



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

**Commission nationale de contrôle
des techniques de renseignement**

CNCTR

5^e Rapport d'activité 2020

Avant-propos	7
Un résumé du cadre juridique en vigueur	9
Une modification de la composition de la CNCTR ...	13
COMPTE-RENDU DE L'ACTIVITÉ DE LA CNCTR	15
1. Les modifications du cadre juridique en 2020 et les perspectives d'évolution : des échéances reportées en raison de la crise sanitaire	16
1.1 Un cadre juridique demeuré stable en 2020	16
1.1.1 Une nouvelle prorogation de l'application de l'article L. 851-3 du code de la sécurité intérieure	16
1.1.2 Une première demande de révision du contingent applicable au recueil de données de connexion par <i>IMSI catcher</i>	18
1.2 Les perspectives d'évolution du cadre juridique : un calendrier bouleversé par la crise sanitaire	22
1.2.1 Un débat parlementaire attendu avant le 31 décembre 2021 sur le devenir de la technique dite de l'algorithme	22
1.2.2 Un cadre légal susceptible d'évoluer du fait de la jurisprudence des deux Cours européennes	23
1.2.2.1 L'arrêt rendu en grande chambre par la Cour de justice de l'Union européenne (CJUE) le 6 octobre 2020 sur la question de la conservation des données de connexion	23
1.2.2.2 Les requêtes introduites devant la Cour européenne des droits de l'Homme (CEDH) contre plusieurs dispositions de la loi du 24 juillet 2015 relative au renseignement	25
1.2.2.3 Les réflexions en cours sur le partage international de données entre services de renseignement	26

2. Le contrôle <i>a priori</i> des demandes d'autorisation de mise en œuvre des techniques de renseignement : une mission prioritaire dont la continuité a été assurée malgré la crise sanitaire	30
2.1 Une activité soutenue face au maintien de la menace terroriste à un niveau élevé, dans un contexte de pandémie mondiale	32
2.1.1 Le nombre d'avis préalables rendus par la CNCTR en matière de surveillance intérieure : une augmentation des demandes d'accès aux données de connexion conjuguée à une baisse des autres demandes, notamment celles relatives aux techniques les plus intrusives	33
2.1.2 Les finalités invoquées dans les demandes de techniques de renseignement relevant de la surveillance intérieure : la prédominance de la prévention du terrorisme	41
2.1.3 Le nombre de personnes surveillées au moyen de techniques de renseignement relevant de la surveillance intérieure : une légère diminution en 2020	44
2.1.4 Le nombre d'avis préalables rendus par la CNCTR au titre de la surveillance internationale : une augmentation témoignant de l'appropriation progressive par les services de renseignement des dispositions législatives introduites en 2018	48
2.2 Un examen renforcé des dossiers les plus sensibles et des techniques de renseignement les plus intrusives	50
2.2.1 La stabilité du nombre de demandes de renseignements complémentaires adressées aux services de renseignement	50
2.2.2 La procédure de suivi des « productions » : un moyen de contrôle exhaustif permettant de vérifier la réalité de la menace et l'absence d'irrégularités	51

2.2.3 Des interactions nombreuses et utiles entre contrôle <i>a priori</i> et contrôle <i>a posteriori</i>	54
2.2.3.1 Certains dossiers instruits dans le cadre du contrôle <i>a priori</i> font l'objet d'un suivi particulier lors des contrôles <i>a posteriori</i>	54
2.2.3.2 Les constats dressés au cours des contrôles <i>a posteriori</i> peuvent éclairer la commission lors de l'instruction des demandes d'autorisation présentées par les services	56
3. Le contrôle <i>a posteriori</i> de la mise en œuvre des techniques autorisées : une mission exercée en 2020 dans des conditions adaptées au risque sanitaire	59
3.1 Une complémentarité renforcée entre les contrôles menés sur pièces et sur place au sein des services de renseignement et ceux réalisés à distance depuis les locaux de la CNCTR	60
3.1.1 Le développement de nouvelles modalités de contrôle à distance pour s'adapter aux mesures destinées à limiter la pandémie de Covid-19	60
3.1.2 Une mise en œuvre à consolider face aux réserves manifestées par les services de renseignement	63
3.2 L'approfondissement du contrôle du recueil et de l'exploitation des données issues des techniques de renseignement : une entreprise à long terme qui progresse	65
3.2.1 Une application sérieuse du cadre légal : des irrégularités en nombre limité et de faible portée	65
3.2.1.1 Les irrégularités constatées en matière de surveillance intérieure	66
3.2.1.2 Les irrégularités constatées en matière de surveillance des communications électroniques internationales	70

3.2.2 Un contrôle <i>a posteriori</i> qui doit encore être facilité et perfectionné : des évolutions toujours attendues en matière d'accès, de centralisation et de traçabilité de l'exploitation des données recueillies	72
3.2.2.1 Un approfondissement continu et progressif du contrôle <i>a posteriori</i> à l'épreuve des réserves des services de renseignement	72
3.2.2.2 Une centralisation croissante des données recueillies par la mise en œuvre des techniques de renseignement mais encore incomplète	75
3.2.2.3 Des évolutions contrastées en matière de traçabilité de la mise en œuvre des techniques de renseignement et d'exploitation des données recueillies	77

4. Un usage modéré des recours contre la mise en œuvre des techniques de renseignement 79

4.1 Une légère diminution du nombre de réclamations adressées à la CNCTR	79
--	----

4.2 Une augmentation limitée du nombre de requêtes introduites devant le Conseil d'État	83
---	----

ANNEXE 89

Délibération de la CNCTR n° 1/2020 du 20 mai 2020	90
(avis sur deux articles d'un projet de loi relatif à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure)	

Avant-propos

La crise sanitaire liée à la pandémie de Covid-19 a eu un fort impact sur l'activité de la Commission nationale de contrôle des techniques de renseignement (CNCTR) durant l'année 2020.

Alors qu'au printemps 2020 la pandémie contraignait notre pays à se confiner, la CNCTR a dû mettre en place des modalités d'organisation permettant de concilier les exigences liées à la poursuite de sa mission de contrôle avec celles tenant à la protection de la santé de ses membres et de ses agents.

S'appliquant à des informations couvertes par le secret de la défense nationale, le contrôle des techniques de renseignement se prête mal au travail à distance depuis le domicile. La plupart des outils de communication disponibles n'offrent pas, en effet, une protection suffisante de ces informations. Le recours au « télétravail » a dû être limité à des tâches de secrétariat ou de recherches sans lien direct avec l'activité de contrôle de la commission. Le contrôle *a priori* des demandes d'autorisation de surveillance formulées par les services de renseignement a donc continué à être exercé dans les locaux sécurisés de la commission.

La poursuite sans discontinuité de cette activité de contrôle *a priori* a été rendue possible par le dévouement des membres et des agents de la CNCTR qui ont accepté, même au plus fort de la crise sanitaire, de continuer à exercer leur activité sur leur lieu de travail. Je tiens à les en remercier.

Pendant le premier confinement, au printemps 2020, tous les déplacements de contrôle *a posteriori* sur pièces et sur place dans les services de renseignement ont dû être suspendus durant plusieurs semaines. Ils ont repris par la suite, dans des conditions adaptées au risque sanitaire, mais, globalement, sur l'ensemble de l'année 2020, la CNCTR a effectué moins de contrôles de ce type qu'en 2019. Elle a en contrepartie renforcé les contrôles qu'elle peut exercer sur la mise en œuvre de certaines techniques depuis ses locaux. Elle a également proposé des modalités nouvelles de contrôle dématérialisé destinées à compléter les contrôles réalisés sur place dans les services de renseignement mais qui suscitent encore des réserves de la part de ces derniers. Il est pourtant nécessaire de

poursuivre les efforts de développement d'outils techniques permettant à la commission d'exercer, lorsque cela est adapté, un contrôle dématérialisé de la mise en œuvre des techniques de renseignement. La crise sanitaire en a souligné le besoin mais celui-ci va perdurer à l'issue de cette crise.

Le rapport poursuit l'évolution entamée l'année dernière consistant à rendre publiques des informations plus précises et chiffrées sur l'exercice du contrôle *a posteriori*. Il détaille ainsi les divers types d'irrégularités constatées, dont aucune ne révèle une volonté de fraude, et met en évidence la manière dont le contrôle préalable et le contrôle de mise en œuvre viennent se compléter.

Comme les années précédentes, le rapport contient des données chiffrées sur les techniques de renseignement demandées et sur les motifs fondant les demandes. Mais, cette année, il va plus loin en publiant, pour la première fois, un décompte précis des demandes pour chaque type de technique ainsi que l'évolution du nombre de demandes depuis 2016.

Si le nombre total des demandes progresse de près de 8 %, c'est en raison d'une forte augmentation de celles relatives aux accès aux données de connexion alors que chute le nombre des demandes de techniques nettement plus intrusives, qui impliquent la mise en place de moyens techniques au contact physique de la personne surveillée. Par ailleurs, si la finalité de la prévention du terrorisme demeure nettement prédominante, celle de la prévention de la criminalité organisée connaît un léger recul et celle de la défense et de la promotion des intérêts économiques, industriels et scientifiques majeurs de la France une forte baisse.

Après avoir connu une progression modérée mais continue depuis 2016, le nombre de personnes surveillées au moyen de techniques de renseignement est, pour la première fois, en légère baisse.

Il est vraisemblable qu'une part de ces évolutions soit conjoncturelle. La crise sanitaire a en effet eu des conséquences notables sur l'activité des services de renseignement.

J'évoquais l'année dernière les perspectives d'évolution du cadre légal en 2020. Là encore, la crise sanitaire est venue bouleverser le calendrier. C'est en 2021 que cette évolution devrait intervenir.

