N° 690

SÉNAT

SESSION ORDINAIRE DE 2020-2021

Enregistré à la Présidence du Sénat le 15 juin 2021

AVIS

PRÉSENTÉ

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la **prévention** *d'***actes** *de* **terrorisme** *et au* **renseignement***,*

Par M. Olivier CIGOLOTTI,

Sénateur

(1) Cette commission est composée de : M. Christian Cambon*, président ;* MM. Pascal Allizard, Olivier Cadic, Olivier Cigolotti, Robert del Picchia, André Gattolin, Guillaume Gontard, Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Cédric Perrin, Gilbert Roger, Jean-Marc Todeschini*, vice-présidents ;* Mmes Hélène Conway-Mouret, Joëlle Garriaud-Maylam, MM. Philippe Paul, Hugues Saury*, secrétaires ;* MM. François Bonneau, Gilbert Bouchet, Mme Marie-Arlette Carlotti, MM. Alain Cazabonne, Pierre Charon, Édouard Courtial, Yves Détraigne, Mme Nicole Duranton, MM. Philippe Folliot, Bernard Fournier, Mme Sylvie Goy-Chavent, M. Jean-Pierre Grand, Mme Michelle Gréaume, MM. André Guiol, Alain Houpert, Mme Gisèle Jourda, MM. Alain Joyandet, Jean-Louis Lagourgue, Ronan Le Gleut, Jacques Le Nay, Mme Vivette Lopez, MM. Jean-Jacques Panunzi, François Patriat, Gérard Poadja, Mme Isabelle Raimond-Pavero, MM. Stéphane Ravier, Bruno Sido, Rachid Temal, Mickaël Vallet, André Vallini, Yannick Vaugrenard, Richard Yung.

Voir les numéros :

Assemblée nationale (**15**ème législ.) : **4104**, **4185** et T.A. **622**

Sénat : **672** et **685** (2020-2021)

SOMMAIRE

Pages

L'ESSENTIEL

Depuis 2015, la lutte contre le terrorisme a particulièrement mobilisé la justice, la police et les services de renseignement. Les armées y ont également pris une part très importante, que ce soit au Levant avec l'opération *Chammal*, au Sahel avec Barkhane ou sur le territoire national avec l'opération *Sentinelle*.

Ainsi, le concept de continuum de sécurité-défense est-il devenu plus concret que jamais, en réponse à une menace terroriste continuellement élevée. Parallèlement, les services de renseignement continuent à poursuivre les six autres finalités fixées par la loi. En particulier, il leur faut s'adapter à des acteurs de la criminalité organisée faisant constamment évoluer leurs méthodes et à des États « décomplexés » mettant en œuvre toute les techniques possibles, de l'espionnage « classique » au cyber, en passant par la désinformation.

Dans ce contexte, les dispositions du présent projet de loi relatives au renseignement, inscrites dans les articles 7 à 19 dont la commission des affaires étrangères, de la défense et des forces armées s'est saisie pour avis, visent à permettre aux services de rester dans la course technologique, tout en encadrant leurs nouvelles prérogatives selon les principes et les procédures fixés par la loi du 24 juillet 2015.

I. UNE ADAPTATION DU CADRE LÉGISLATIF AUX ÉVOLUTIONS DES TECHNOLOGIES SANS REMISE EN CAUSE DES PRINCIPES FONDAMENTAUX

L'ensemble des missions des services de renseignement s'inscrivent dans **un cadre législatif qui s'efforce de protéger les libertés publiques tout en préservant l'efficacité de leur action**. Ce cadre a été construit progressivement au cours des dernières années. Ainsi, aux lois du 10 juillet 1991 encadrant les interceptions de sécurité (les « écoutes ») et du 9 octobre 2007 créant la délégation parlementaire au renseignement (DPR), a succédé **la loi du 24 juillet 2015 relative au renseignement. Elle définit et encadre les principales techniques de renseignement** et a transformé la Commission nationale de contrôle des interceptions de sécurité (CNCIS) en une commission nationale de contrôle des techniques de renseignement (CNCTR), dotée de prérogatives étendues. Cette loi a constitué une avancée considérable en construisant **un cadre législatif exhaustif fondé sur le principe « une finalité, une technique, un service »**. Ce cadre juridique est complexe par nécessité, mais la DPR, dans son rapport annuel pour 2020, a estimé qu'il était désormais **bien assimilé par les services,** comme le montre la baisse tendancielle du taux d'avis défavorables prononcés par la CNCTR.

Évolution du taux d'avis défavorables rendus par la CNCTR

	2016	2017	2018	2019
Taux d'avis défavorables (hors accès en temps différé aux données de connexion)	6,9 %	3,6 %	2,1 %	1,4 %
Taux d'avis défavorables (accès en temps différé aux données de connexion uniquement)	0,14 %	0,3 %	0,3 %	0,2 %

Source : Délégation parlementaire au renseignement sur la base des données transmises par la CNCTR.

Les textes suivants ont constitué de simples adaptations sur des points ponctuels, ne remettant nullement en cause l'essentiel de cette architecture. La loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales est venue préciser le cadre légal des techniques de surveillance internationale ; la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a remédié à la censure constitutionnelle de la surveillance des communications radio. Enfin, la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 a élargi les conditions d'exploitation des données recueillies dans le cadre des techniques de surveillance internationale visant des personnes disposant d'un identifiant rattachable au territoire national.

