, notamment si les incidents et les vulnérabilités sont susceptibles d'affecter des entités françaises sensibles.

---

[1] *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*

Lors de l'examen du projet de loi à l'Assemblée nationale, **plusieurs amendements ont été adoptés afin de garantir que le dispositif ne porterait pas une atteinte disproportionnée aux entreprises et à la liberté d'entreprendre**. Ainsi, les députés ont souhaité prévoir que les éditeurs de logiciels ne seraient soumis à l'obligation d'information que si l'incident ou la vulnérabilité porte une **atteinte significative** à leurs produits. L'emploi du terme « significatif » permet de restreindre l'obligation aux cas les plus graves. De surcroît, ils ont prévu que l'information des utilisateurs devrait se faire dans **un délai qui devra prendre en compte le temps nécessaire aux éditeurs pour prendre les mesures coercitives**. Enfin, **cette obligation n'est assortie d'aucune sanction**, en-dehors de la menace « réputationnelle » qui résulterait de la divulgation par l'ANSSI du manquement de l'éditeur.

Enfin, l'Assemblée nationale a souhaité restreindre le champ de l'obligation d'information aux **seuls utilisateurs « professionnels »** du logiciel concerné, afin de ne pas faire peser sur les éditeurs de logiciels une charge excessive.

3. La position de la commission : une obligation d'information proportionnée et encadrée, qui mérite de s'appliquer à l'ensemble des usagers concernés

La commission souscrit sans réserves au dispositif proposé par l'article 34, qui lui paraît à la fois **adapté** et **proportionné** aux objectifs de renforcement de la cyber-protection des entités françaises et d'amélioration des pratiques de bonne gouvernance des acteurs numériques à l'égard de leurs usagers.

Toutefois, elle estime que la restriction par l'Assemblée nationale du champ de l'obligation d'information aux seuls utilisateurs « professionnels » est **très contestable**, dès lors qu'un incident informatique ou une vulnérabilité critique est susceptible d'avoir des conséquences importantes pour tout utilisateur du logiciel concerné, y compris lorsque ce dernier n'est pas utilisé dans un cadre ou dans un but professionnel. Par conséquent, et au vu de l'ensemble des autres garanties apportées, la commission a souhaité rétablir l'information initialement prévue **à l'ensemble des utilisateurs du logiciel** (**amendement COM-137 du rapporteur**).

La commission a donné un avis favorable à l'adoption de l'article 34 **ainsi modifié.**

Article 35

Renforcement des compétences de l'ANSSI en matière de détection des cyberattaques et d'information des victimes

L'article 35 vise à renforcer et compléter les compétences dévolues à l'Agence nationale de sécurité des systèmes d'information (ANSSI). Il poursuit plusieurs objectifs :

- il permet à l'ANSSI de mettre en œuvre des dispositifs de recueil de données sur le réseau d'un opérateur de communications électroniques, ou sur le système d'information d'un fournisseur d'accès, d'un hébergeur ou d'un centre de données afin de détecter et de caractériser des menaces graves sur les systèmes d'informations des autorités publiques, des opérateurs stratégiques ou de leurs sous-traitants ;

- il rend obligatoire la mise en place de capacités de détection chez les opérateurs de communication électronique (OCE) désignés « opérateurs d'importance vitale » (OIV) ;

- il renforce les capacités d'information des victimes par l'ANSSI, en élargissant aux hébergeurs de données l'obligation de lui communiquer des informations concernant des utilisateurs ou détenteurs de systèmes d'informations vulnérables ou attaqués, et en élargissant la communication des données techniques des sous-traitants des autorités publiques et des opérateurs stratégiques ;

- enfin, il supprime l'obligation d'assermentation des agents de l'ANSSI habilités à obtenir ces informations, afin de rationaliser la procédure.

La commission a donné un avis favorable à l'adoption de cet article, après avoir adopté plusieurs amendements supprimant l'obligation d'assermentation des agents de l'ANSSI, que les députés avaient rétablie, précisant le délai de suppression des informations non pertinentes et prévoyant que le décret en Conseil d'État définissant les modalités d'application de cet article serait soumis pour avis à la CNCTR.

1. Les compétences actuelles de l'ANSSI : des moyens de détection de cyber-attaques et d'information des victimes encore insuffisants

1.1 Les moyens de l'ANSSI pour détecter des cyber-attaques sur les systèmes d'information des autorités publiques et des opérateurs stratégiques

Adopté lors de la dernière loi de programmation militaire[1], l'article L. 2321-2-1 du code de la défense permet à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de mettre en œuvre, sur les réseaux de communication électroniques exploités par les opérateurs de

[1] *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*

communication électroniques (OCE), les hébergeurs ou les fournisseurs d'accès Internet, des dispositifs mettant en œuvre **des marqueurs techniques** afin de détecter des évènements susceptibles **d'affecter la sécurité des systèmes d'information des autorités publiques, des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE).** Ces marqueurs techniques, définis à l'article R. 2321-1-3 du code de la défense comme des « *éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante ou d'identifier une menace* », ne peuvent être exploités que pour une durée utile et dans la mesure strictement nécessaire à la caractérisation de la menace. Par l'intermédiaire de ces dispositifs exploitants les marqueurs techniques, assimilés à des sondes, l'ANSSI peut analyser les données techniques pertinentes pour caractériser la menace. Aux termes 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 contrôler la bonne application de ces dispositions.