Francis DELON

Conseiller d'État honoraire

Président de la CNCTR

Un résumé du cadre juridique en vigueur

Le livre VIII du code de la sécurité intérieure, créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement¹ et complété notamment par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, prévoit que les services de renseignement peuvent être autorisés à mettre en œuvre, pour des finalités limitativement énumérées, des techniques destinées à recueillir des renseignements. Chaque autorisation est accordée par le Premier ministre.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) s'assure que les techniques de renseignement sont mises en œuvre sur le territoire national conformément au cadre légal. Elle est consultée préalablement à la décision du Premier ministre sur toutes les demandes tendant à mettre en œuvre une technique ou, s'agissant de la surveillance des communications électroniques internationales, sur toutes les demandes tendant à exploiter des communications interceptées. La CNCTR vérifie également *a posteriori* que les prescriptions légales ont été respectées, en contrôlant l'exécution des autorisations accordées et en vérifiant qu'aucun recueil ou qu'aucune exploitation soumis à autorisation n'a été irrégulièrement mis en œuvre. Elle exerce un contrôle de légalité, qui inclut un contrôle de la proportionnalité des atteintes portées à la vie privée par rapport aux finalités poursuivies.

Les services de renseignement sont notamment des services spécialisés, dits du « premier cercle ». Ce sont :

- la direction générale de la sécurité extérieure (DGSE) ;
- la direction du renseignement et de la sécurité de la défense (DRSD) ;
- la direction du renseignement militaire (DRM) ;
- la direction générale de la sécurité intérieure (DGSI) ;

¹ - Cette loi sera désormais mentionnée comme la loi du 24 juillet 2015.

- le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) ;
- le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin).

D'autres services peuvent se voir confier des missions de renseignement. Ces services, dits du « second cercle », se trouvent notamment au sein de la direction générale de la police nationale, de la direction générale de la gendarmerie nationale, de la préfecture de police de Paris et de la direction de l'administration pénitentiaire.

En matière de surveillance intérieure, c'est-à-dire visant le territoire national, les techniques de renseignement qui peuvent être autorisées sont :

- **les accès administratifs aux données de connexion²**, qui comprennent :
 - les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
 - les accès aux données de connexion en temps réel, à la seule fin de prévention du terrorisme (article L. 851-2 du code de la sécurité intérieure) ;
 - la mise en œuvre, à la seule fin de prévention du terrorisme, de traitements automatisés sur les seules données de connexion acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de services en ligne (article L. 851-3 du code de la sécurité intérieure) ;
 - la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) ;
 - le balisage (article L. 851-5 du code de la sécurité intérieure) ;

² - Définies à l'article L. 851-1 du code de la sécurité intérieure, les données de connexion sont les « informations ou documents traités ou conservés par [les] réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ». Cette définition a été précisée à l'article R. 851-5 du code de la sécurité intérieure.

- le recueil de données de connexion par *IMSI catcher*³ (article L. 851-6 du code de la sécurité intérieure).

- **les interceptions de sécurité**, qui comprennent :
 - l'interception, *via* le groupement interministériel de contrôle (GIC) ou par *IMSI catcher*, des communications acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de service en ligne (article L. 852-1 du code de la sécurité intérieure) ;
 - l'interception des communications échangées au sein d'un réseau privatif empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques (article L. 852-2 du code de la sécurité intérieure).
- **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'introduction dans un lieu privé**, y compris à usage d'habitation (article L. 853-3 du code de la sécurité intérieure), qui ne constitue pas à proprement parler une technique de renseignement mais peut être autorisée, par décision spécifique, à la seule fin de mettre en place, utiliser ou retirer un dispositif de balisage, de captation de paroles, de captation d'images ainsi que de recueil ou de captation de données informatiques.

En matière de surveillance des communications électroniques internationales, l'interception de ces communications ainsi que différentes mesures d'exploitation portant sur des communications ou des seules données de connexion peuvent être autorisées (articles L. 854-1 et suivants du code de la sécurité intérieure).

³ - Il s'agit de dispositifs techniques permettant de capter des données de connexion d'équipements terminaux, notamment le numéro de leur carte SIM ou IMSI (international mobile subscriber identity).

Les finalités pouvant justifier la mise en œuvre des techniques de renseignement sont limitativement énumérées à l'article L. 811-3 du code de la sécurité intérieure :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- 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 ;
- les intérêts économiques, industriels et scientifiques majeurs de la France ;
- la prévention du terrorisme ;
- la prévention des atteintes à la forme républicaine des institutions, la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous et la prévention des violences collectives de nature à porter gravement atteinte à la paix publique ;
- la prévention de la criminalité et de la délinquance organisées ;
- la prévention de la prolifération des armes de destruction massive.

Le service du « second cercle » chargé du renseignement pénitentiaire peut en outre être autorisé à recourir à un nombre limité de techniques pour une finalité propre, prévue à l'article L. 855-1 du code de la sécurité intérieure, à savoir prévenir les évasions et assurer la sécurité au sein des établissements pénitentiaires.

Toute personne peut saisir la CNCTR d'une réclamation tendant à ce que la commission vérifie qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Une fois cette faculté de réclamation utilisée, la personne peut présenter une requête devant une formation spécialisée du Conseil d'État pour demander au juge administratif de mener des vérifications similaires.

Pour une description plus détaillée du cadre légal et de ses évolutions, le lecteur est invité à consulter le premier rapport d'activité pour la période 2015/2016 de la CNCTR ainsi qu'à se référer aux premières parties des rapports d'activité des années suivantes.

Une modification de la composition de la CNCTR


Le collège de la CNCTR a connu trois renouvellements en 2020.

Le 31 juillet 2020, madame Françoise SICHLER-GHESTIN, conseillère d'État honoraire, a été nommée membre de la commission, par le vice-président du Conseil d'État, à compter du 1^{er} septembre 2020, en remplacement de madame Martine JODEAU qui avait démissionné.


Le 23 novembre 2020, madame Chantal DESEYNE, sénatrice d'Eure-et-Loir, et monsieur Yannick VAUGRENARD, sénateur de la Loire-Atlantique, ont été nommés membres de la CNCTR par le président du Sénat. Ils ont remplacé, respectivement, madame Catherine DI FOLCO, sénatrice du Rhône, et monsieur Michel BOUTANT, sénateur de la Charente, dont le mandat parlementaire était parvenu à son terme.

À la fin de l'année 2020, le collège de la commission était composé des neuf membres suivants :

- monsieur Francis DELON, conseiller d'État honoraire, président ;
- madame Chantal DESEYNE, sénatrice d'Eure-et-Loir ;
- monsieur Yannick VAUGRENARD, sénateur de la Loire-Atlantique ;
- madame Constance LE GRIP, députée des Hauts-de-Seine ;
- monsieur Jean-Michel CLÉMENT, député de la Vienne ;
- madame Françoise SICHLER-GHESTIN, conseillère d'État honoraire ;
- madame Christine PÉNICHON, avocate générale honoraire à la Cour de cassation ;
- monsieur Gérard POIROTTE, conseiller honoraire à la Cour de cassation ;
- monsieur Patrick PUGES, personnalité qualifiée en matière de communications électroniques.



Le secrétariat général de la CNCTR se composait, à la même date, d'une secrétaire générale, d'un conseiller placé auprès du président de la commission, de onze chargés de mission et de quatre agents exerçant des missions de soutien.



Compte-rendu de l'activité de la CNCTR

1. Les modifications du cadre juridique en 2020 et les perspectives d'évolution : des échéances reportées en raison de la crise sanitaire

1.1 Un cadre juridique demeuré stable en 2020

1.1.1 Une nouvelle prorogation de l'application de l'article L. 851-3 du code de la sécurité intérieure

La technique dite de l'« algorithme », codifiée à l'article L. 851-3 du code de la sécurité intérieure, avait été introduite, à titre expérimental, par l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, jusqu'au 31 décembre 2018. Un rapport sur l'application de cette disposition devait, en outre, être adressé au Parlement par le Gouvernement au plus tard le 30 juin 2018.

La première autorisation de mise en œuvre de cette technique n'ayant été délivrée qu'à compter du 12 octobre 2017, les échéances indiquées ci-dessus avaient été reportées, à la demande du Gouvernement, respectivement aux 30 juin et 31 décembre 2020 par l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

Le 18 mai 2020, la CNCTR a été saisie pour avis de deux articles d'un projet de loi tendant, notamment, à proroger d'une année supplémentaire, jusqu'au 31 décembre 2021, l'expérimentation de la technique. Le Gouvernement faisait valoir que les conditions sanitaires exceptionnelles résultant de l'épidémie de Covid-19 rendaient difficile l'examen par le Parlement, en temps utile et dans des conditions de débat appropriées,

d'un projet de loi spécifique portant sur les conditions de la pérennisation ou de la suppression de l'article L. 851-3 du code de la sécurité intérieure⁴.

Réunie en formation collégiale plénière, la CNCTR a estimé, par un avis du 20 mai 2020⁵, que, compte tenu du contrôle étroit qu'elle exerce sur cette technique, du contexte sanitaire exceptionnel, des incertitudes pesant sur l'issue de la crise ainsi que du bouleversement du calendrier parlementaire provoqué par cette crise, la prorogation pour un an de l'expérimentation en cours n'appelait pas d'observation de sa part.

L'article L. 851-3 du code de la sécurité intérieure prévoit que le Premier ministre peut, après avis de la CNCTR, imposer aux opérateurs de communications électroniques et aux fournisseurs de services sur internet la mise en œuvre, sur leurs réseaux, de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste. Les algorithmes ne portent que sur des données de connexion, sans permettre d'identifier les personnes auxquelles se rapportent ces données. Ce n'est que lorsque des données susceptibles de révéler une menace terroriste ont été détectées que le Premier ministre peut, après un nouvel avis de la CNCTR, autoriser le recueil par les services de renseignement de ces seules données détectées ainsi que l'identification des personnes auxquelles elles se rapportent.

Dans une décision classifiée du 27 avril 2017, le Premier ministre a fixé les règles générales de mise en œuvre des algorithmes, en reprenant l'ensemble des observations et recommandations formulées par la CNCTR dans une délibération classifiée du 28 juillet 2016. Trois traitements automatisés sont aujourd'hui en fonctionnement. Le premier a été autorisé en 2017, les deux autres en 2018.

Le projet de loi prévoyant la prorogation de l'application de l'article L. 851-3 du code de la sécurité intérieure a été présenté en Conseil des

4 - La CNCTR a examiné deux articles d'un projet de loi relatif à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure. L'article 2 de ce projet visait à proroger d'un an l'expérimentation de la technique prévue par l'article L. 851-3 du code de la sécurité intérieure. L'article 3 rendait cette disposition applicable dans les collectivités de l'article 74 de la Constitution ainsi qu'en Nouvelle Calédonie.