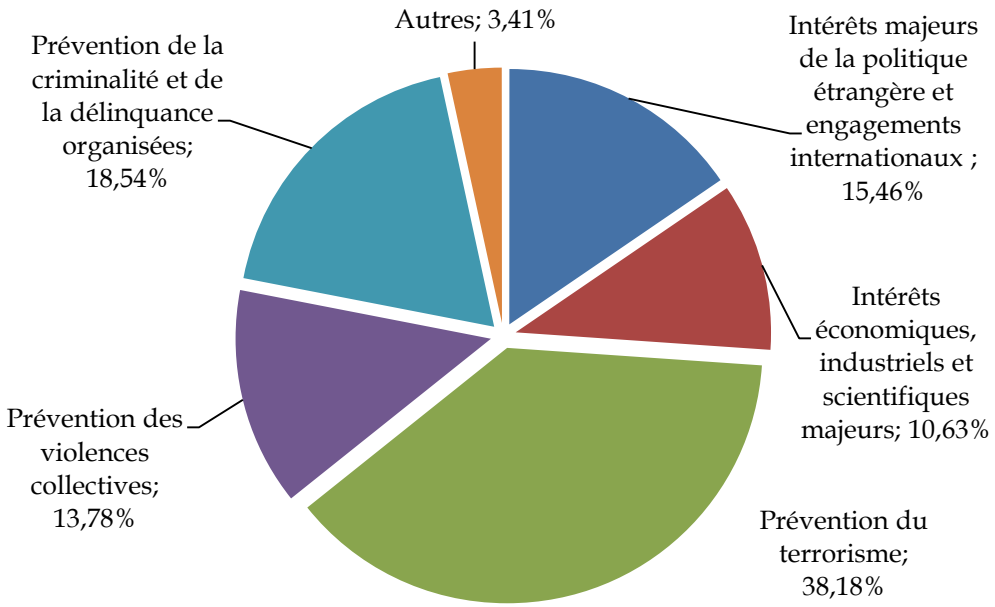
Le texte s'inscrit pleinement dans la continuité des dispositions de la loi du 24 juillet 2015.

Le nouveau projet de loi vise à assurer l'adaptation des moyens dont disposent les services aux dernières évolutions technologiques, comme **l'expansion des communications satellitaires** et la mise en place de la **5G** téléphonique. Il permet également de répondre aux exigences formulées par le Conseil d'Etat dans sa décision *French Data Network* du 21 avril 2021, lui-même pris à la suite de la décision de la CJUE du 21 décembre 2016 dite *Tele2 Sverige*, en matière de conservation des données techniques de connexion des opérateurs de télécommunication.

II. DE NOUVELLES TECHNIQUES DE RENSEIGNEMENT POUR SUIVRE LES ÉVOLUTIONS TECHNOLOGIQUES

Les techniques de renseignement sont encadrées par la loi du 24 juillet 2015, qui prévoit un avis préalable de la CNCTR. Elles sont mises en œuvre pour les finalités suivantes :

Répartition des demandes de techniques de renseignement par finalité en 2019 (toutes finalités confondues)



Source : Délégation parlementaire au renseignement, sur la base des données fournies par la CNCTR

Le projet de loi prévoit un certain nombre d'innovations et d'adaptations de ces techniques afin de faire face à de nouveaux enjeux.

A. L'ENJEU ESSENTIEL DU SATELLITAIRE

Une véritable révolution est en cours dans le domaine des communications satellitaires. **Des constellations regroupant parfois plusieurs milliers de satellites** vont être déployées dans les toutes prochaines années, ainsi *Starlink* de *Space X*, avec plus de 4 000 satellites dans un premier temps et *Kuiper* d'*Amazon*, qui regroupera également des milliers d'unités.

Ces satellites permettront aux personnes souhaitant améliorer leur connexion à internet dans des zones mal desservies par les opérateurs traditionnels, **mais également aux criminels ou aux terroristes, de contourner les moyens classiques de communication, échappant ainsi aux**

techniques d'interception habituelles des services. Ainsi ce type de communication est-il déjà mis en œuvre sur le territoire national en Guyane par des orpailleurs, mais aussi en mer ou dans la bande sahélo-saharienne. Les faisceaux de ces satellites peuvent être concentrés sur un carré de moins de 100 km à l'intérieur du territoire national.

Le caractère inéluctable du développement de cette technique rendait indispensable la création d'un cadre juridique. L'interception satellitaire est encore largement expérimentale. Le défi est notamment de pouvoir cibler le plus précisément possible les personnes suspectées. Le caractère intrusif de cette technique justifie les garanties importantes prévues par le texte : expérimentation pendant 4 ans, caractère subsidiaire (la technique ne pourra être mobilisée qu'en cas d'impossibilité de réaliser des interceptions classiques), centralisation au GIC des interceptions réalisées, fixation d'un nombre maximal d'interceptions simultanées.

La commission a adopté **un amendement** précisant que dans un premier temps, s'agissant d'une expérimentation nécessitant des compétences technologiques de pointe et impliquant un spectre d'interception assez large, **cette technique ne serait ouverte qu'aux services du premier cercle.** Toutefois, si cet usage des satellites se généralisait, il faudrait alors veiller à ce que certains services du deuxième cercle, notamment au sein de la gendarmerie nationale, puissent la mettre en œuvre, sous peine de perdre toute efficacité dans leurs investigations.

B. LA NÉCESSITÉ DE S'ADAPTER À LA MISE EN PLACE DE LA « 5G »

La deuxième avancée relative aux techniques de renseignement consiste en la possibilité de solliciter les opérateurs de télécommunication lors de la mise en œuvre de la technique dite de l' « IMSI-catching ». Celle-ci permet actuellement de recueillir des données de connexion à proximité d'une personne ciblée par les services.

L'objectif de la nouvelle disposition est d'anticiper le déploiement de la 5G, qui aura pour effet de rendre temporaires les identifiants des téléphones portables, ces identifiants évoluant à une fréquence élevée et étant fournis par le réseau. Seul l'opérateur pourra ainsi relier ces identifiants aux abonnements ou téléphones utilisés. L'objectif de cette disposition est finalement de **garantir l'intérêt opérationnel des IMSI-catchers**, qui, sans cette adaptation, risquerait de disparaître totalement.