Toutefois, la collecte de ces seules données techniques n'est pas suffisante pour pouvoir face faire aux menaces croissantes et aux modes opératoires de plus en plus complexes des cyberattaques. En effet, ces marqueurs techniques ne représentent qu'une faible partie des données du flux d'un réseau ciblé, et permettent seulement d'obtenir les flux entrants et sortants vers une machine affectée, c'est-à-dire de savoir avec quelles autres machines l'attaquant communique et la méthode de communication utilisée. Ainsi, l'ANSSI n'a aujourd'hui accès qu'aux effets et aux conséquences des activités malveillantes, et non à leurs causes (qui sont présentes dans des données de code, de logs ou de contenu stocké). Les données sont donc **trop limitées pour pouvoir connaître en amont les modes opératoires utilisés par les attaquants, les analyser et en tirer des marqueurs spécifiques afin de les détecter**.

S'il apparaît dans l'étude d'impact que la rédaction issue de la loi de programmation militaire de 2018 avait pour intention de donner accès à l'ANSSI aux contenus des flux, l'interprétation du texte qui en a été faite *a posteriori* a restreint la collecte aux seules données techniques, et non aux données présentes sur l'intégralité du flux ciblé.

1.2 Les capacités de détection des menaces sur les réseaux des opérateurs de communication électroniques

Également issu de la dernière loi de programmation militaire du 13 juillet 2018, l'article L. 33-14 du code des postes et des communications électroniques (CPCE) ouvre **la faculté, pour un opérateur de communication électronique** (OCE), après en avoir informé l'ANSSI, d'employer des dispositifs mettant en œuvre **des marqueurs techniques sur ses réseaux**, sans s'intéresser au contenu, afin de détecter des évènements susceptibles d'affecter la sécurité des systèmes d'exploitation de l'ensemble de ses abonnés.

Des modalités d'échanges techniques entre les OCE et l'ANSSI ont également été mises en place par cet article et le second alinéa de l'article L. 2321-3 du code de la défense. L'ANSSI peut en effet demander aux OCE d'exploiter ces systèmes de détection, **en leur fournissant des « marqueurs d'attaque » dont elle aurait déjà connaissance**, en d'autres termes des marqueurs techniques propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant. En cas d'attaque informatique similaire sur un OCE, leurs systèmes de détection produisent alors une alerte de sécurité contenant uniquement les informations techniques de l'attaque. **L'ANSSI est informée sans délai de cette alerte**, et peut demander aux OCE d'informer leurs abonnés d'une vulnérabilité ou d'une atteinte sur leur système. Si l'attaque malveillante **concerne une autorité publique, un OIV ou un OSE, elle peut alors demander des données techniques complémentaires,** strictement nécessaires à l'analyse de l'évènement et qui ne peuvent être exploitées qu'aux seules fins de caractériser la menace affectant la sécurité de ces systèmes.

Là encore, il appartient à l'ARCEP de contrôler le respect du recueil de données opérées par l'ANSSI à la suite d'une attaque détectée par un OCE.

Toutefois, si ce dispositif paraît permettre un renforcement général de la cybersécurité, notamment du fait du positionnement clé des OCE au sein du réseau mondial, **son caractère facultatif n'a permis de produire que peu d'effets** en termes de sécurisation des réseaux et de détection des cyberattaques.

1.3 L'obligation d'information de l'ANSSI par les OCE en cas de vulnérabilité ou d'attaque sur les systèmes d'information

L'article L. 2321-3 du code de la défense a octroyé à l'ANSSI la possibilité **d'enjoindre aux OCE de lui communiquer des informations** :

- elle peut demander l'identité, l'adresse postale et l'adresse électroniques d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, **aux seuls fins de les alerter sur la vulnérabilité ou l'atteinte des systèmes qu'ils utilisent ou possèdent**, et seulement pour les besoins de la sécurité des systèmes d'information des autorités publiques, des OIV ou des OSE ;

- comme indiqué *supra*, lorsqu'elle est informée par un OCE de l'existence d'un évènement affectant la sécurité des systèmes des autorités publiques, des OIV ou des OSE, elle peut demander à ces OCE des données techniques strictement nécessaires à l'analyse de l'évènement, qui ne peuvent être exploitées qu'aux seules fins de caractériser la menace affectant la sécurité de ces systèmes.

Il est précisé à ce même article L. 2321-3 que les agents de l'ANSSI à qui les OCE communiquent ces informations **doivent être spécialement habilités et assermentés**.

2. Le dispositif proposé par le projet de loi : renforcer les compétences de l'ANSSI en matière de détection des cyberattaques et d'information des victimes

En premier lieu, le présent article propose de remédier à la divergence d'interprétation relative aux données que l'ANSSI peut collecter afin de caractériser une menace portant sur les systèmes d'information des autorités publiques et des opérateurs d'importance. Il vient donc clarifier, mais également compléter la rédaction de l'article L. 2321-2-1 du code de la défense :

- à titre principal, il insère la possibilité pour l'ANSSI de **mettre en œuvre des dispositifs permettant de recueillir l'ensemble des données de flux sur un réseau,** et ainsi d'accéder aux données, métadonnées et **contenus** sur le réseau de différents opérateurs (alinéa 5) ;

- il inclut les **opérateurs de centres de données**, aux côtés des opérateurs de communications électroniques, des fournisseurs d'accès et des hébergeurs, **dans le périmètre des opérateurs sur les réseaux desquels l'ANSSI peut apposer un marqueur technique** ou **obtenir la copie des serveurs** (alinéa 3) ;

- enfin, il 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 évènements** susceptibles d'affecter la sécurité de leur système d'information (alinéa 6).