5 - Voir la délibération de la CNCTR n°1/2020 du 20 mai 2020, publiée en annexe n°1 au présent rapport et sur le site internet de la commission.

ministres le 17 juin 2020 puis soumis au Parlement. Il a été définitivement adopté le 17 décembre 2020 et promulgué le 24 décembre suivant.

L'article 2 de la loi n° 2020-1671 du 24 décembre 2020 relative à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure prévoit : « *L'article L. 851-3 du code de la sécurité intérieure est applicable jusqu'au 31 décembre 2021. Le Gouvernement adresse au Parlement un rapport sur l'application de cette disposition au plus tard le 30 juin 2021* ».

1.1.2 Une première demande de révision du contingent applicable au recueil de données de connexion par *IMSI catcher*

Les dispositions de l'article L. 851-6 du code de la sécurité intérieure autorisent le recueil, au moyen d'un appareil ou d'un dispositif technique de type *IMSI catcher*, des données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que des données relatives à la localisation des équipements terminaux utilisés.

Le recueil de données de connexion par *IMSI catcher* fait partie des techniques de renseignement soumises au principe de contingentement en application duquel le nombre d'autorisations de mise en œuvre simultanément en vigueur ne peut excéder un maximum fixé par décision du Premier ministre après avis de la CNCTR.

Le nombre total d'appareils ou de dispositifs techniques pouvant être simultanément autorisés en application de l'article L. 851-6 du code de la sécurité intérieure avait été fixé à 60 par un arrêté du Premier ministre en date du 15 janvier 2016 pris suivant la recommandation émise par la CNCTR dans une délibération adoptée en formation plénière le 18 décembre 2015. Le contingent était alors réparti de la manière suivante : 35 pour le ministère de l'intérieur, 20 pour le ministère de la défense, 5 pour le ministère chargé des douanes. Ce contingent n'avait, depuis, fait l'objet d'aucune demande de révision.

Saisie par le Premier ministre le 24 décembre 2020 d'un projet d'arrêté visant à augmenter le nombre maximal d'autorisations simultanément en vigueur accordées sur le fondement de l'article L. 851-6 du code de la sécurité intérieure, la CNCTR s'est prononcée par une délibération classifiée adoptée en formation plénière le 7 janvier 2021. Elle a rappelé que le principe de contingentement est destiné à opérer une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée, et doit conduire les services de renseignement à ne recourir aux techniques concernées que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi* », ainsi que l'énonce l'article L. 801-1 du code de la sécurité intérieure.

La CNCTR a estimé que le contingent initialement proposé n'était pas suffisamment proportionné au regard des intérêts fondamentaux de la Nation susceptibles d'être invoqués pour recourir à cette technique de renseignement et de l'atteinte que celle-ci porte au droit au respect de la vie privée. Elle a proposé de le limiter à 100, tous ministères confondus.

Par une décision du 11 janvier 2021, le Premier ministre a suivi l'avis de la CNCTR. Il a fixé et réparti le contingent de la manière suivante :

Intérieur	70
Défense	20
Économie, budget ou douanes	5
Justice ⁶	5
TOTAL	100

⁶ - Le service chargé du renseignement pénitentiaire (aujourd'hui dénommé service national du renseignement pénitentiaire) a été autorisé à recueillir des données de connexion par *IMSI catcher* par le décret du n°2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure. C'est pour cette raison que ce service ne figurait pas dans l'arrêté du Premier ministre en date du 15 janvier 2016.

Les techniques de renseignement soumises à contingentement

Au 31 décembre 2020, sept techniques de renseignement étaient soumises au principe de contingentement en application duquel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par décision du Premier ministre après avis de la CNCTR :

- les recueils de données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure) ;
- les interceptions de sécurité *via* le GIC (I de l'article L. 852-1) ;
- les recueils de données de connexion par *IMSI catcher* (article L. 851-6) ;
- les autorisations d'exploitation des communications internationales des personnes utilisant un identifiant technique rattachable au territoire national⁷ (V de l'article L. 854-2) ;
- les techniques d'interception de sécurité sur les réseaux exclusivement hertziens (article L. 852-2), de captation de paroles prononcées à titre privé ou d'images dans un lieu privé (article L. 853-1) et d'introduction dans un lieu privé (L. 853-3) mises en œuvre par le service national du renseignement pénitentiaire (SNRP) sur le fondement de l'article L. 855-1 du code de la sécurité intérieure⁸.

Les contingents, surveillés quotidiennement par le groupement interministériel de contrôle (GIC) qui en informe la commission, sont conçus comme des incitations à ne recourir aux techniques concernées que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi* », ainsi que l'énonce l'article L. 801-1 du code de la sécurité intérieure.

⁷ - Ces autorisations seront ci-après désignées par l'acronyme « AETN ».

⁸ - Voir les points 1.1.1 et 1.1.3.3 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

Tableau récapitulatif des contingents en vigueur à la date de publication du présent rapport, par ministère et par technique

	Intérieur	Défense	Économie, budget ou douanes	Justice	TOTAL
Recueils de données de connexion en temps réel <i>(article L. 851-2)</i>	650	50	20	/	720
Recueils de données de connexion par IMSI catcher <i>(article L. 851-6)</i>	70	20	5	5	100
Interceptions de sécurité <i>(I de l'article L. 852-1)</i>	3 050	550	150	50	3 800
« AE-TN » Communications <i>(article L. 854-2)</i>	750	210	40	/	1 000
Interceptions de sécurité sur les réseaux exclusivement hertziens mises en œuvre sur le fondement de l'article L.855-1	/	/	/	20	20
Captations de paroles prononcées à titre privé ou captations d'images dans un lieu privé mises en œuvre sur le fondement de l'article L.855-1	/	/	/	20	20
Introductions dans un lieu privé mises en œuvre sur le fondement de l'article L.855-1	/	/	/	20	20

1.2 Les perspectives d'évolution du cadre juridique : un calendrier bouleversé par la crise sanitaire

1.2.1 Un débat parlementaire attendu avant le 31 décembre 2021 sur le devenir de la technique dite de l'algorithme

Ainsi que cela a été exposé au point 1.1.1 du présent rapport, le Parlement sera amené à débattre, en 2021, du devenir de la technique de renseignement prévue par l'article L. 851-3 du code de la sécurité intérieure consistant à mettre en œuvre des algorithmes sur des données de connexion issues des réseaux des opérateurs de communications électroniques, à la seule fin de détecter une menace terroriste. En effet, si l'article 2 de la loi du 24 décembre 2020 citée précédemment a prorogé l'application de l'article L. 851-3 du code de la sécurité intérieure jusqu'au 31 décembre 2021, le législateur devra, avant cette date, décider s'il souhaite supprimer la technique, prolonger la période expérimentale ou pérenniser les dispositions concernées.

Le débat à venir au Parlement sur une question relevant du droit du renseignement permettra sans doute de dresser un bilan plus général de l'application du cadre légal entré en vigueur en 2015. L'article 27 de la loi du 24 juillet 2015 a, au demeurant, prévu que l'application des dispositions de cette loi fasse l'objet d'une évaluation par le Parlement dans un délai maximal de cinq ans après son entrée en vigueur. En application de cet article, les commissions des lois et de la défense de l'Assemblée nationale ont créé, le 31 octobre 2019, une mission d'information commune sur l'évaluation de la loi du 24 juillet 2015 et en ont confié la présidence à monsieur Guillaume Larrivé⁹. Le rapport d'information réalisé par cette mission a été déposé le 10 juin 2020¹⁰. Il comporte plusieurs propositions de modification du cadre légal applicable au renseignement. De la même

⁹ - Député de l'Yonne et membre de la commission des lois.

¹⁰ - Ce rapport est disponible sur le site internet de l'Assemblée nationale, dans la rubrique « travaux parlementaires » / « rapports d'information » / rapport n° 3069.

manière, la délégation parlementaire au renseignement, institution commune à l'Assemblée nationale et au Sénat, chargée d'exercer le contrôle parlementaire de l'action du Gouvernement en matière de renseignement et d'évaluer la politique publique en ce domaine, a effectué un bilan de la mise en œuvre de la loi du 24 juillet 2015 et a formulé des recommandations dans la perspective de ce débat parlementaire. Le rapport public dressant le bilan de son activité, déposé le 11 juin 2020, rend compte de cette évaluation¹¹.

La CNCTR a été informée de la préparation d'un projet de loi modifiant plusieurs dispositions de la loi du 24 juillet 2015. Elle en sera préalablement saisie pour avis.

Dans son troisième rapport d'activité pour l'année 2018, la CNCTR a émis des réflexions et formulé un certain nombre de propositions destinées à renforcer la cohérence du cadre juridique applicable au renseignement et à approfondir le contrôle sur le recueil et l'exploitation des données¹².

1.2.2 Un cadre légal susceptible d'évoluer du fait de la jurisprudence des deux Cours européennes

1.2.2.1 L'arrêt rendu en grande chambre par la Cour de justice de l'Union européenne (CJUE) le 6 octobre 2020 sur la question de la conservation des données de connexion

Dans un arrêt du 21 décembre 2016 dit *Tele2 Sverige AB*, la Cour de justice de l'Union européenne (CJUE) a jugé que le droit de l'Union¹³ s'opposait à une « réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble

11 - Ce rapport est disponible sur le site internet du Sénat, dans la rubrique « travaux parlementaires » / « offices et délégations » / « délégation parlementaire au renseignement » / « rapport n° 506 (2019-2020) du 11 juin 2020.

12 - Voir en particulier le point 1.2 du troisième rapport d'activité pour l'année 2018 de la CNCTR, disponible sur le site internet de la commission.

13 - En l'espèce, la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, cette directive étant interprétée à la lumière des stipulations de la Charte des droits fondamentaux de l'Union européenne.

des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ».