C. UNE EXTENSION DU CHAMP DES ALGORITHMES

Passer de l' « ancien monde » de la téléphonie au « nouveau monde » des IP et des URL

La troisième évolution relative aux techniques de renseignement concerne **l'extension du champ des « algorithmes » introduits par la loi de 2015**. Cette technique avait alors été créée à titre expérimental. Le champ d'application de cette expérimentation, d'emblée limité aux données téléphoniques, n'a pas permis d'obtenir de résultats décisifs. C'est pourquoi l'article 13, outre qu'il pérennise cette technique, **en étend l'application aux « URL », c'est-à-dire aux adresses des pages internet**. Cette évolution est, selon les services, susceptible de rendre les algorithmes plus efficaces. Elle permet en quelque sorte de passer de l' « ancien monde » de la téléphonie au « nouveau monde » des adresses IP et des URL.

Les garanties prévues par le texte pour encadrer cette extension sont importantes : **les algorithmes sont contrôlés par la CNCTR, qui dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies**. Pas plus qu'actuellement, les nouveaux algorithmes étendus aux URL ne permettront d'identifier les personnes. C'est seulement dans un second temps, si l'algorithme donne des résultats, que les services demanderont à la CNCTR l'autorisation d'identifier les personnes concernées et le recueil de leurs données. Dans ces conditions, **la commission a approuvé cette extension de la technique des algorithmes**.

D. TRAITER LA MENACE CROISSANTE QUE REPRÉSENTENT LES DRONES SUR LE TERRITOIRE NATIONAL

Les drones, qui peuvent dans certains cas être munis d'une charge explosive, représentent une menace croissante dans le cadre de grands événements sportifs ou politiques, de certains convois (convois officiels, convois de matières dangereuses...), ou encore au-dessus des emprises militaires. Le projet de loi prévoit ainsi que **l'autorité administrative pourra demander des opérations de brouillage destinés à neutraliser de tels drones**.

Il convient de rappeler que **les gendarmes jouent déjà un rôle essentiel dans la lutte anti-drones**. Le texte permettra ainsi de fixer un cadre clair et prévisible pour la mise en œuvre de ces opérations. La prochaine étape sera probablement de former certains agents de sécurité privée à cette technique, de nombreux sites importants étant désormais protégés par de tels agents.

III. UN POINT DE VIGILANCE : LA REMISE EN CAUSE DE LA COLLECTE GÉNÉRALE ET INDIFFÉRENCIÉE DES DONNÉES

Dans sa décision du 21 décembre 2016 dite « Tele2 », **la Cour de justice de l'Union européenne avait estimé que la conservation généralisée et indifférenciée des données de connexion par les opérateurs de télécommunication était contraire aux traités**. Actuellement, la loi française

impose à ces opérateurs de garder ces données pendant un an. C'est ce qui fournit ensuite aux services de renseignement la matière de leurs investigations ciblées sur des individus.

Cette décision de la CJUE a placé l'ensemble des services de renseignement européens dans l'embarras. En France, la persistance et l'ampleur de la menace terroriste rendent plus que jamais nécessaires les opérations de collecte des données de connexion menées par les services de renseignement.

Toutefois le Conseil d'Etat, dans son arrêt « French Data Network » du 21 avril 2021, a été amené à interpréter la décision de la CJUE. Selon le Conseil, le juge européen n'interdit pas en tout temps cette conservation générale et indifférenciée des données. Il exige plutôt en réalité que soit alléguée une « *menace grave, réelle et actuelle ou prévisible pour la sécurité nationale* » pour justifier cette conservation. **Le Conseil d'Etat a donc simplement jugé qu'il serait dorénavant nécessaire – c'est ce que prévoit le projet de loi – que le premier ministre prenne chaque année un décret constatant l'existence d'une telle menace grave et actuelle**. En tout état de cause, avec 8 attentats en 2020 et déjà 3 en 2021, la France connaît bien actuellement une telle menace, et la conservation des données pourra donc se poursuivre jusqu'à nouvel ordre sous couvert d'un décret du Premier ministre.

Ainsi les services pourront-ils continuer leurs opérations d'interceptions de communication, indispensables en matière de sécurité nationale et d'anti-terrorisme. Il est cependant nécessaire de rester très vigilant sur cette question, car cette prérogative sera désormais réexaminée chaque année. L'évaluation de la menace, à laquelle concourent l'ensemble des services de renseignement ainsi que, plus largement, des services de sécurité intérieure et extérieure, devra donc être réalisée avec le plus grand soin. La DPR pourra également se prononcer sur cet aspect.

IV. DES GARANTIES PERTINENTES POUR LES LIBERTÉS

Le projet de loi apporte plusieurs nouvelles garanties afin d'encadrer les atteintes à la vie privée qui résultent de l'action des services de renseignement.

A. LE NOUVEL ENCADREMENT JURIDIQUE DES INDISPENSABLES ÉCHANGES DE RENSEIGNEMENTS ENTRE SERVICES

Chaque service redoute désormais qu'un attentat soit commis parce qu'il n'aurait pas communiqué une information dont il disposait au bon destinataire.

Avec la mobilisation anti-terroriste, on est passé dans les échanges inter-services du principe « ne rien transmettre sauf » au principe« tout transmettre sauf »

Il apparaît cependant nécessaire d'encadrer ces échanges, sans quoi les règles posées pour limiter et définir précisément l'emploi des techniques de renseignement, ainsi que le principe même de la distinction entre un premier et un deuxième cercle de services, deviendraient caduques. **Le projet de loi met en place cet encadrement avec suffisamment de souplesse pour ne pas casser une dynamique très profitable à l'efficacité du travail des services**. Ainsi, les échanges d'informations issues de la mise en œuvre des techniques de renseignement resteront-ils possibles, sous réserve qu'ils soient strictement nécessaires à l'exercice des missions du service destinataire. En outre, la transmission sera subordonnée à l'autorisation du Premier ministre, après avis de la CNCTR, lorsqu'elle concernera des renseignements à l'état brut et poursuivra une finalité différente de celle ayant justifié leur recueil, ou lorsque cette transmission concernera des renseignements recueillis par la mise en œuvre d'une technique à laquelle le service destinataire n'aurait pu recourir lui-même dans le même but.