Le recueil de l'ensemble des données de contenus ne sera possible que s'il répond aux mêmes conditions que celles permettant la mise en place de dispositifs mettant en œuvre des marqueurs techniques, à savoir :

- lorsque l'ANSSI a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE) ;

- pour une durée et dans une mesure strictement nécessaire à la caractérisation de la menace et aux seules fins de détecter et de caractériser des évènements susceptibles d'affecter la sécurité des systèmes d'information des acteurs susmentionnés ;

- seuls les agents de l'ANSSI individuellement désignés et spécialement habilités peuvent procéder au recueil de ces données et à leur analyse, aux seules fins de prévenir et caractériser la menace.

Au regard du caractère privé des données pouvant être collectées *via* ce dispositif, l'accroissement des compétences de l'ANSSI s'accompagne également **d'une garantie supplémentaire,** puisqu'elle devra recueillir **un avis conforme *a priori* de l'ARCEP** avant de pouvoir mettre en place ce dispositif de recueil de données En outre, le projet de loi ramène **de 10 ans à 2 ans** le délai de conservation de l'ensemble des données pouvant être utiles à la prévention et la caractérisation des menaces**.**

En deuxième lieu, l'article 35 modifie l'article L. 33-14 du code des postes et des communications électroniques et supprime la faculté d'utilisation de dispositifs mettant en œuvre des marqueurs techniques pour les OCE afin de **la rendre obligatoire pour les seuls OCE désignés opérateurs d'importance vitale** (alinéas 21 et 22).

En troisième lieu, cet article prévoit de modifier l'article L. 2321-3 du code de la défense afin :

- d'étendre aux hébergeurs de données l'obligation de communiquer à l'ANSSI des données permettant d'identifier des victimes de systèmes vulnérables ou attaqués, ou des données techniques lors d'attaques sur des autorités publiques ou des opérateurs importants (alinéa 11) ;

- comme pour la modification à l'article L. 2321-2-1 précité, d'étendre aux alertes **sur un sous-traitant** d'une autorité publique, d'un OIV ou d'un OSE, **l'obligation de communication de données techniques** (alinéa 13) **;**

- de supprimer l'obligation d'assermentation des agents de l'ANSSI, déjà spécialement habilités pour pouvoir recueillir et analyser les données transmises (alinéa 11).

Toutefois, lors de l'examen du projet de loi, l'Assemblée nationale a souhaité **maintenir cette obligation d'assermentation** des agents de l'ANSSI, dans laquelle elle a vu une garantie supplémentaire à celle apportée par la procédure d'habilitation.

3. La position de la commission : de nouveaux moyens d'action bienvenus et proportionnés aux objectifs poursuivis

Cet article appelle plusieurs observations de la part de la commission.

En premier lieu, au regard de l'importance des flux qui transitent sur les OCE désignés opérateurs d'importance vitale, les finalités poursuivies par la modification de l'article L. 33-14 du code des postes et des communications sont pertinentes. En particulier, la mise en place d'une obligation de pose de dispositifs mettant en œuvre des marqueurs techniques en cas de menace doit permettre d'améliorer significativement la détection d'attaques sur ces serveurs, et la compréhension de celles-ci par l'ANSSI. La commission souligne que le dispositif ne s'appliquera que sur un

périmètre d'opérateurs restreint. Elle approuve par ailleurs les mesures d'indemnisation pour les surcoûts liés à la mise en œuvre de cette mesure.

Concernant les modifications apportées aux articles L. 2321-2-1 et L. 2321-3 du code de la défense, la commission des lois a examiné avec précaution les dispositifs proposés et les garanties associées, l'étude d'impact relevant elle-même que le recueil d'informations sans l'accord de celui concerné, et son exploitation sont « *manifestement de nature à porter atteinte à différents droits constitutionnellement garantis – plus particulièrement au droit au respect de la vie privée, 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* ». Suivant la position du Conseil d'État, la commission a estimé que **ces atteintes étaient nécessaires et justifiées au regard des objectifs d'intérêt général poursuivis par ces dispositions, l'ANSSI ayant pour mission de prévenir et caractériser les menaces visant les systèmes d'information des autorités publiques ou des opérateurs d'importance vitale**, avec des demandes sur un périmètre restreint et pour une durée limitée.

En deuxième lieu, concernant la modification de l'article L. 2321-3 du code de la défense et des conditions d'information de l'ANSSI par les alinéas 11 et 13 de l'article 35, la commission relève le caractère mesuré et justifié de l'extension aux hébergeurs de données de l'obligation de communication d'informations à l'ANSSI , notamment au regard de l'importance pris par le *cloud* dans les systèmes d'information ces dernières années.