L'arrêt a suscité des interrogations sur la conformité au droit de l'Union des législations des États membres qui imposent aux opérateurs de communications électroniques et aux fournisseurs de services en ligne de conserver, pendant une durée limitée, des données de connexion de tous leurs abonnés, dans l'hypothèse de l'éventuelle réquisition de ces données par l'autorité judiciaire ou par des services de renseignement. Eu égard aux difficultés qu'il soulève, tant pour la conduite des enquêtes judiciaires que pour la recherche de renseignement, il a suscité plusieurs questions préjudicielles de juridictions nationales invitant la CJUE à préciser voire reconsidérer sa position¹⁴.

Le Conseil d'État a quant à lui saisi la CJUE le 26 juillet 2018 de plusieurs questions préjudicielles à l'occasion de deux recours dirigés contre divers actes réglementaires applicables aux activités de renseignement. Ses questions portaient sur les points suivants :

- 1°) L'obligation généralisée et indifférenciée imposée aux fournisseurs constitue-t-elle une ingérence justifiée par le « droit à la sûreté » garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne ?
- 2°) La directive du 12 juillet 2002¹⁵ autorise-t-elle des mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés ?
- 3°) La directive du 12 juillet 2002 subordonne-t-elle la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ?

14 - La juridiction britannique chargée de contrôler les activités de renseignement et la Cour constitutionnelle belge ont respectivement posé à la CJUE des questions préjudicielles en ce sens les 31 octobre 2017 et 2 août 2018.

15 - Plus précisément, l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques dite « directive vie privée et communications électroniques ».

La CJUE, réunie en grande chambre, s'est prononcée dans un arrêt du 6 octobre 2020¹⁶. Sans exclure de façon absolue toute possibilité pour les États d'imposer aux opérateurs de communications électroniques une obligation de conservation des données de connexion de leurs clients, la Cour fixe d'importantes restrictions concernant à la fois la conservation et l'accès aux données, en fonction de la nature des données concernées et du motif invoqué pour justifier leur conservation et l'éventuelle autorisation d'y accéder, que ce soit dans un cadre judiciaire ou dans celui de la police administrative du renseignement.

Il appartient maintenant au Conseil d'État de juger, à la lumière des réponses apportées par la CJUE aux questions préjudicielles qu'il lui a posées, des conséquences à tirer sur le dispositif légal en vigueur permettant aux services de renseignement d'accéder, après avis de la CNCTR et décision du Premier ministre, à des données de connexion conservées par les opérateurs de communications électroniques et concernant des personnes pouvant constituer une menace. À la date de rédaction du présent rapport, l'affaire était en cours d'instruction au Conseil d'État dont la décision est attendue au cours du premier semestre 2021.

1.2.2.2 Les requêtes introduites devant la Cour européenne des droits de l'Homme (CEDH) contre plusieurs dispositions de la loi du 24 juillet 2015 relative au renseignement

Comme la CNCTR le rappelait déjà dans son quatrième rapport d'activité pour l'année 2019, quatorze requêtes¹⁷ ont été introduites devant la CEDH par des avocats et des journalistes contre la loi du 24 juillet 2015 relative au renseignement et sont toujours pendantes.

Sur le fondement des articles 8 et 10 combinés de la Convention, certains requérants soutiennent que les techniques de renseignement prévues par la loi n'ont pas de base légale suffisante. Ils estiment ainsi que la notion d'« *informations ou documents* » pouvant être recueillis au moyen d'une technique de renseignement ne serait pas définie et que la loi ne protégerait pas suffisamment les personnes exerçant la profession de

16 - Il s'agit de l'arrêt du 6 octobre 2020 rendu sur les affaires jointes C 551/18, C512/18 et C512/20.

17 - 12 requêtes ont été introduites entre le 7 octobre et le 1^{er} décembre 2015 puis 2 autres ont été introduites le 21 avril 2017.

journaliste ou d'avocat car elle ne garantirait pas, dans un cas, le secret des sources et, dans l'autre, celui des communications passées dans le cadre d'une activité de conseil.

Ils considèrent, en outre, que le législateur a retenu une définition large des finalités légales fondant la mise en œuvre de mesures de surveillance, le régime légal ainsi créé n'étant pas, selon eux, « *strictement nécessaire à la préservation des institutions démocratiques* ».

Sur le fondement de l'article 13 de la Convention, combiné avec les articles 8 et 10, les requérants se plaignent d'une insuffisance des garanties procédurales et allèguent une absence de recours effectif : d'une part, le recours instauré devant la CNCTR et le Conseil d'État ne remplirait pas les exigences conventionnelles (méconnaissance des principes d'équité, de la contradiction et de l'égalité des armes) ; d'autre part, le Conseil d'État ne pourrait être saisi directement de recours concernant des mesures de surveillance internationale ou de recueil et d'exploitation d'informations venant de services étrangers.

L'arrêt de la Cour sur ces affaires devrait intervenir après celui rendu en Grande chambre dans l'affaire Big Brother Watch (évoqué ci-dessous). Aucune indication précise de calendrier n'est disponible à la date de publication de ce rapport. En l'état actuel de la jurisprudence de la Cour en matière de renseignement¹⁸, il est délicat d'émettre des hypothèses sur l'issue de ces requêtes.

1.2.2.3 Les réflexions en cours sur le partage international de données entre services de renseignement

La CEDH, dans un arrêt du 13 septembre 2018¹⁹, a examiné pour la première fois la compatibilité de dispositions légales régissant le partage international de données entre services de renseignement avec les stipulations de la Convention de sauvegarde des droits de l'homme et des

18 - Pour une analyse plus détaillée de cette jurisprudence, le lecteur peut consulter l'étude consacrée aux « Éléments de jurisprudence européenne sur le droit au respect de la vie privée en matière de renseignement » publiée dans le troisième rapport d'activité pour l'année 2018 de la CNCTR.

19 - Il s'agit de l'arrêt de la CEDH du 13 septembre 2018, n° 58170/13, affaire Big Brother Watch et autres contre Royaume-Uni, notamment les paragraphes 422 à 424.

libertés fondamentales, en particulier le droit au respect de la vie privée. Il s'agissait en l'espèce du cadre légal britannique²⁰.

Dans cette affaire, portant exclusivement sur les « flux entrants », la Cour a estimé que, comme pour tout dispositif permettant d'obtenir des renseignements, celui consistant à recevoir des données de partenaires étrangers devait avoir une base légale, accessible et prévisible, ainsi qu'être proportionné et contrôlable de manière adéquate. Elle a précisé que pourrait constituer une garantie adaptée le fait de subordonner l'exploitation de ces « flux » au respect des exigences légales applicables à la mise en œuvre de techniques de renseignement sur le territoire de l'État receveur et, qu'à tout le moins, la législation nationale devrait entourer de garanties la conservation, l'exploitation, la transmission et la destruction des données issues de ces échanges.

Cet arrêt de chambre n'est cependant pas définitif. Le 4 février 2019, le collège de la Grande chambre a, en effet, accepté la demande des requérants de lui renvoyer l'affaire. L'audience s'est tenue le 10 juillet 2019. Au moment de la rédaction du présent rapport, la CNCTR ne disposait pas d'information sur la date à laquelle l'arrêt serait rendu.

20 - Après avoir observé que les services britanniques ne pouvaient exploiter de données transmises par des partenaires étrangers que sur le fondement d'une autorisation de droit interne, que cette transmission devait être proportionnée aux buts poursuivis, que les données ne pouvaient être conservées qu'aussi longtemps qu'elles étaient nécessaires à ces buts, enfin qu'un organe de contrôle indépendant, dénommé Investigatory Powers Commissioner's Office, se reconnaissait compétent pour contrôler les accords de partage international de renseignements, la CEDH a jugé que la législation britannique ne méconnaissait pas les stipulations de la Convention relatives au droit au respect de la vie privée.

La CNCTR face à la crise sanitaire résultant de la pandémie de Covid-19

Confrontée à la pandémie de Covid-19, la CNCTR s'est employée à limiter le risque sanitaire pour ses membres et ses agents ainsi que pour les personnes à leur contact tout en assurant la continuité de son activité de contrôle qui, à aucun moment, n'a été interrompue.

Durant le premier confinement qui a débuté en mars 2020, la CNCTR a mis en œuvre son plan de continuité d'activité en application duquel la présence sur le site de la CNCTR des membres et des agents a été réduite au strict nécessaire pour assurer la continuité du contrôle *a priori* des demandes d'autorisation de surveillance formulées par les services de renseignement. Les membres et agents non présents sur site ont eu recours à des formes de télétravail adaptées à la nature particulière des missions de la commission et aux exigences de confidentialité ou ont bénéficié d'autorisations spéciales d'absence.

Les réunions collégiales ont été limitées au strict nécessaire et il a été recouru, lorsque cela a été possible, aux modalités de l'article 7 du règlement intérieur de la CNCTR prévoyant l'adoption de délibérations par moyens de communications électroniques sécurisés. Les déplacements dans les services de renseignement pour les besoins du contrôle *a posteriori* ont été temporairement suspendus. L'accent a été mis sur le contrôle *a posteriori* exercé depuis les locaux de la commission grâce aux outils informatiques disponibles.

Pour accompagner la sortie du premier confinement à compter du 11 mai 2020, la CNCTR a adopté, le 20 avril 2020, un plan de retour progressif à la pleine activité. Il impliquait qu'un plus grand nombre de membres et d'agents de la CNCTR reviennent travailler sur site, dans le strict respect des mesures barrières et dans des conditions assurant leur protection.

Ce retour s'est effectué de manière graduelle et maîtrisée afin de limiter, autant que possible, la présence simultanée des agents au sein d'un espace commun. Les réunions collégiales sur site ont progressivement repris ainsi que les contrôles *a posteriori* sur pièces et sur place.

Un dispositif similaire a été appliqué durant la deuxième période de confinement et à la fin de l'année 2020. Toutefois, les contrôles réalisés sur place dans les locaux des services de renseignement ont alors pu être maintenus avec un protocole sanitaire adapté. Les réunions collégiales de la commission ont également été maintenues sur le site.

La CNCTR a dû, tout au long de l'année 2020, mettre en place une organisation destinée à garantir la continuité de son activité. À cette fin, des membres et des agents ont été alternativement placés en réserve pour être en mesure d'intervenir sur site en cas d'indisponibilité de collègues affectés par le virus.