B. UN RENFORCEMENT DES PRÉROGATIVES DE LA DPR

L'idée qu'il est nécessaire de garder un équilibre entre les prérogatives des services de renseignement d'une part, et les pouvoirs de contrôle de la délégation d'autre part, a conduit à un renforcement progressif de celle-ci au cours des dernières années. C'est ainsi que d'un simple suivi des services de renseignement, la DPR est passée à un véritable **contrôle de la politique de renseignement**.

Le Gouvernement n'avait pas proposé de nouvelle avancée sur ce point au sein du présent projet de loi. L'Assemblée nationale a, en revanche, adopté un amendement de la présidente de la DPR, Françoise Dumas. **Les dispositions ainsi introduites élargissent d'abord le champ d'action de la DPR** en lui reconnaissant explicitement la possibilité de traiter des enjeux d'actualité liés au renseignement. Il s'agit, sans interférer sur les opérations en cours, de pouvoir néanmoins mener des travaux en prise avec l'actualité. En outre, il est prévu que le Gouvernement transmette à la DPR, chaque semestre, la liste des rapports de l'inspection des services de renseignement (ISR) et de ceux des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence. S'agissant enfin des personnalités susceptibles d'être auditionnées par la DPR, la liste en est complétée par la mention de « toute personne exerçant des fonctions de direction » au sein des services, au-delà des seuls directeurs de ces services. Toutefois, les auditions de ces personnes devront se tenir en présence de leur hiérarchie, sauf si celle-ci y renonce.

Ces avancées sont certes modérées et les prérogatives des organes similaires des autres pays occidentaux restent souvent plus développées. Toutefois, il est indéniable que la délégation parlementaire au renseignement continue à monter en puissance et ces évolutions ne feront que conforter cette progression.

La commission a par ailleurs adopté **deux amendements** ayant pour but de renforcer dans la durée la protection des éléments couverts par le secret de la défense nationale au sein des rapports de la DPR et de la commission de vérification des fonds spéciaux (CVFS), en prévoyant que ces rapports seront « présentés » et non plus « transmis » à certaines autorités (présidents des assemblées et des commissions des finances, rapporteurs généraux de celles-ci).

C. LA NÉCESSITÉ D'ADAPTER LES MOYENS AUX BESOINS DES SERVICES DE RENSEIGNEMENTS

L'appropriation du nouveau cadre législatif issu de la loi de 2015, en particulier la mise en œuvre des procédures de contrôle et de validation internes et externes prévus pour les techniques de renseignement, a nécessité une augmentation des moyens humains affectés à ces tâches. Si les services de grande taille, qui ont bénéficié de hausses d'effectifs importantes au cours des dernières années, ont pu absorber cette évolution assez facilement, l'adaptation a été plus difficile pour les services de taille modeste. **Il conviendra donc de veiller à ce que la trajectoire des effectifs de ces services permette d'absorber dans les prochaines années les évolutions prévues par le nouveau texte**, en particulier l'encadrement prévu pour les échanges de données entre services par l'article 7 du projet de loi.

V. UN SUJET PARTICULIÈREMENT DÉBATTU : LA RÉFORME DES RÈGLES DE COMMUNICATION DES DOCUMENTS INTÉRESSANT LA DÉFENSE NATIONALE

L'article 19 du projet de loi vise à **résoudre un conflit entre, d'une part, les dispositions du code du patrimoine, qui prévoient une communicabilité de plein droit des archives** au bout d'un délai variant en fonction de la sensibilité de ces archives (de 25 à 100 ans) et, d'autre part, l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, **qui exige une déclassification explicite des documents qui portent atteintes à des secrets de la défense nationale**. En effet, cette dernière instruction a pour effet de retarder, parfois considérablement, la divulgation de documents qui devraient être communicables selon le code du patrimoine.

Le texte prévoit ainsi une déclassification automatique des documents à leur date de communicabilité, mais, en contrepartie, une

protection sans limite de durée pré-fixée pour les archives les plus sensibles (installations militaires, armements, procédures opérationnelles des services de renseignement). **C'est ce caractère non limité dans le temps qui a suscité l'inquiétude, notamment, de certains historiens,** car la prévisibilité de la date d'accessibilité des documents est essentielle au lancement de travaux de recherche dans un domaine donné.

Toutefois, il convient d'observer que la décision de ne pas communiquer un document pourra toujours faire l'objet d'une saisine de la CADA et, en cas de rejet de la demande, d'un recours en justice. Par ailleurs, malgré les restrictions prévues, le nouveau système prévu par l'article 19 constitue un progrès important car la communicabilité de plein droit devrait permettre l'accès à de très nombreux documents aujourd'hui inaccessibles.

EXAMEN EN COMMISSION

Réunie le 15 juin 2021, sous la présidence de M. Pascal Allizard, vice-président, la commission des affaires étrangères, de la défense et des forces armées a procédé à l'examen du rapport pour avis de M. Olivier Cigolotti sur le projet de loi n° 672 (2020-2021) relatif à la prévention d'actes de terrorisme et au renseignement.

M. Olivier Cigolotti, rapporteur.- Ce projet de loi comporte deux catégories de dispositions. Je n'évoquerai que brièvement les premières, qui relèvent de la justice et de la sécurité intérieure. Elles pérennisent et renforcent les mesures créées, à la suite de l'état d'urgence, par la loi dite « SILTE » (sécurité intérieure et lutte contre le terrorisme). Il s'agit notamment des mesures individuelles de contrôle administratif et de surveillance (dites MICAS). Dans ce domaine, le texte prévoit par ailleurs une nouvelle mesure de sûreté pour les détenus pour terrorisme qui restent dangereux après leur sortie. Il s'agit d'un enjeu qui revêt actuellement une importance essentielle. La nouvelle mesure est taillée au plus juste pour éviter une censure du Conseil constitutionnel semblable à celle qui avait frappé la loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine.