En revanche, la commission a considéré que **le dispositif d'assermentation obligatoire des agents de l'ANSSI, rétabli à l'Assemblée nationale, créait une contrainte procédurale importante**, tant pour les services de l'ANSSI que pour les magistrats et services du tribunal judiciaire chargés de recevoir le serment, **sans apporter de garantie complémentaire, les agents concernés devant déjà être dûment habilités** pour exercer leurs missions et étant, du fait de leur statut, déjà soumis à une obligation de secret professionnel et de discrétion professionnelle. Elle rappelle à cet égard que l'assermentation est une garantie exigée pour les agents dont la mission est la recherche ou la poursuite d'infractions pénales, ce qui ne correspond pas aux missions de l'ANSSI qui exploite les informations collectées auprès des OCE afin d'**identifier et d'informer les victimes**.

A l'initiative du rapporteur, la commission a donc adopté un amendement (**COM-140**) visant à **revenir à la lettre initiale du projet de loi et à supprimer l'obligation d'assermentation de ces agents**.

Enfin, concernant l'extension des données pouvant être recueillies par l'ANSSI et la modification de l'article L. 2321-2-1 du code de la défense par les alinéas 3 à 6 de l'article 35, la commission a considéré que les garanties entourant le dispositif, notamment **les contrôles *a priori* et *a posteriori* effectués par l'ARCEP** sur les nouvelles compétences en matière

de recueil de données, la réduction du délai de conservation des données de 10 à 2 ans, étaient suffisamment solides pour que l'atteinte ne soit pas disproportionnée. Cependant, au regard des données sensibles collectées, elle a considéré, comme pour l'article 32 du présent projet de loi, que la mention d'une **suppression « sans délai » des données non pertinentes était trop imprécise** et a considéré que la définition d'un délai fixe était nécessaire pour permettre à l'ARCEP d'effectuer un contrôle utile sur la mise en œuvre des dispositions par l'ANSSI. Elle a ainsi complété le projet de loi pour prévoir que ce délai, qui sera nécessairement bref, sera précisé par voie réglementaire (**amendement COM-138 du rapporteur**).

La commission a également adopté un **amendement du rapporteur COM-139** afin que le décret d'application en Conseil d'État soit pris après un avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

La commission a donné un avis favorable à l'adoption de l'article 35 **ainsi modifié.**

EXAMEN EN COMMISSION

_____

MARDI 13 JUIN 2023

- Présidence de Mme Catherine Di Folco, vice-présidente -

Mme Catherine Di Folco, présidente. – Nous commençons nos travaux par l'examen du rapport pour avis sur le projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.

M. François-Noël Buffet, rapporteur pour avis. – Le projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, dont la commission des affaires étrangères, de la défense et des forces armées est saisie au fond, est d'abord une loi de programmation budgétaire destinée à renforcer les capacités de nos forces armées.

À ce titre, nous pouvons nous féliciter que les trois services de renseignement relevant du ministère des armées – la direction générale de la sécurité extérieure (DGSE), la direction du renseignement et de la sécurité de la défense (DRSD) et la direction du renseignement militaire (DRM) voient leurs effectifs augmenter et leurs investissements immobiliers et opérationnels financés.

Nous ne sommes donc pas, à l'égard de nos services de renseignement, dans une situation de difficulté de moyens financiers ou d'emplois budgétaires, mais, dans certains cas, en dépit de nos besoins, nous ne parvenons pas à recruter.

Notre commission ne s'est pas saisie pour avis du volet budgétaire du texte, mais de certaines des « diverses dispositions intéressant la défense » : les dispositions concernant les services de renseignement, les dispositions relatives à la sécurité des systèmes d'information et le régime de protection contre les drones malveillants.

Ces dispositions, pour l'essentiel très ponctuelles et techniques, s'inscrivent dans le prolongement des textes antérieurs, que ce soit la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, dite loi « Silt », et la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Mais on peut également souligner que le projet de loi ne comporte aucune disposition visant à renforcer le contrôle des services de renseignement, et ce alors même que l'équilibre entre l'extension des pouvoirs des services et les instruments de contrôle est essentiel à la conformité de notre régime aux exigences constitutionnelles en matière de

protection des libertés et à la jurisprudence européenne. Les amendements que je vous proposerai, en accord avec les autres membres de la délégation parlementaire au renseignement (DPR) représentant le Sénat, à savoir Agnès Canayer, le président Christian Cambon, et Yannick Vaugrenard, entendent porter certaines avancées en ce domaine. Nous déposons, tous les quatre, des amendements identiques, manifestant ainsi la volonté unitaire du Sénat de progresser quant aux pouvoirs octroyés à la DPR.

Quatre articles concernent les services de renseignement.

L'article 19 autorise les services chargés des enquêtes administratives à consulter le bulletin n° 2 du casier judiciaire afin de mieux mesurer les vulnérabilités, voire les risques posés par des personnes susceptibles d'être recrutées ou d'avoir accès à des lieux ou informations protégés.

L'article 21 permet la transmission d'informations figurant dans une procédure judiciaire ouverte pour crime contre l'humanité ou de crime de guerre afin de renforcer la capacité des services à traiter l'évolution de la menace pesant sur la France et sur ses intérêts.

L'article 22 renforce la protection des anciens agents et membres des unités spéciales en leur garantissant l'anonymat lors de leur témoignage dans une procédure judiciaire, dans les mêmes conditions qu'à ceux qui sont actuellement en activité.