2. Le contrôle *a priori* des demandes d'autorisation de mise en œuvre des techniques de renseignement : une mission prioritaire dont la continuité a été assurée malgré la crise sanitaire

Au cours de l'année 2020, la CNCTR a dû adapter son organisation et ses modalités de travail aux contraintes engendrées par la crise sanitaire. Malgré ces contraintes, elle a veillé à ce que la continuité du contrôle préalable soit assurée.

En dépit du contexte sanitaire, le contrôle préalable de la CNCTR a porté en 2020 sur un volume de demandes tendant à la mise en œuvre de techniques de renseignement supérieur à celui constaté en 2019 (+ 8 %).

Il s'est, comme les années précédentes, exercé sur l'intégralité des demandes formulées par les services. Aucune demande n'a, en effet, été présentée selon la procédure d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure, qui dispense le Premier ministre, dans des cas exceptionnels, de consulter la CNCTR avant d'autoriser la mise en œuvre de certaines techniques.

Les moyens financiers et humains de la CNCTR

Composée d'un collège de neuf membres qui s'appuie sur un secrétariat général de dix-sept agents, la CNCTR dispose d'un budget propre qu'elle gère en toute indépendance.

Les crédits alloués par le Parlement à la CNCTR sont inscrits au budget général de l'État (mission « Direction de l'action du Gouvernement », programme n° 308 « Protection des droits et libertés », action n° 12 « Commission nationale de contrôle des techniques de renseignement »).

La loi de finances initiale pour 2020²¹ a attribué à la CNCTR des montants de 2,3 millions d'euros pour ses dépenses de personnel et de 365 000 euros pour ses dépenses de fonctionnement. Comme en 2019, ces crédits ont été presque entièrement consommés.

En raison de la diminution du nombre de déplacements effectués par les membres et les agents de la commission pour contrôler l'activité des services de renseignement sur l'ensemble du territoire national, les dépenses de fonctionnement ont connu une légère baisse en 2020. Celle-ci a cependant été, en partie, compensée par une augmentation des dépenses liées à l'achat et la maintenance des matériels informatiques constituant le réseau interne sécurisé de la commission. Enfin, ces dépenses ont contribué à l'aménagement des locaux de la CNCTR, qui sont caractérisés par un niveau de sécurité très élevé, destiné à respecter toutes les règles prévues par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

21 - Voir la loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020.

2.1 Une activité soutenue face au maintien de la menace terroriste à un niveau élevé, dans un contexte de pandémie mondiale

Comme dans ses quatre précédents rapports d'activité, la CNCTR présente des statistiques sur les techniques de renseignement relevant de la surveillance intérieure, c'est à dire destinées à surveiller des personnes se trouvant sur le territoire national.

Ces éléments portent sur le nombre d'avis rendus par la commission sur les demandes d'autorisation de mise en œuvre de techniques de renseignement dont celle-ci a été saisie, sur les finalités invoquées à l'appui de ces demandes ainsi que sur le nombre de personnes surveillées.

Si la CNCTR est tenue, à travers la publication de son rapport annuel d'activité, de rendre compte de son action, elle doit prendre en considération les exigences, qui peuvent être contradictoires et qu'elle doit concilier, de transparence de l'action publique et de protection du secret de la défense nationale.

Dans son premier rapport d'activité pour la période 2015/2016, la CNCTR avait fait le choix, afin de prévenir tout risque de divulgation d'informations susceptible de nuire aux intérêts fondamentaux de la Nation, en particulier certaines méthodes opérationnelles des services de renseignement, de publier une présentation statistique consolidée du nombre d'avis rendus par technique de renseignement. Cette présentation détaillait uniquement les données relatives aux accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), aux interceptions de sécurité mises en œuvre *via* le GIC (I de l'article L. 852-1 du même code) et aux géolocalisations en temps réel (article L. 854-1 de ce code) et regroupait, dans une catégorie unique, l'ensemble des « autres techniques de renseignement ». Elle a été reconduite dans les rapports d'activité ultérieurs de la commission.

La CNCTR estime aujourd'hui, à l'aune de l'expérience tirée de ses cinq premières années d'activité, que les données statistiques relatives à chacune des techniques de renseignement prévues par le titre V du livre VIII du code de la sécurité intérieure peuvent être publiées sans que cela compromette le secret des méthodes opérationnelles des services de renseignement. Elle fournit ainsi, dans son rapport d'activité pour l'année 2020, une information plus complète sur son activité de contrôle.

Ce rapport, qui rend compte de la cinquième année d'activité de la CNCTR, est également l'occasion de porter un regard sur l'évolution de l'utilisation des techniques de renseignement sur l'ensemble de la période 2016-2020.

Par ailleurs, ainsi qu'elle le fait depuis son troisième rapport d'activité pour l'année 2018, la commission indique le nombre d'avis préalables qu'elle a rendus en 2020 sur les demandes relevant de la surveillance des communications électroniques internationales.

Les éléments statistiques figurant dans ce rapport sont le fruit d'un travail d'extraction et d'agrégation de données conduit par la CNCTR conjointement avec le GIC, puis de fiabilisation des résultats.

2.1.1 Le nombre d'avis préalables rendus par la CNCTR en matière de surveillance intérieure : une augmentation des demandes d'accès aux données de connexion conjuguée à une baisse des autres demandes, notamment celles relatives aux techniques les plus intrusives

En matière de surveillance intérieure, les avis préalables rendus par la CNCTR se répartissent comme indiqué dans le tableau général ci-dessous.

Les chiffres indiqués dans ce tableau incluent l'ensemble des demandes présentées par les services de renseignement au titre des années 2016 à 2020.

	2016	2017	2018	2019	2020	Évolution 2019/ 2020	Évolution 2016/ 2020
Accès aux données de connexion en temps différé (identification d'abonnés ou recensement de numéros d'abonnement) (article L. 851-1 du code de la sécurité intérieure)	32 096	30 116	28 741	25 051	30 758	+ 22,8%	- 4,2%
Accès aux données de connexion en temps différé (autres demandes, dont celles de « factures détaillées ») (article L. 851-1 du code de la sécurité intérieure)	15 021	18 512	17 443	14 568	18 006	+ 23,6%	+ 19,9%
Accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure)	368	115	278	1 184	1 644	+ 38,9 %	+ 346,7 %
Géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure)	2 426	3 751	5 191	7 601	8 394	+ 10,4 %	+ 246 %
Localisations des personnes ou des objets (« Balisages ») (article L. 851-5 du code de la sécurité intérieure)	1 048	1 330	1 510	1 793	1 598	- 10,9 %	+ 52,5 %
Recueils de données de connexion par IMSI catcher (article L. 851-6 du code de la sécurité intérieure)	254	277	272	288	311	+ 8 %	+ 22,4 %
Interceptions de sécurité via le GIC (I de l'article L. 852-1 du code de la sécurité intérieure)	8 137	8 758	10 562	12 574	12 891	+ 2,5 %	+ 58,4 %
Interceptions des communications par IMSI catcher (II de l'article L. 852-1 du code de la sécurité intérieure)	6	0	0	0	0	-	- 100 %
Interceptions de sécurité sur les réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure)	0	1	3	3	0	- 100 %	-

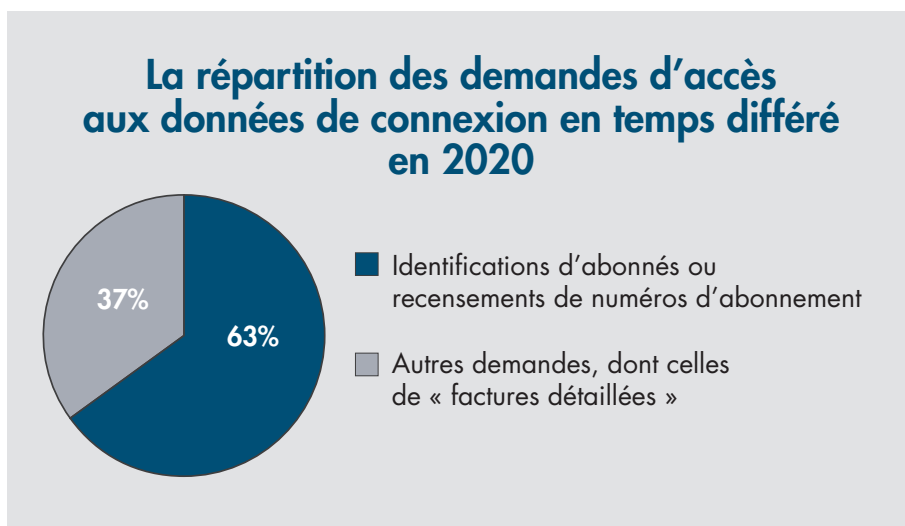
	2016	2017	2018	2019	2020	Évolution 2019/ 2020	Évolution 2016/ 2020
Captations de paroles prononcées à titre privé et captations d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure)	2 427	2 438	3 003	3 282	1 564	- 52,3 %	- 35,6 %
Recueils et captations de données informatiques (article L. 853-2 du code de la sécurité intérieure)	2 713	2 518	3 082	3 591	2 418	- 32,7 %	- 10,9 %
	2016	2017	2018	2019	2020	Évolution 2019/ 2020	Évolution 2016/ 2020
Introductions dans des lieux privés (article L. 853-3 du code de la sécurité intérieure)	2 598	2 571	3 206	3 599	2 021	- 43,8 %	- 22,2 %
	2016	2017	2018	2019	2020	Évolution 2019/ 2020	Évolution 2016/ 2020
Ensemble des techniques de renseignement	67 094	70 390	73 298	73 543	79 605	+ 8,2 %	+ 18,6 %

Ce tableau fait apparaître que, s'il était resté stable entre 2018 et 2019, le nombre total de demandes tendant à la mise en œuvre de techniques de renseignement enregistre en 2020 une augmentation d'environ 8 %. Ce résultat global recouvre toutefois des évolutions contrastées selon les techniques de renseignement considérées.

Technique de renseignement la plus utilisée mais la moins intrusive de toutes celles prévues au livre VIII du code de la sécurité intérieure, les demandes d'**accès aux données de connexion en temps différé** (article L. 851-1 du code de la sécurité intérieure) affichent, en 2020, une hausse de près de 23 %, interrompant ainsi le recul observé depuis deux ans. Cette hausse, appliquée à un volume de demandes représentant plus de 60 % du total des demandes de techniques, explique l'augmentation constatée en 2020 de 8 % de l'ensemble des techniques de renseignement.