J'en viens à la seconde catégorie de mesures, qui nous intéressent plus directement : il s'agit d'ajustements relatifs aux prérogatives des services de renseignement. Je rappelle en effet que trois des services du « premier cercle » de la communauté du renseignement relèvent du ministère des armées : la DGSE, la DRM et la DRSD.

Il y a ici pour nous d'emblée un premier point de vigilance : lors des auditions, tous les services ont en effet souligné qu'ils aspiraient à une certaine stabilité législative.

Or, heureusement, le projet de loi ne constitue en aucun cas une remise en cause des principes fondamentaux posés par la loi du 24 juillet 2015. Ces principes sont les suivants : un contrôle *a priori* des techniques de renseignement par la Commission nationale de contrôle des techniques de renseignement (CNCTR), un encadrement des demandes par un certain nombre de finalités, enfin une définition précise des compétences des services, par ailleurs répartis en deux cercles. Cet encadrement est souvent résumé en évoquant le principe « une finalité, une technique, un service ».

Le bilan effectué en 2020 par la délégation parlementaire au renseignement, sous la direction de notre président, a montré que cet encadrement avait été très bien assimilé par les services, même si cela ne s'est pas fait sans efforts. Aujourd'hui, tous les services nous ont dit que le fonctionnement était fluide, et le contrôle de la CNCTR bien intégré.

Le projet de loi préserve donc ces équilibres et nous pouvons nous en féliciter.

Il nous faut cependant porter une attention particulière à plusieurs nouvelles techniques de renseignement introduites par le texte. En effet, le caractère très évolutif des technologies sur lesquelles elles s'appuient rendent leur efficacité en partie incertaine. Il faudra donc suivre attentivement leur déploiement et les résultats obtenus.

Il s'agit d'abord de la captation des communications satellitaires. Vous le savez, nous assistons ici à une véritable révolution. Des constellations, regroupant parfois plusieurs milliers de satellites, vont être déployées de manière imminente. Je pense en particulier à Starlink de Space X avec plus de 4 000 satellites dans un premier temps ou à Kuiper d'Amazone, qui regroupera également des milliers d'unités. Ceci permettra aux personnes qui souhaitent améliorer leur connexion à Internet, mais aussi aux criminels ou aux terroristes, de contourner les moyens classiques de communication. Ils échapperont ainsi aux moyens d'interception habituels des services. Ce n'est pas une hypothèse fantaisiste : cet usage est déjà à l'œuvre en Guyane par exemple. La possibilité pour les services de s'adresser à ces nouveaux opérateurs étrangers est envisageable, mais présente deux inconvénients majeurs : seront-ils coopératifs, et aurons-nous envie de leur donner des indications sur nos cibles ? Il y a là pour notre pays un vrai sujet de souveraineté !

Dès lors, l'autre solution est de capter directement les faisceaux satellitaires. C'est l'hypothèse envisagée par le texte. Il faut garder à l'esprit qu'il s'agit d'une technique encore largement balbutiante. Des garanties importantes sont prévues : expérimentation pendant 4 ans, caractère subsidiaire, centralisation des interceptions réalisées au groupement interministériel de contrôle (GIC), fixation d'un nombre maximal d'interceptions simultanées. Le directeur technique de la DGSE, Patrick Pailloux, nous l'a bien précisé : les services ne savent pas encore exactement quelles technologies ils utiliseront. En tout cas, cela relèvera dans un premier temps de la DGSE, qui préfère garder la main sur ce sujet pour éviter des expérimentations hasardeuses. C'est pourquoi je vous proposerai un amendement de précision pour indiquer que seuls les services du premier cercle pourront mener cette expérimentation. Il sera temps, au moment de son éventuelle pérennisation, d'élargir l'accès à cette technique.

Au total, il s'agit là d'un apport important de cette loi, qui permettra aux services de rester dans la course technologique.

Il en va de même de la deuxième avancée que je souhaite évoquer : la possibilité de solliciter les opérateurs lors de la mise en œuvre de la technique dite de l'« IMSI-catching ». Celle-ci permet actuellement de recueillir des données de connexion à proximité d'une personne ciblée. L'objectif de la nouvelle disposition est d'anticiper le déploiement de la 5G.

Celle-ci aura pour effet de rendre temporaires les identifiants des téléphones portables. Il n'y a que l'opérateur qui pourra relier ces identifiants aux abonnements ou téléphones utilisés. L'objectif de cette disposition est ainsi finalement de garantir l'intérêt opérationnel des IMSI-catcher, qui sans cela risquerait de disparaître totalement, après le déploiement de la SG.

Troisième innovation : l'extension du champ des désormais fameux « algorithmes » introduits par la loi de 2015. Je rappelle que cette technique avait alors été créée à titre expérimental. À vrai dire, son champ d'application, d'emblée limité aux données téléphoniques, a empêché qu'on obtienne des résultats vraiment probants. C'est pourquoi le texte, outre qu'il pérennise cette technique, en étend l'application aux « URL », c'est-à-dire aux adresses des pages internet. Les services estiment qu'avec cette extension, les algorithmes sont très prometteurs. On passe en quelque sorte de l' « ancien monde » de la téléphonie, de moins en moins utilisé, au « nouveau monde » des adresses IP et des URL. Là encore, les garanties prévues nous semblent sérieuses : les algorithmes sont contrôlés par la CNCTR, qui dispose d'un accès permanent à ces traitements. Je rappelle que les algorithmes ne permettent pas en soi d'identifier les personnes et que l'ajout des URL ne changera rien sur ce plan. C'est seulement dans un second temps, si l'algorithme aboutit, que les services demandent à la CNCTR l'autorisation d'identifier les personnes. Dans ces conditions, il me semble que nous pouvons approuver les dispositions qui nous sont soumises.