Ces mesures n'appellent pas de modification de notre part.

L'article 20, quant à lui, est plus ambitieux. Il marque la volonté de lutter contre les ingérences étrangères et de protéger les intérêts supérieurs de la France. Il met en place un mécanisme de contrôle des activités exercées par les militaires ou anciens militaires et par certains personnels civils ayant occupé des fonctions d'une sensibilité particulière et souhaitant exercer une activité lucrative pour le compte d'un État étranger ou d'une entreprise étrangère ou sous contrôle étranger intervenant dans le domaine de la défense et de la sécurité. Il convient que notre pays soit vigilant à leur égard. Ce mécanisme est intéressant, même si sa portée sera nécessairement limitée. Il sera en effet difficile d'agir contre une personne exerçant à l'étranger avec un contrat de droit étranger, à moins qu'elle ne revienne en France. C'est d'ailleurs sans doute à ce moment-là qu'il faudra s'assurer de son activité à l'étranger, un peu plus que nous ne le faisons aujourd'hui. Je vous proposerai de préciser les modalités d'application de cet article s'agissant des personnels civils.

S'agissant de la sécurité des systèmes d'information, les articles 32 à 35 renforcent la capacité de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de détecter, d'identifier et de prévenir les attaques informatiques visant les systèmes d'information des autorités publiques, des opérateurs stratégiques ou de leurs sous-traitants.

En ce sens, l'article 32 dote l'ANSSI de la possibilité d'enjoindre aux acteurs du numérique de filtrer ou de rediriger les noms de domaine utilisés par des cyberattaquants en cas de menace pour la défense et la sécurité nationales. Cela permettra à l'ANSSI de neutraliser les noms de domaine de façon à ce qu'ils n'atteignent pas leur cible, ou de saisir le nom de domaine utilisé et de le déporter de façon à observer le mode opératoire employé.

L'article 33 permet de recevoir communication des données de cache – c'est-à-dire l'ensemble des historiques de recherche d'un site – non identifiantes, afin de mieux comprendre les modes opératoires des attaquants.

Enfin, l'article 35 étend à plusieurs titres les données pouvant être recueillies par l'ANSSI. Il rend notamment obligatoire la mise en place de capacités de détection chez les opérateurs de communication électronique d'importance vitale, et supprime l'assermentation des agents de l'ANSSI habilités à analyser les données recueillies.

En outre, les dispositions prévoient de renforcer l'information des victimes des cyberattaques. À cette fin, l'article 34 oblige les éditeurs de logiciels à notifier à l'ANSSI et aux utilisateurs concernés les incidents et vulnérabilités significatives susceptibles de compromettre la sécurité de leurs produits, tandis que l'article 35 élargit aux hébergeurs de données l'obligation de communiquer à l'ANSSI les informations concernant des utilisateurs ou détenteurs de systèmes d'information vulnérables ou attaqués afin de les en informer.

Je vous proposerai de clarifier la rédaction retenue et d'ajuster les dispositifs afin de les rendre pleinement opérationnels, notamment pour que l'ensemble des utilisateurs d'un logiciel présentant une vulnérabilité critique soient informés par l'éditeur de cette dernière, et pas uniquement les seuls utilisateurs professionnels, comme le prévoit le texte issu des travaux de l'Assemblée nationale. Les particuliers peuvent aussi être victimes et donc en droit d'être informés.

S'agissant enfin du régime de lutte contre les drones malveillants, l'article 27 du projet de loi vise à doter les services de l'État des moyens de parer sans délai à une menace imminente pour l'ordre public, la sécurité et la défense nationales ou le service public de la justice, en les autorisant à recourir à tout moyen permettant de « neutraliser » un drone qui représente une menace – cela peut aller jusqu'à la destruction du drone. Il me paraît nécessaire de renforcer les garanties en matière de protection du droit de propriété et du droit à informer. En effet, la plupart du temps, ces moyens seront mis en œuvre alors que le drone se trouve dans une zone de survol interdit à titre temporaire ou permanent – centrale nucléaire, grand événement sportif, etc. Que le drone soit « neutralisé » alors qu'il se trouve dans une zone interdite de survol ne me paraît pas soulever de difficulté de principe. Mais le dispositif n'exclut pas que ces moyens puissent également

être mis en œuvre dans une zone dans laquelle la circulation du drone est autorisée. Je vous propose donc de renvoyer à un décret en Conseil d'État la définition des conditions dans lesquelles, en cas de menace imminente, les moyens de neutralisation seront mis en œuvre, en particulier dans cette hypothèse.

J'en viens maintenant aux trois amendements portant articles additionnels que j'ai évoqués précédemment. Deux de ces amendements concernent les pouvoirs de la DPR et ses liens avec la Commission nationale de contrôle des techniques de renseignement (CNCTR), tandis que le troisième vise les pouvoirs de la CNCTR.

Ces amendements tendent à garantir que, lorsque des sujets d'actualité concernant une action des services de renseignement sont révélés par la presse et ont été admis par le Gouvernement, ceux-ci pourront faire l'objet d'une information de la DPR. Je rappelle que la DPR et ses membres sont soumis au secret le plus absolu. Il arrive parfois, comme ce fut le cas l'année dernière, que la presse révèle au grand public des opérations dans lesquelles des moyens mis à disposition par nos services ont été utilisés à d'autres fins. La possibilité pour la DPR d'auditionner les ministres compétents faisait débat. Au début de cette année, le chef de l'État a rendu un arbitrage sur ce point, que nous traduisons ici pour consacrer ce pouvoir de la DPR – c'est une avancée importante.