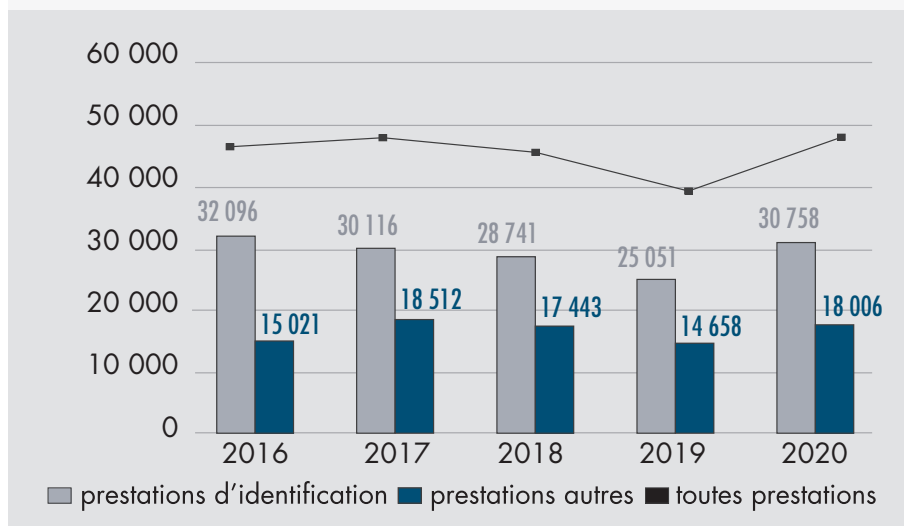
Il est rappelé qu'en application de la méthode de comptabilisation de la commission, une demande présentée sur le fondement de l'article L. 851-1 du code de la sécurité intérieure est susceptible de porter sur plusieurs accès à la fois. Ainsi, une demande de recensement de numéros d'abonnement téléphonique d'une personne peut entraîner le recueil de plusieurs numéros auprès de plusieurs opérateurs de communications électroniques et, partant, l'émission de plusieurs réquisitions.

Comme le montre le graphique ci-dessous, la répartition entre prestations d'identification et autres prestations, parmi lesquelles les factures détaillées ou « fadets », s'inscrit dans une proportion approchant, respectivement, deux tiers/un tiers qui est stable depuis 2016.



Le nombre total de demandes d'accès aux données de connexion en temps différé demeure globalement stable à l'échelle des cinq années d'activité de la commission puisqu'il affiche une hausse totale de 3 % par rapport à 2016. La distinction entre les prestations d'identification et les « autres » prestations fait cependant apparaître un recul de 4 % des premières compensé par une augmentation de près de 20 % des secondes.

Évolution de la répartition des demandes d'accès aux données de connexion entre 2016 et 2020



Les demandes de **géolocalisations en temps réel** (article L. 851-4 du code de la sécurité intérieure) ont poursuivi leur progression en 2020 bien que celle-ci, de l'ordre de 10 %, soit plus modérée que celle constatée l'année précédente. Les demandes de géolocalisations en temps réel sont celles qui ont le plus significativement augmenté durant la période 2016-2020 (+ 246 %).

Les demandes d'**interceptions de sécurité** réalisées *via* le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) ont de nouveau crû en 2020 bien que le taux d'augmentation, s'élevant à 2,5 %, soit nettement inférieur à ceux constatés en 2018 et 2019, lesquels atteignaient respectivement 20 et 19 %.

La volumétrie concernant les **autres techniques de renseignement** enregistre sur l'année écoulée un recul global de 25 %. Cette importante baisse touche la quasi-totalité des techniques composant cet agrégat puisque seules les demandes d'accès aux données de connexion en temps réel et les recueils de données de connexion par *IMSI catcher* connaissent une évolution positive entre 2019 et 2020.

S'agissant des demandes d'**accès aux données de connexion en temps réel** (article L. 851-2 du code de la sécurité intérieure), technique de renseignement soumise à contingentement, la variation sur cinq ans fait apparaître une très forte augmentation (+ 347 %). Celle-ci doit s'expliquer en partie par l'appropriation tardive par les services de renseignement de cette technique dont la mise en œuvre nécessite des capacités d'analyse technique poussées. De ce fait, son utilisation, très faible jusqu'en 2018, ne s'est effectivement développée qu'au cours de l'année 2019 et a poursuivi sa progression au cours de l'année 2020.

Les demandes de **recueils de données de connexion par IMSI catcher** (article L. 851-6 du code de la sécurité intérieure) ont augmenté en 2020 (+ 8 %) mais connaissent une évolution limitée depuis 2016 (+ 22,4 %). Cette technique, également soumise à contingentement, dont la mise en œuvre requiert le déploiement d'opérations techniques assez lourdes, a fait l'objet de 311 demandes en 2020.

Les demandes portant sur les **autres techniques de renseignement** prévues aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure ont connu, en 2020, un recul plus ou moins marqué selon les techniques concernées, en 2020. Cette baisse, probablement conjoncturelle, est l'une des conséquences de la crise sanitaire résultant de l'épidémie de Covid-19.

Il est, en effet, vraisemblable que les mesures de confinement et les restrictions de déplacement imposées durant l'année 2020 aient rendu plus difficile la mise en œuvre des techniques, souvent très intrusives, réalisées physiquement au contact de la cible.

Ainsi, le nombre de demandes d'introduction dans un lieu privé diminue en 2020 de près de 44 %. La CNCTR précise que l'introduction dans un lieu privé ne constitue pas à proprement parler une technique de renseignement autonome dans la mesure où elle ne permet pas, à elle seule, le recueil de renseignement. Elle constitue plutôt un accessoire de mise en œuvre d'autres techniques de renseignement énumérées par l'article L. 853-3 du code de la sécurité intérieure. Elle ne peut en effet

être utilisée que pour mettre en place, utiliser ou retirer les dispositifs techniques mentionnés aux articles L. 851-5, L. 853-1 et L. 853-2 du code de la sécurité intérieure, dans le respect du principe de subsidiarité, c'est-à-dire lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé.

S'agissant, enfin, de la technique de l'**algorithme** sur des données de connexion en vue de détecter une menace terroriste, aucune nouvelle autorisation de mise en œuvre n'a été sollicitée en 2020. Les trois algorithmes autorisés depuis l'entrée en vigueur du cadre légal étaient toujours en fonctionnement à la fin de l'année 2020.

Les avis défavorables rendus par la CNCTR en 2020

En 2020, la CNCTR a rendu, hors demandes d'accès aux données de connexion en temps différé prévues à l'article L. 851-1 du code de la sécurité intérieure, 262 avis défavorables, soit 0,8 % du nombre d'avis rendus.

Le taux d'avis défavorables était de 6,9 % lors de la première année de fonctionnement de la commission. Il a connu une baisse régulière depuis lors²².

Cette évolution témoigne, de manière générale, des efforts accomplis d'année en année par les services de renseignement pour se conformer à l'ensemble des exigences imposées par le cadre juridique en vigueur ainsi qu'à la doctrine établie par la CNCTR, soit en présentant des demandes mieux proportionnées à la défense ou à la promotion des intérêts fondamentaux de la Nation justifiant le recours aux techniques de renseignement, soit en renonçant à présenter des demandes vouées à la désapprobation de la commission. Elle constitue, pour la CNCTR, un indicateur de la qualité et de l'utilité du dialogue qu'elle entretient de façon continue avec les services demandeurs quant à la mise en œuvre du cadre légal.

Le taux d'avis défavorables rendus en 2020 est, au surplus, à mettre en relation avec le nombre plus limité, cette année, de demandes tendant à recourir aux techniques de renseignement les plus intrusives, sur lesquelles la commission émet davantage d'avis défavorables fondés sur la prise en compte des principes de proportionnalité et de subsidiarité.

La commission a, par ailleurs, rendu 78 avis défavorables sur les demandes d'accès aux données de connexion en temps différé, soit un ratio de 0,2 % des avis rendus sur cette technique. Ce chiffre est identique à celui constaté en 2019.

Comme les années précédentes, le Premier ministre n'a, en 2020, accordé aucune autorisation après un avis défavorable de la commission. Depuis l'entrée en vigueur du cadre légal, le 3 octobre 2015, les avis défavorables de la CNCTR ont toujours été suivis par le Premier ministre.

22 - Ce taux était l'année suivante de 3,6 %, de 2,1 % en 2018 et de 1,4 % en 2019.

2.1.2 Les finalités invoquées dans les demandes de techniques de renseignement relevant de la surveillance intérieure : la prédominance de la prévention du terrorisme

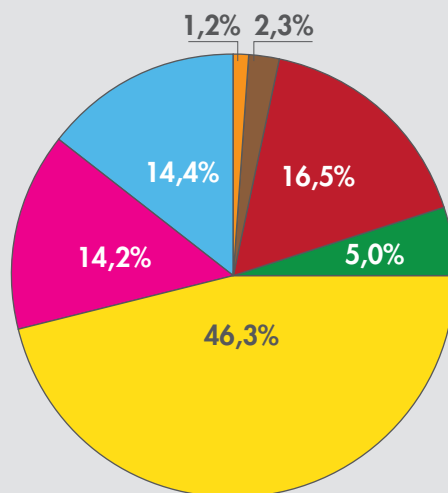
Les techniques de renseignement ne peuvent être mises en œuvre que pour la défense ou la promotion des intérêts fondamentaux de la Nation limitativement énumérés à l'article L. 811-3 du code de la sécurité intérieure²³.

Dans la continuité de la présentation retenue dans ses précédents rapports d'activité, la CNCTR mentionne, pour l'ensemble des demandes tendant à la mise en œuvre d'une technique de renseignement, la proportion de chacune des sept finalités mentionnées à l'article L. 811-3.