Je souhaitais également évoquer une nouvelle faculté ouverte à plusieurs services de l'État par l'article 18 : il s'agit du brouillage de drones. On sait la menace croissante que représentent ces engins dans le cadre de grands événements sportifs ou politiques, de certains convois officiels, ou encore au-dessus de nos emprises militaires. L'autorité administrative pourra donc demander des opérations de brouillage dans le cadre juridique fixé par la loi. Les gendarmes jouent déjà un rôle essentiel dans la mise en œuvre de cette technique. Depuis 2017, 52 drones ont ainsi été neutralisés par des gendarmes formés à cette tâche. En tout état de cause, nous pouvons nous féliciter de cette nouvelle disposition, s'agissant d'une menace qui ne fait que croître.

Au-delà de ces quatre nouvelles techniques prévues par la loi, je souhaitais toutefois signaler un point de vigilance très important. Par sa décision du 21 décembre 2016 dite « Tele 2 », la Cour de justice de l'Union européenne a estimé que la conservation généralisée et indifférenciée des données de connexion par les opérateurs de télécommunication était illégale. Actuellement, la législation impose à ces opérateurs de garder ces données pendant un an. C'est ce qui permet ensuite aux services de renseignement de faire des demandes ciblée sur des individus. Il va de soi que cette décision de la CJUE a placé l'ensemble des services de renseignement européens dans l'embarras. Compte-tenu de la menace qui pèse sur la France, la

consternation a été particulièrement forte au sein de nos services de renseignement.

C'était sans compter l'interprétation constructive que le Conseil d'Etat, dans son arrêt « French Data Network » du 21 avril 2021, a donné de cette décision de la CJUE. En effet, que demande au fond le juge européen ? Il exige, pour justifier la conservation généralisée et indifférenciée des données, que soit alléguée une « *menace grave, réelle et actuelle ou prévisible pour la sécurité nationale* ». Le Conseil d'Etat a donc simplement indiqué qu'il serait dorénavant nécessaire - et c'est ce que prévoit le texte - que le premier ministre prenne chaque année un décret constatant cette menace grave. Avec 8 attentats en 2020 et déjà 3 en 2021, notre pays connaît bien actuellement une telle menace. Ainsi, les services pourront continuer leurs opérations d'interceptions de communications, indispensables en matière de sécurité nationale et d'anti-terrorisme.

Mais qu'adviendra-t-il à l'avenir ? Suffira-t-il d'une légère diminution de la menace pour que le Premier ministre ne puisse plus prendre de décret, et que toute interception soit rendue impossible ? On peut certes imaginer, comme certaines associations, un Gouvernement qui surévalue la menace, mais après tout, on peut aussi imaginer l'inverse. Il est donc impératif que le Parlement, et en particulier la DPR, suive ce sujet avec la plus grande attention chaque année.

Enfin, l'article 19 concerne les archives intéressant la défense nationale. Il clarifie le régime de communicabilité des archives classifiées au bénéfice de l'ensemble des usagers, en particulier des chercheurs et des historiens, tout en garantissant mieux la protection des documents les plus sensibles. Il rend en effet communicable l'écrasante majorité des documents classifiés datant de plus de cinquante ans, allégeant ainsi la charge pesant actuellement sur les services publics d'archives pour la préparation des demandes de déclassification. Le service historique de la défense estime que cet article permettra ainsi l'ouverture de 650 000 dossiers. Inversement, le texte mentionne quatre types de documents dont la communication, même au bout de 50 ans, pourrait être préjudiciable : les plans de centrales nucléaires, de barrages hydrauliques, d'infrastructures militaires ; les matériels de guerre ; les procédures opérationnelles des services de renseignement ; enfin le système de contrôle gouvernemental de la dissuasion nucléaire. Cet article atteint ainsi un équilibre qui nous semble satisfaisant. En effet, il n'y aura pas, comme le craignent certains chercheurs, de refus de communication sans possibilité de recours : de tels refus, même dans les quatre cas mentionnés, pourront bien faire l'objet d'un recours en justice. Toutefois, les discussions entre la commission des lois et la commission de la culture, qui s'est saisie de cette question, sont toujours en cours pour faire bouger le curseur. Peut-être pourront-nous rejoindre ce travail d'ici la séance.

Par ailleurs, le texte comporte également des avancées sur le plan des garanties apportées au regard des libertés publiques. Il s'agit d'abord de l'encadrement des échanges entre services. D'une situation où la communication entre services était fondée sur le « rien sauf », on est passé progressivement à une situation de « tout sauf ». Ce que redoutent désormais le plus les services, c'est qu'un attentat soit commis parce qu'ils n'ont pas transmis une information au bon destinataire. Cependant, on voit bien qu'il faut encadrer ces échanges. Sans cela, la distinction entre un premier et un deuxième cercle des services deviendrait caduque. C'est ce que fait le texte avec suffisamment de souplesse pour ne pas casser cette dynamique finalement très profitable à l'efficacité des services.

Je terminerai en évoquant les évolutions qui concernent la délégation parlementaire au renseignement. L'idée, depuis quelques années, est qu'il convient de garder un équilibre entre les prérogatives des services de renseignement d'une part, et les pouvoirs de contrôle de la délégation d'autre part. C'est ainsi que d'un simple suivi des services de renseignement, la DPR est passée à un véritable contrôle de la politique de renseignement.

Le Gouvernement n'avait pas proposé de nouvelle avancée sur ce point. L'Assemblée nationale y a pourvu, par un amendement déposé par la présidente de la délégation, Françoise Dumas. Cet article élargit d'abord le champ d'action de la DPR en lui reconnaissant la possibilité de traiter des enjeux d'actualité liés au renseignement. En outre, le Gouvernement devra transmettre à la DPR, chaque semestre, la liste des rapports d'inspection portant sur les services de renseignement. S'agissant enfin des personnalités susceptibles d'être auditionnées par la DPR, la liste en est élargie à toute personne exerçant des fonctions de direction au sein des services, au-delà des seuls directeurs de ces services.