Ces amendements permettent également de renforcer les liens entre la DPR et la CNCTR en prévoyant la présentation à la DPR d'un bilan annuel des recommandations de la commission, ainsi que son information sur les saisines du procureur de la République dans le cadre du dispositif de lanceur d'alerte. La loi de juillet 2015 relative au renseignement donne aux lanceurs d'alerte la possibilité de signaler les faits qu'ils constatent et dénoncent à la CNCTR, à charge pour elle, tout en conservant l'anonymat de la saisine, de transmettre les informations aux autorités judiciaires. Nous souhaitons que la DPR soit informée de ces procédures.

Enfin, le troisième amendement tend à permettre l'accès immédiat de la CNCTR aux éléments collectés par les services de renseignement lors de la mise en œuvre des techniques les plus intrusives : la collecte des données informatiques, la captation d'image et de son et la destruction des données. Cette mesure est particulièrement nécessaire pour permettre l'efficacité du contrôle face au développement de ces techniques de renseignement, dont je souligne que nous ne contestons pas la légitimité.

Dans la même logique, afin d'éviter l'émiettement du contrôle, je vous proposerai trois amendements prévoyant que la CNCTR puisse donner un avis avant la prise des décrets renforçant les pouvoirs de l'ANSSI. En effet, si l'ANSSI n'est pas un service de renseignement, ses liens avec ceux-ci sont étroits et la nature de son intervention appelle un regard informé par la pratique de ces services.

Enfin, je vous présenterai un amendement tendant à supprimer, suivant la position constante du Sénat, la référence proposée à la création d'une délégation au renseignement économique, qui ne pourrait conduire qu'à une dispersion des moyens. La DPR peut parfaitement assurer un contrôle en matière économique – elle a d'ailleurs consacré l'un de ses rapports sur l'ingérence économique.

Un mot, enfin, sur un sujet qui va peser sur le cadre légal du renseignement. Nous savons que, selon toute vraisemblance, la France sera prochainement condamnée par la Cour européenne des droits de l'homme pour non-conformité à la convention européenne du régime encadrant les échanges d'informations entre les services français de renseignement et les services étrangers. Ce sujet étant sensible, il importe de trouver une solution acceptable par tous. Les discussions avancent, mais il ne nous revient pas ici de faire des propositions, afin de ne pas porter atteinte aux intérêts de la France. Une évolution législative doit intervenir dans les mois qui viennent.

Sous réserve des amendements que je vous soumettrai et qui viennent compléter et renforcer le texte, il m'apparaît que celui-ci comporte des mesures utiles pour les services de renseignement.

M. Jean-Yves Leconte. – Sur l'article 32, je comprends le rôle accordé à l'ANSSI dans des situations identifiées et immédiates. Toutefois, si la situation perdure est-il opportun que l'ANSSI garde la main au lieu de passer le relais à l'Arcom, qui est une autorité administrative indépendante ? Dans le cadre des relations avec les plateformes, il me semble préférable de centraliser plutôt que de multiplier le nombre de structures opérant dans l'interface.

Le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a vocation à identifier les ingérences étrangères sur les réseaux, mais nous déplorons qu'il n'ait pas les moyens de réagir. Cette loi de programmation va-t-elle lui donner des moyens supplémentaires ?

Je formulerai enfin une remarque concernant les échanges d'informations avec les services étrangers. Les décisions de la CEDH ont déjà été évoquées il y a deux ans, mais la discussion a été reportée. Aujourd'hui, si d'autres services dans d'autres pays occidentaux sont soumis aux mêmes contraintes, alors il devient nécessaire d'évoluer afin de ne pas bloquer nos capacités d'échanges. Avez-vous des assurances du Gouvernement en la matière ?

M. Philippe Bas. – Je remercie le rapporteur pour les amendements qu'il nous propose d'adopter, en particulier ceux qui visent à renforcer les pouvoirs de la DPR. C'est un sujet que nous traitons depuis plusieurs années puisque nous avions adopté, il y a cinq ans, contre l'avis du Gouvernement, des amendements, présentés par le président de la commission des affaires étrangères et de la défense et le président de la commission des lois, visant à

aligner les pouvoirs de la DPR sur ceux des institutions équivalentes de grands pays démocratiques comme la Grande-Bretagne ou l'Allemagne. Ces dispositions n'ont pas été reprises dans le texte final adopté par le Parlement. Les dispositions qui nous sont aujourd'hui proposées sont certes plus modestes, mais elles ont le mérite de nous faire espérer qu'elles entreront en vigueur. C'est la raison pour laquelle je les soutiendrai.