En outre, et ainsi que l'a rappelé la commission dans ses rapports d'activité pour les années 2018 et 2019, le service national du renseignement pénitentiaire (SNRP), service du « second cercle » relevant du ministère de la justice, peut recourir, en application de l'article L. 855-1 du code de la sécurité intérieure, à une liste limitative de techniques pour des finalités qui lui sont propres, à savoir la prévention des évasions et le maintien de la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues. En 2020, ces finalités ont été invoquées dans 0,1 % des demandes de mise en œuvre de techniques de renseignement, cette proportion demeurant comparable à celle constatée en 2019 (0,08 % des demandes). Parce qu'elles ne concernent qu'un seul service de renseignement et qu'elles demeurent toujours marginales en volume de demandes, les finalités propres au SNRP ne figurent pas dans le diagramme ci-dessous.

23 - Cette liste est reproduite dans l'encadré consacré au résumé du cadre juridique en vigueur du présent rapport.

Les finalités fondant toutes les demandes de techniques de renseignement en 2020



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- 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
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

La prévention du terrorisme, dont le premier rapport d'activité de la CNCTR avait montré qu'elle était devenue, dès janvier 2015, le fondement légal le plus fréquemment invoqué à l'appui des demandes d'interception de sécurité, est demeurée, les années suivantes, très nettement prédominante. Alors qu'un léger déclin avait été enregistré l'année dernière (la proportion de cette finalité passant de 44 % en 2018 à 38 % en 2019), la tendance s'est inversée en 2020 puisque la prévention du terrorisme a motivé plus de 46 % des demandes soumises à l'examen de la commission.

Suit, en deuxième position, avec un ratio de 20 %, le groupe de **finalités relevant des intérêts géostratégiques de la France** (indépendance et défense nationales, intérêts majeurs de la politique étrangère et prévention de toute forme d'ingérence étrangère, lutte contre la prolifération des armes de destruction massive). Le recours à ces finalités est stable d'une année sur l'autre. Par comparaison, celles-ci représentaient, en 2018 et 2019, respectivement 20 % et 18 % du fondement légal des demandes.

En troisième position, viennent deux finalités invoquées dans des proportions comparables (environ 14 %) à savoir, d'une part, **la prévention de la criminalité et de la délinquance organisées** et, d'autre part, **la prévention des violences collectives de nature à porter gravement atteinte à la paix publique**. Par comparaison, ces taux étaient respectivement de 18 % et 13 % en 2019.

Le recul relatif de la finalité de prévention de la criminalité et de la délinquance organisées, en 2020, s'explique probablement par les mesures de restriction voire d'interdiction de déplacement adoptées dans le cadre de l'état d'urgence sanitaire.

La proportion occupée par la prévention des violences collectives de nature à porter gravement atteinte à la paix publique est en augmentation constante depuis trois ans. Après être passée de 6,2 % à 9,5 % en 2018 puis à 13,8 % en 2019, elle atteint 14,2 % en 2020. La CNCTR rappelle qu'elle se montre particulièrement vigilante sur les demandes fondées sur cette finalité, considérant que la prévention des violences collectives ne saurait être interprétée comme permettant la pénétration d'un milieu syndical

ou politique ou la limitation du droit constitutionnel de manifester ses opinions, fussent-elles extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.

En quatrième et dernière position, la finalité relative à **la défense et à la promotion des intérêts économiques, industriels et scientifiques majeurs de la France** représente cette année 5 % des demandes examinées par la CNCTR, en recul d'environ six points par rapport à 2019. Cette diminution marquée constitue probablement, là encore, une conséquence directe de la pandémie de Covid-19 qui a entraîné une réduction drastique de l'activité économique.

2.1.3 Le nombre de personnes surveillées au moyen de techniques de renseignement relevant de la surveillance intérieure : une légère diminution en 2020

La CNCTR a repris, comme chaque année, l'indicateur qu'elle avait créé à l'occasion de son premier rapport d'activité²⁴ et a calculé le nombre de personnes ayant fait l'objet, en 2020, d'au moins une technique de renseignement prévue aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure. Comme les années précédentes, ce chiffre ne comprend pas les accès aux données de connexion en temps différé mentionnés au deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, c'est-à-dire les identifications d'abonnés ou les recensements de numéros d'abonnement²⁵.

Les éléments de calcul utilisés comportent une marge d'erreur, évaluée à moins de 10 %, dès lors que les demandes tendant à la mise en œuvre de techniques de renseignement sont présentées par technique et non par personne, que le traitement informatisé des demandes n'a pas encore été

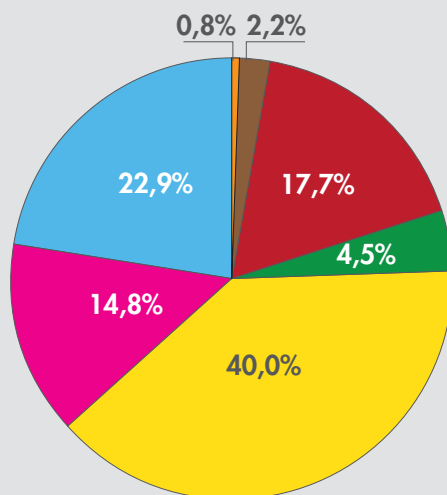
24 - Voir le point 3.3 du premier rapport d'activité 2015/2016 de la CNCTR.

25 - La CNCTR considère en effet que les identifications d'abonnés et les recensements de numéros d'abonnement constituent moins une mesure de surveillance à proprement parler qu'un acte préparatoire à des mesures de surveillance. De telles mesures commencent, pour la CNCTR, dès l'obtention de « factures détaillées » de la personne concernée en application du même article L. 851-1 du code de la sécurité intérieure.

entièrement harmonisé et, enfin, que certaines personnes faisant l'objet de surveillance ne sont pas nommément identifiées. Cependant, grâce aux développements informatiques constamment conduits par le GIC et à l'amélioration progressive des outils conçus par la commission lors de sa première année de fonctionnement, la fiabilité du calcul a été renforcée.

	2016	2017	2018	2019	2020	Évolution 2019/ 2020	Évolution 2016/ 2020
Nombre de personnes surveillées	20 360	21 386	22 038	22 210	21 952	- 1,2 %	+ 7,8 %
Dont, au titre de la prévention du terrorisme	9 475 (46,5 % du total)	9 157 (42,8 % du total)	8 579 (38,9 % du total)	7 736 (34,8 % du total)	8 786 (40 % du total)	+ 13,6 %	- 7,3 %
Dont, au titre de la prévention de la criminalité et de la délinquance organisées	4 969 (24,4 % du total)	5 528 (25,8 % du total)	5 416 (24,6 % du total)	5 693 (25,6 % du total)	5 021 (22,9 % du total)	- 11,8 %	+ 1 %

La répartition des personnes surveillées selon les finalités motivant leur surveillance



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- 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
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

Le nombre de personnes surveillées recule de 1,2 % entre 2019 et 2020. Cette évolution contraste, en apparence, avec celle des demandes de mise en œuvre de techniques de renseignement qui enregistrent une augmentation d'environ 8 %. Cette différence peut s'expliquer, d'une part, en raison de la dangerosité de certains profils qui justifie de mettre en œuvre plusieurs techniques de renseignement à l'encontre d'une même cible et, d'autre part, par les diverses mesures de confinement qui ont parfois contraint les services à recourir à d'autres techniques que celles utilisées habituellement.

De manière cohérente avec le diagramme présentant la répartition des finalités invoquées dans les demandes de techniques de renseignement, la proportion des personnes surveillées au titre de la prévention du terrorisme, qui s'élève à 40 % en 2020 contre près de 35 % l'an passé, demeure prédominante. Elle est suivie par la prévention de la criminalité et la délinquance organisées qui justifie la surveillance de 23 % des cibles.

On observe, par ailleurs, tout comme en 2019, une progression (de 13,6 % à 14,8 %) de la proportion de personnes surveillées sur le fondement de la prévention des violences collectives de nature à porter gravement atteinte à la paix publique. La part des personnes surveillées sur le fondement de la défense et de la promotion des intérêts économiques, industriels et scientifiques majeurs de la France est en forte diminution (de 10,4 % en 2019 à 4,5 % en 2020), de manière cohérente avec ce qui a été dit plus haut sur la part de cette finalité dans les demandes.

2.1.4 Le nombre d'avis préalables rendus par la CNCTR au titre de la surveillance internationale : une augmentation témoignant de l'appropriation progressive par les services de renseignement des dispositions législatives introduites en 2018

Comme elle le fait depuis 2018, la CNCTR publie le nombre de demandes d'autorisation en matière de surveillance des communications électroniques internationales sur lesquelles elle s'est prononcée en 2020.

Les autorisations d'exploitation prévues au III de l'article L. 854-2 du code de la sécurité intérieure peuvent concerner les communications ou les seules données de connexion émises ou reçues au sein d'une zone géographique, par une organisation, par un groupe de personnes ou par une seule personne.

L'autorisation prévue, depuis l'entrée en vigueur de la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, au V du même article ne concerne, quant à elle, qu'une seule personne. Elle permet l'exploitation des communications ou des seules données de connexion de cette personne lorsque celle-ci utilise un identifiant technique rattachable au territoire national, y compris lorsqu'elle l'utilise pour communiquer depuis la France.

Quelle que soit leur nature, ces autorisations d'exploitation ne peuvent être fondées que sur les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure²⁶.

En 2020, la commission a rendu 4 316 avis sur des demandes tendant à l'exploitation de communications internationales interceptées, contre 2 133 en 2019. Alors que le nombre des autorisations d'exploitation prévues au III de l'article L. 854-2 du code de la sécurité intérieure demeure stable, les autorisations délivrées sur le fondement du V du même article affichent une forte croissance. Cette montée en puissance

²⁶ - L'autorisation prévue au V de l'article L. 854-2 du code de la sécurité ne peut être délivrée que pour la défense ou la promotion des finalités mentionnées aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du même code.

s'observe depuis le dernier trimestre de l'année 2019. La CNCTR rappelle que les autorisations permettant l'exploitation des communications internationales de personnes utilisant un identifiant technique rattachable au territoire national sont soumises à contingentement.