S'agissant de la DPR, je vous proposerai deux amendements ayant trait à une meilleure protection du secret de la défense nationale. En effet le rapport de la DPR, et surtout celui de la commission de vérification des fonds spéciaux (CVFS), sont remis à certaines autorités en plus du Gouvernement à qui ils sont destinés : présidents des assemblées mais aussi présidents des commissions des finances et rapporteurs généraux de ces commissions. Or la CVFS ne pouvant s'assurer que son rapport soit alors conservé dans des conditions conformes à l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (dite « IGI 1300 »), elle a décidé d'en faire chaque année une présentation à ces autorités puis de le tenir à leur disposition, au lieu de le leur remettre. Ces amendements mettent ainsi le droit en conformité avec le fait.

Mes chers collègues, le projet de loi que nous examinons aujourd'hui répond parfaitement aux demandes opérationnelles des services, tout en offrant des garanties précises pour la préservation des libertés fondamentales. Le président de la CNCTR, qui effectue un contrôle très approfondi de la mise en oeuvre des techniques de renseignement, nous a

confirmé que ce texte, qui prend en compte la plupart des recommandations qu'il avait faites, est équilibré.

Je vous propose donc, sous réserve des amendements que je vais vous présenter, de donner un avis favorable à l'adoption de ce projet de loi.

Examen des amendements

M. Olivier Cigolotti. - Le premier amendement vise à limiter l'expérimentation des interceptions satellitaires aux services du « premier cercle ».

M. André Gattolin. - Je me pose la question de l'interaction entre services du premier et du second cercle. Nous avons évoqué avec le SGDSN la création d'un service dédié aux tentatives d'influence lors des élections. Cela ne sera pas un service du second cercle et pourtant en cas de péril pour la sincérité du vote, il faudra bien que des échanges puissent avoir lieu. Pour les interceptions satellitaires, la période d'expérimentation prévue est longue, ce qui est une garantie. Ne faut-il pas, cependant, être moins strict sur la distinction entre les deux cercles ?

M. Olivier Cigolotti. - Les gendarmes nous ont fait valoir que, dans l'état actuel des choses, ils ne sont pas intéressés par l'interception satellitaire. Toutefois, dans quatre ans, il sera sans doute nécessaire de leur permettre, par voie législative, de bénéficier de cette technique. Par prudence toutefois, nous avons décidé de restreindre l'expérimentation au premier cercle.

Mme Michelle Gréaume. - Nous ne voterons pas l'article 11. La question de la sécurité des satellites français est posée.

M. Olivier Cigolotti. - Le développement du satellitaire est déjà en cours. Les narcotrafiquants en mer, les terroristes dans le désert s'en servent. Il faut que nos services gardent une longueur d'avance. Et la 5G sera une révolution technologique, avec des identifiants temporaires. Les technologies avancent et il faut permettre à nos services d'avancer au même rythme, sous réserve de la garantie des libertés.

L'amendement ETRD 1 est adopté.

M. Olivier Cigolotti. - L'amendement suivant vise à mieux protéger les éléments secrets défense au sein des recommandations de la DPR.

M. Pascal Allizard. - Il est vrai qu'il y a un sujet sur la conservation dans la durée de ce type de documents classés.

M. Olivier Cigolotti. - L'amendement suivant est similaire mais concerne le rapport de la CVFS.

M. Bruno Sido. - Les documents sont-ils transmis ou simplement présentés à l'oral ?

M. Olivier Cigolotti. - Pour l'instant ils sont transmis, ce qui ne permet pas d'assurer leur protection en tout temps.

Par ailleurs, je souhaitais souligner que nous avons eu peu de temps pour examiner ce texte et nous avons travaillé intensivement pendant ce délai.

Les amendements ETRD 2 et ETRD 3 sont adoptés.

M. Yannick Vaugrenard. - Il est vrai que ce texte est le prolongement de la loi de 2015, qui a suivi les attentats. Il y a des évolutions technologiques relativement récentes comme la 5G et les satellites à basse altitude : ce seront pour les services eux-mêmes des sujets de recherche fondamentale. Membre à la fois de la DPR et de la CNCTR, je peux arguer du fait que le temps a été très bref pour examiner ce texte. Je partage les conclusions du rapporteur mais j'aurais trois points de vigilance.

S'agissant des MICAS, il eût été préférable que le Gouvernement demande au Conseil s'il y avait un risque constitutionnel à faire passer les MICAS d'une durée de un an à une durée de deux ans. Le Conseil d'État a souligné un tel risque. L'application de la loi pourrait alors être reportée, ce qui serait dommageable.

S'agissant des services de renseignement, nous sommes un des seuls pays européens à ne pas contrôler *a posteriori* les échanges de nos services avec les services étrangers. Les États-Unis le font aussi. La CEDH, par un arrêt du 25 mai dernier, a indiqué qu'un encadrement était nécessaire. Nous risquons une condamnation. Il faudra nécessairement légiférer. Il s'agirait bien entendu d'un contrôle par une instance indépendante tenue au secret-défense. Les documents fournis à la CNCTR ou à la DPR contiennent parfois des éléments caviardés et nous pouvons consulter les éléments manquants dans des coffres forts au sein des services.

Enfin, autre point de vigilance, c'est le Premier ministre, par décret, qui doit déclarer que nous sommes en situation de menace terroriste majeure. Il faut toujours imaginer la possibilité que nous soyons gouvernés un jour par des groupements extrémistes. Dès lors, il serait préférable que l'Assemblée nationale et le Sénat puissent donner leur accord. Ce serait une assurance supplémentaire au regard de notre vie démocratique et républicaine.