Les services de renseignement sont des administrations et, en vertu de l'article 15 de la Déclaration des droits de l'homme et du citoyen, elles n'échappent pas au contrôle parlementaire. Néanmoins, l'efficacité de leur mission exige, dans l'intérêt de la Nation, que le secret de leurs méthodes et de leurs investigations soit préservé. C'est la raison pour laquelle a été créée, au début du XXIe siècle, une délégation spécifique, qui a l'originalité d'être composée de députés et de sénateurs. Cette délégation ne peut bien faire son travail que si elle inspire confiance aux services de renseignement. Elle est assujettie au secret de la défense nationale. Il faut toutefois que la confiance soit réciproque. Or la liste des informations que la DPR est susceptible d'obtenir est très restreinte par rapport à ce qu'elle est dans d'autres pays. Les services de renseignement invoquent la sécurité nationale. Or le contrôle parlementaire ne doit pas apparaître insuffisant aux yeux de nos concitoyens. La confiance que nous cherchons à entretenir avec ces services ne doit pas nous faire oublier l'exigence d'un contrôle parlementaire, car ces derniers recourent à des technologies intrusives, qui pourraient porter atteinte aux libertés individuelles et au secret de la vie privée.

Voilà pourquoi cette évolution est nécessaire, car nous n'avons pas encore atteint le point ultime du contrôle parlementaire de l'activité de ces services.

M. Alain Richard. – Je veux rebondir sur le propos de Philippe Bas. Aucun pays ne dispose d'une capacité de renseignement intégrale et infinie. La coopération et les échanges d'informations sont forcément nécessaires. L'expérience m'a appris que plus le contrôle parlementaire est intrusif, moins le service fournit d'informations et moins il en reçoit. Il importe donc de maintenir la valeur relative des services de renseignement français, qui bénéficient, me semble-t-il, de la confiance de leurs pairs. L'intensité de ce lien de confiance, facteur d'efficacité et de sécurité, n'est pas compatible avec une intensité excessive du contrôle parlementaire, comme c'est le cas en Allemagne.

Mme Agnès Canayer. – Je félicite le rapporteur d'avoir cherché à parvenir à un équilibre : il faut donner des marges de manœuvre aux services de renseignement pour leur permettre de collecter des informations, tout en contrôlant le respect des règles et des libertés individuelles. Je veux rappeler la force des liens, au sein de la DPR, entre les deux assemblées, comme en attestaient les amendements déposés conjointement lors de l'examen de la loi de 2021. Je me félicite donc des avancées proposées, même si elles sont modestes.

Par ailleurs, avec l'évolution des technologies, auxquelles recourent les cybercriminels, les groupes de criminalité organisée, les terroristes, il importe de renforcer le rôle de l'ANSSI.

M. François-Noël Buffet, rapporteur pour avis. – Monsieur Leconte, je rappelle que la mission de l'ANSSI est de documenter les modalités d'attaque, et d'assurer la sécurité des systèmes d'information en protégeant ceux des autorités publiques et des opérateurs stratégiques, ce qui est très différent de la mission de l'Arcom. Il ne faut pas oublier que ce travail se fait sous le contrôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). De plus, le nombre de cas n'est pas très important.

Les services de l'ANSSI participent au travail de coordination de Viginum. Viginum attribue l'attaque, alors que l'ANSSI travaille en amont. Leurs tâches sont différentes, mais leur collaboration essentielle.

M. Jean-Yves Leconte. – Viginum identifie les ingérences, mais ne dispose pas des moyens de faire de la contre-ingérence.

M. François-Noël Buffet, rapporteur pour avis. – Tel n'est pas le rôle de Viginum. La décision est prise au niveau gouvernemental.

Concernant les échanges avec les services étrangers, nous n'éludons pas le sujet, nous connaissons les besoins, mais il convient d'élaborer un texte spécifique : la DPR doit travailler pour ce faire en collaboration avec le Gouvernement.

Enfin, s'agissant des pouvoirs de la DPR, je comprends la nécessité d'aller plus loin, mais la DPR entretient aujourd'hui une relation étroite avec la CNCTR ; les membres de la DPR remplissent la mission de contrôle dont ils ont la charge. Il faut qu'elle saisisse les moyens qui sont les siens pour exercer ce contrôle. Ce texte permet une avancée supplémentaire, nous irons sans doute plus loin encore dans les années à venir.

EXAMEN DES AMENDEMENTS DU RAPPORTEUR

Article 2

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-141 a pour objet de supprimer la mention de la création d'une délégation parlementaire à la sécurité économique.

L'amendement COM-141 est adopté.

Article 20

L'amendement rédactionnel COM-126 *est adopté.*

Après l'article 22

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-127 prévoit l'accès immédiat de la CNCTR aux éléments collectés par les services de renseignement lors de la mise en œuvre des techniques les plus intrusives.

L'amendement COM-127 portant article additionnel est adopté.

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-128 tend à renforcer le droit à l'information de la délégation parlementaire au renseignement et à lui communiquer un bilan annuel des recommandations présenté par la Commission nationale de contrôle des techniques de renseignement.

L'amendement COM-128 portant article additionnel est adopté.

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-129 assure une coordination avec les missions de la CNCTR.

L'amendement COM-129 portant article additionnel est adopté.

Article 27

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-130 porte sur le contrôle des drones.

L'amendement COM-130 est adopté.

Article 32

L'amendement rédactionnel COM-131 *est adopté.*

M. François-Noël Buffet, rapporteur pour avis – L'amendement COM-132 tend à supprimer une mention inutile et incomplète.

L'amendement COM-132 est adopté.

M. François-Noël Buffet, rapporteur pour avis – L'amendement COM-133 vise à préciser la notion de « bref délai » par voie réglementaire.

L'amendement COM-133 est adopté.

