…le projet de loi relatif à

LA PRÉVENTION D'ACTES DE TERRORISME ET LE RENSEIGNEMENT

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.

1. 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.

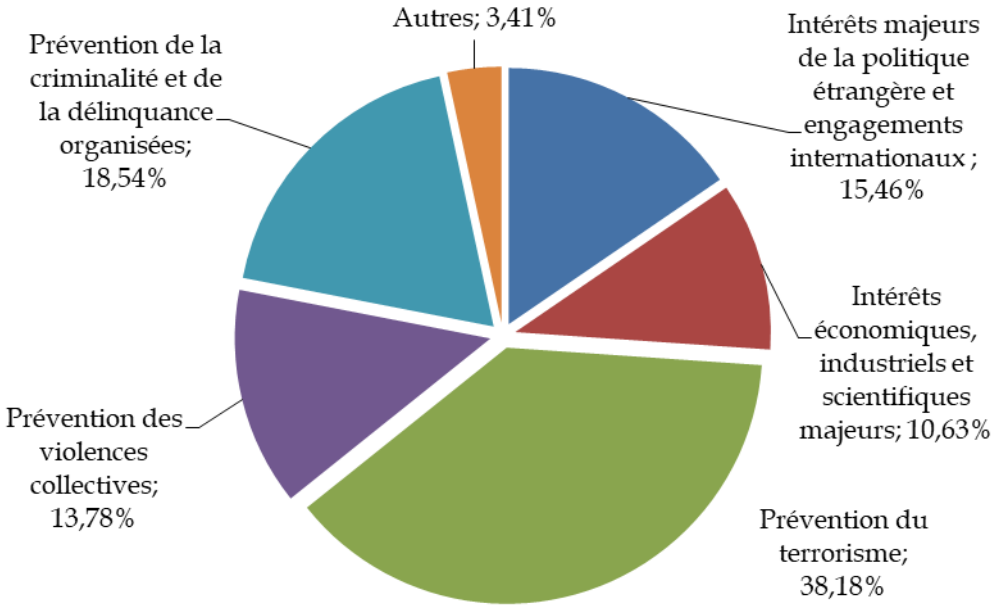
Le texte s'inscrit pleinement dans la continuité des dispositions de la loi du 24 juillet 2015.

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.

2. 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.

3. 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.

4. 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.

5. 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.

Christian Cambon

Président de la commission
Sénateur
(Les Républicains)
du Val-de-Marne

Olivier Cigolotti

Rapporteur

Sénateur
(Union Centriste)
de la Haute Loire

Commission des affaires étrangères, de la défense et des forces armées

http://www.senat.fr/commission/etr/index.html

Consulter le dossier législatif :

http://www.senat.fr/dossier-legislatif/pjl20-672.html