Les terroristes actuels ne sont pas téléguidés de l'extérieur comme c'était le cas il y a quelques années. Ils sont souvent atteints de problèmes psychiques majeurs. Les algorithmes sont utiles dans ce domaine. Les trois premiers algorithmes ont été mis en place en 2017. Il faut du temps. Au-delà de ces éléments, le rapport d'Olivier Cigolotti conviendra à notre groupe.

M. Philippe Folliot. - Je voudrais saluer l'intervention de Yannick Vaugrenard, qui a bien situé l'ensemble des enjeux au regard de l'équilibre entre l'efficacité des services pour défendre nos démocraties contre le fléau

du terrorisme et la nécessité de préserver les libertés individuelles, alors qu'on ne peut pas exclure que le pouvoir ne tombe un jour entre de mauvaises mains. C'est vrai qu'il y a des évolutions techniques. En réalité, l'un des enjeux est de préserver une zone grise, qui est le propre de tous les services de renseignement : c'est le gage de l'efficacité. Selon vous, ce texte permet-il d'atteindre un équilibre dans ce domaine ?

M. Bruno Sido. - Un Etat a certes besoin de services de renseignement. Il faut que le Parlement soit dans la boucle de contrôle, mais cela ne suffit pas. Qui aujourd'hui contrôle véritablement les services du renseignement ? Des fonctionnaires assurent-ils en permanence ce contrôle ?

M. Olivier Cigolotti. - S'agissant des MICAS, la DGSI nous en a rappelé l'utilité. L'allongement de la durée de ces mesures pose question. Il faut trouver une rédaction qui évite tout risque d'inconstitutionnalité. Il y aura un débat lors de l'examen du texte. Le contrôle *a posteriori* des échanges des services de renseignement avec leurs homologues étrangers est une vraie question : à un moment ou à un autre il nous faudra évoluer.

Nous sommes passés d'une menace structurée et pilotée depuis l'étranger à une menace plus endogène, avec des individus qui ont souvent des problèmes psychologiques et qui sont plus difficiles à détecter. Les algorithmes devraient nous apporter une aide dans les années à venir en la matière.

S'agissant de l'équilibre du texte, la stabilité législative est unanimement demandée par les services et le présent texte n'y déroge pas. Avant 2015, chaque service gardait jalousement ses informations et le résultat de ses interceptions. Après 2015, il y a eu l'instauration d'un vrai partage de données. L'appréhension des services, c'est qu'il y ait de nouveau un attentat et qu'il n'y ait pas eu les bons échanges entre services en amont. Enfin, le contrôle des services est parfaitement effectué par la CNCTR, qui va très régulièrement à la DGSE, en lien avec le GIC. La CNCTR est un organisme de 17 personnes qui contrôle bien la finalité, le service et la technique pour chaque demande.

M. Yannick Vaugrenard. - C'est le GIC qui centralise toutes les informations. La CNCTR se réunit toutes les semaines pour donner son accord sur l'utilisation des techniques. Si la technique concerne un parlementaire, un avocat, un juge, un journaliste, la CNCTR doit se réunir avec l'ensemble de ses membres : quatre parlementaires, deux membres de la Cour de cassation, deux membres du Conseil d'Etat, le président et un technicien. Nous devons être d'une vigilance extrême et ne pas considérer que notre démocratie est éternelle. C'est pourquoi il est vraiment important qu'une autorité indépendante et le Parlement puissent exercer un contrôle et que ce ne soit pas le Premier ministre seul qui décide s'il y a une menace terroriste majeure ou pas.

M. Olivier Cigolotti. - J'ajoute à titre d'exemple, s'agissant de l'équilibre du texte, que l'article 7 assure un tel équilibre entre les prérogatives des services, en l'occurrence les échanges d'informations, et le contrôle de la CNCTR.

M. Pascal Allizard. - président. - Merci pour ce travail de fond dans des conditions compliquées. Nous aurons un beau débat en séance publique.

Le sort des amendements est retracé dans le tableau suivant :

Auteur	N°	Objet	Sort de l'amendement
Article 11			
M. CIGOLOTTI	ETRD 1	Limitation de l'expérimentation satellitaire au premier cercle.	**à déposer**
Article 17 *bis*			
M. CIGOLOTTI	ETRD 2	Présentation du rapport de la DPR	**à déposer**
Article additionnel après l'article 17 *bis*			
M. CIGOLOTTI	ETRD 3	Présentation du rapport de la CVFS.	**à déposer**

LISTE DES PERSONNES AUDITIONNÉES

Ministère des armées

Secrétariat général pour l'administration

- Mme Claire Legras, directrice des affaires juridiques

Direction du renseignement et de la sécurité de la défense (DRSD)

- Général de division Thierry de Ladoucette, chef d'état-major

- M. Paul Chiappore, sous-directeur de la stratégie et des ressources

Direction générale de la sécurité extérieure (DGSE)

- Général de corps d'armée Olivier de Paillerets, directeur de cabinet

- M. Patrick Pailloux, directeur technique

- M. Benjamin de Maillard, conseiller du directeur général

Direction du renseignement militaire (DRM)

- Général Jean-François Ferlet, directeur

- Mme Elody Justo, cheffe du bureau des affaires juridiques

Ministère de l'intérieur

Direction des libertés publiques et des affaires juridiques

- Mme Pascale Léglise, directrice et chef du service du conseil juridique

Direction générale de la sécurité intérieure (DGSI)

- M. Nicolas Lerner, directeur général

Sous-direction de l'anticipation opérationnelle (SDAO-gendarmerie nationale)

- Général Patrick Henry, sous-directeur de l'anticipation opérationnelle

Ministère de l'économie, des finances et de la relance

Direction nationale du renseignement et des enquêtes douanières (DNRED)

- M. Florian Colas, directeur

- Mme Alice Chérif, magistrate détachée à la DNRED

- M. Sébastien Tiran, adjoint opérationnel à la direction des opérations douanières

Centre national de contre-terrorisme (CNCT)

- M. Laurent Nuñez, coordonnateur nat