M. François-Noël Buffet, rapporteur pour avis – L'amendement COM-134 prévoit que la CNCTR soit saisie pour avis du projet de décret d'application de cet article.

L'amendement COM-134 est adopté.

Article 33

L'amendement rédactionnel, d'harmonisation et de précision COM-135 est *adopté.*

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-136 prévoit également que la CNCTR soit saisie pour avis du projet de décret d'application de cet article.

L'amendement COM-136 est adopté.

Article 34

M. François-Noël Buffet, rapporteur pour avis. – L'article 34 crée une double obligation pour les éditeurs de logiciels, afin qu'ils informent l'ANSSI et les utilisateurs d'incidents ou de la vulnérabilité de leurs produits. L'amendement COM-137 rétablit l'obligation initialement prévue d'informer l'ensemble des utilisateurs de logiciels, préalablement supprimée à l'Assemblée nationale, et non plus seulement les professionnels.

L'amendement COM-137 est adopté.

Article 35

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-138 prévoit que les données recueillies par l'Arcep soient détruites « dans un délai bref, précisé par voie réglementaire », et non pas « sans délai ».

L'amendement COM-138 est adopté.

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-139 concerne également la saisine de la CNCTR pour avis sur le décret d'application de cet article.

L'amendement COM-139 est adopté.

M. François-Noël Buffet, rapporteur pour avis. – L'amendement COM-140 vise à supprimer l'assermentation des agents de l'ANSSI, l'habilitation, déjà existante, étant suffisante pour leurs missions.

L'amendement COM-140 est adopté.

La commission a adopté les amendements suivants du rapporteur :

Auteur	N°	Objet	Sort de l'amendement
Article 2 (rapport annexé)			
M. BUFFET, rapporteur pour avis	COM-141	Suppression de la référence dans le rapport annexé à la création d'une délégation parlementaire à la sécurité économique	**Adopté**
Article 20			
M. BUFFET, rapporteur pour avis	COM-126	Précision que les conditions dans lesquelles l'obligation de déclaration créée par l'article 20 pourra être étendue à certains agents civils de l'État et de ses établissements publics participant au développement de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires devront être définies par décret en Conseil d'État.	**Adopté**
Après l'article 22			
M. BUFFET, rapporteur pour avis	COM-127	Renforcement des pouvoirs de contrôle de la Commission nationale de contrôle des techniques de renseignement (CNCTR)	**Adopté**
M. BUFFET, rapporteur pour avis	COM-128	Préciser et compléter le droit à l'information de la délégation parlementaire au renseignement	**Adopté**
M. BUFFET, rapporteur pour avis	COM-129	Coordination des compléments d'information de la délégation parlementaire au renseignement avec les missions de la CNCTR	**Adopté**
Article 27			
M. BUFFET, rapporteur pour avis	COM-130	Renvoi des conditions de mise en œuvre de cet article à un décret en Conseil d'Etat	**Adopté**
Article 32			
M. BUFFET, rapporteur pour avis	COM-131	Rédactionnel	**Adopté**
M. BUFFET, rapporteur pour avis	COM-132	Amendement supprimant une mention incomplète et non nécessaire	**Adopté**
M. BUFFET, rapporteur pour avis	COM-133	Amendement de précision du délai de suppression de données non pertinentes	**Adopté**
M. BUFFET, rapporteur pour avis	COM-134	Avis de la CNCTR sur le décret d'application	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Article 33			
M. BUFFET, rapporteur pour avis	COM-135	Amendement de clarification et d'harmonisation	**Adopté**
M. BUFFET, rapporteur pour avis	COM-136	Avis de la CNCTR sur le décret d'application	**Adopté**
Article 34			
M. BUFFET, rapporteur pour avis	COM-137	Rétablissement de l'information par les éditeurs de logiciels à l'ensemble des utilisateurs	**Adopté**
Article 35			
M. BUFFET, rapporteur pour avis	COM-138	Amendement de précision du délai de suppression de données non pertinentes	**Adopté**
M. BUFFET, rapporteur pour avis	COM-139	Avis de la CNCTR sur le décret d'application	**Adopté**
M. BUFFET, rapporteur pour avis	COM-140	Suppression de l'assermentation des agents de l'ANSSI au profit de leur seule habilitation.	**Adopté**

LISTE DES PERSONNES ENTENDUES PAR LE RAPPORTEUR POUR AVIS

Ministère des armées - Direction des affaires juridiques (DAJ)

Mme Laurence Marion, directrice

M. Vincent Droullé, chef de service, adjoint à la directrice

M. Mathieu Rhée, sous-directeur adjoint du droit public et du droit privé

Agence nationale de la sécurité des systèmes d'information (ANSSI)

M. Vincent Strubel, directeur général

Commission nationale de contrôle des techniques de renseignement (CNCTR)

M. Serge Lasvignes, président

Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Mme Julie Holveck, conseillère juridique

M. Gwénaël Jézéquel, conseiller « institutions »

Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)

Mme Cécile Dubarry, directrice générale

M. Olivier Delclos, directeur de la direction « Internet, Presse, Postes et utilisateurs »

LA LOI EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, le tableau synoptique de la loi en construction est disponible sur le site du Sénat à l'adresse suivante :

https://www.senat.fr/dossier-legislatif/pjl22-712.html