2.2 Un examen renforcé des dossiers les plus sensibles et des techniques de renseignement les plus intrusives

2.2.1 La stabilité du nombre de demandes de renseignements complémentaires adressées aux services de renseignement

Dans son précédent rapport d'activité, la CNCTR décrivait la procédure suivie lorsqu'elle reçoit une demande nécessitant une information plus complète de la commission²⁷. Il peut s'agir d'une demande qu'elle estime insuffisamment motivée, difficile à apprécier ou d'une légalité incertaine. Cette procédure permet à la commission de demander au service concerné, ou à son ministre de tutelle, des renseignements complémentaires, le plus souvent pour lui faire préciser les faits mis en avant pour justifier la surveillance ou les modalités de mise en œuvre de la technique sollicitée.

Il revient, ensuite, au service concerné de communiquer à la commission les éléments demandés, s'il en dispose, voire, si cela s'avère nécessaire, de compléter sa demande par des informations supplémentaires de nature à étayer la motivation qui la fonde. Selon les cas, le dialogue mené avec le service permettra à la commission de s'assurer que la personne ciblée est, de façon plausible, personnellement impliquée dans un projet susceptible d'affecter les intérêts fondamentaux de la Nation, que la menace qu'elle représente ou les intérêts publics invoqués à l'appui de sa demande peuvent justifier le recours à la mesure de surveillance sollicitée, voire que les conditions envisagées pour sa mise en œuvre sont conformes aux prescriptions légales, notamment si l'opération de surveillance nécessite de pénétrer dans un lieu privé. À défaut, la CNCTR émet un avis défavorable.

Le recours à cette procédure permet à la commission d'approfondir son contrôle *a priori*. Elle est ainsi en mesure de discerner les demandes

²⁷ - Voir le point 2.2.1 du quatrième rapport d'activité pour l'année 2019 de la CNCTR consacré à la procédure de demande de renseignements complémentaires.

entachées d'une illégalité justifiant un avis défavorable de celles qui, bien que justifiées, sont maladroitement formulées ou insuffisamment précises.

Le nombre de demandes de renseignements complémentaires adressées aux services en 2020 est stable par rapport à 2019. De 1 732 demandes (dont 836 en matière d'accès aux données de connexion en temps différé), toutes techniques et tous services de renseignement confondus en 2019, celui-ci est passé à 1 776 (dont 706 en matière d'accès aux données de connexion en temps différé) en 2020. Si ce nombre a très légèrement augmenté en valeur absolue il a, en revanche, très légèrement diminué en proportion (2,2 % du nombre total de demandes de techniques de renseignement en 2020 contre 2,4 % en 2019).

Ces éléments chiffrés témoignent ainsi d'une mise en œuvre ciblée et mesurée de cette procédure, sur un volume de demandes comparable d'une année sur l'autre.

2.2.2 La procédure de suivi des « productions » : un moyen de contrôle exhaustif permettant de vérifier la réalité de la menace et l'absence d'irrégularités

La commission rappelle que les développements informatiques entrepris et constamment améliorés par le GIC depuis 2016 lui permettent de réaliser, à tout moment, depuis ses locaux, des vérifications portant, notamment, sur les interceptions de correspondances émises par la voie des communications électroniques auprès des opérateurs (I de l'article L. 852-1 du code de la sécurité intérieure).

En la matière, la CNCTR a accès tant aux données brutes recueillies qu'aux extractions et transcriptions effectuées à partir de ces données²⁸. Comme elle l'avait expliqué dans son rapport de l'année 2019²⁹, les opérations

28 - Voir le point 2.2.1 du troisième rapport d'activité pour l'année 2018 de la CNCTR dans lequel celle-ci rappelle que l'exploitation des données recueillies peut prendre la forme d'extractions, lorsqu'une partie de ces données, par exemple une image ou une parole, est prélevée, ou de transcriptions, lorsque des données brutes font l'objet d'une transformation destinée à en faciliter l'analyse.

29 - Voir le point 3.2.2 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

de transcription, plus communément dénommées « productions », sont exclusivement réalisées dans les locaux du GIC, à partir d'une application informatique dédiée. Toutes les productions sont ensuite soumises à la validation de ce service du Premier ministre avant de pouvoir être transmises au service de renseignement et aux agents intéressés, sous la forme d'un document imprimé ou par voie dématérialisée sécurisée. Lorsque l'une de ces opérations soulève une difficulté, le GIC sollicite des explications auprès du service. Si la difficulté ne peut être surmontée, le service ne peut disposer de la transcription litigieuse.

La CNCTR assure elle aussi, depuis ses locaux, un suivi régulier de ces productions. Cette procédure peut être mise en œuvre soit de manière spontanée soit de manière programmée, certains des avis de la commission conditionnant le renouvellement éventuel d'autorisations d'interceptions de sécurité à la réalisation de ce contrôle.

Lorsque la motivation d'une demande de renouvellement³⁰ d'une interception de sécurité apparaît incomplète ou trop succincte, l'agent chargé de l'instruction préalable de cette demande effectue ce suivi en consultant l'ensemble des transcriptions (voire, le cas échéant, les extractions) réalisées par le service au cours de la dernière période d'autorisation de la technique. Il peut également solliciter des renseignements complémentaires du service demandeur.

D'une part, ce suivi permet à la commission d'apprécier le bien-fondé de la motivation de la demande soumise à son examen et de vérifier le caractère plausible de l'implication personnelle de la cible au regard de la finalité invoquée. Il est également le moyen, le cas échéant, de recueillir des éléments complémentaires lui permettant d'apprécier avec discernement le respect des principes de nécessité et de proportionnalité.

Ce suivi peut, par ailleurs, être réalisé au cours de l'instruction d'une demande qui vise à mettre en œuvre, à l'égard d'une cible faisant déjà l'objet d'une interception de sécurité, une autre technique de

30 - Cette procédure ne peut pas être mise en œuvre au stade de l'autorisation initiale puisqu'elle consiste à consulter les résultats d'exploitation de l'interception de sécurité. Elle suppose ainsi une durée minimale de fonctionnement de la technique.

renseignement plus intrusive. Il permettra alors à la commission de contrôler, en outre, le respect du principe de subsidiarité³¹, en s'assurant que les renseignements recherchés à travers cette nouvelle demande ne peuvent légalement être obtenus par un autre moyen moins attentatoire à la vie privée de la personne concernée.

D'autre part, la procédure de suivi des productions permet à la CNCTR de s'assurer que les services se bornent à recueillir des données en lien avec l'exercice de leurs missions. Elle veille, en particulier, à ce que des éléments sans rapport avec les finalités légales ne soient pas conservés par le service. Lorsque la commission relève des irrégularités, un dialogue auquel le GIC est associé est engagé avec le service concerné quant à la pertinence de la conservation des données concernées et leur rattachement à la finalité invoquée. Cet échange est susceptible de conduire à une demande de destruction de ces données³².

Une vigilance particulière est, de surcroît, portée aussi bien par le GIC que par la CNCTR aux transcriptions et extractions se rapportant à des cibles exerçant l'une des professions ou mandats protégés par les dispositions de l'article L. 821-7 du code de la sécurité intérieure³³. Le contrôle préalable du GIC est ici doublé d'un contrôle de la CNCTR qui s'assure que l'atteinte, le cas échéant portée aux garanties attachées à l'exercice de ces professions ou mandats, est nécessaire et proportionnée aux finalités légales poursuivies.

En outre, lorsque le service de renseignement, le GIC ou la CNCTR découvre ou suspecte, au stade de l'exploitation des données recueillies, que la cible exerce une profession ou un mandat protégés, l'exploitation de l'interception de sécurité est immédiatement suspendue jusqu'à ce que le service procède aux vérifications nécessaires. Si l'exercice de l'une de ces

31 - Toutes les techniques de renseignement doivent être mises en œuvre, en vertu de l'article L. 801-1 du code de la sécurité intérieure, en respectant un principe de proportionnalité entre les atteintes portées à la vie privée et les menaces affectant les intérêts fondamentaux de la Nation. En outre, les techniques les plus intrusives ne peuvent être utilisées que lorsque les renseignements recherchés ne peuvent être recueillis par un autre moyen légal : il s'agit des captations de paroles prononcées à titre privé ou des captations d'images dans un lieu privé (article L. 853-1 du code), des recueils et des captations de données informatiques (article L. 853-2 du code) et, enfin, des introductions dans un lieu privé (article L. 853-3 du code).

32 - Voir sur ce point l'encadré consacré à la procédure de détection d'une irrégularité au point 3.2.1 du présent rapport.

33 - Il est rappelé qu'aux termes de ces dispositions : « Les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats ».

professions ou mandats est confirmé, le service est tenu de présenter, afin de poursuivre l'exploitation, une demande de modification de l'autorisation dont il dispose qui sera alors examinée par la CNCTR réunie en formation plénière, comme la loi le prévoit. L'interception de sécurité ne pourra être poursuivie que si les faits justifiant la demande de surveillance peuvent être regardés comme détachables de l'exercice des fonctions ou mandats exercés par la cible, et si la mesure de surveillance est nécessaire et proportionnée à la finalité poursuivie. Dans le cas contraire, la ou les techniques en cours seront interrompues et l'ensemble des renseignements collectés et des transcriptions et extractions réalisées sera détruit.

La CNCTR bénéficie par ailleurs, depuis la fin de l'année 2020, d'un accès immédiat, depuis ses locaux, aux données recueillies, extraites ou transcrites par l'intermédiaire des techniques de captation de paroles dont la mise en œuvre fait l'objet d'une centralisation par le GIC³⁴. Bien que cette centralisation concerne encore un nombre limité d'autorisations³⁵, elle a permis un élargissement notable des capacités de contrôle de la commission qui peut désormais effectuer un suivi des productions réalisées à partir de ces techniques.

2.2.3 Des interactions nombreuses et utiles entre contrôle *a priori* et contrôle *a posteriori*

2.2.3.1 Certains dossiers instruits dans le cadre du contrôle *a priori* font l'objet d'un suivi particulier lors des contrôles *a posteriori*

Certaines demandes d'autorisation de techniques de renseignement, en raison notamment de leur caractère très intrusif, nécessitent pour la commission de réaliser un examen approfondi des dossiers concernés et d'effectuer un suivi particulièrement attentif de leur exécution.

34 - Voir, s'agissant des progrès accomplis en matière de centralisation, le point 3.2.2.2 du présent rapport.

35 - Toutes les techniques de captation de paroles ne bénéficient pas encore d'une centralisation effective. En outre, la DGSE et la DGSJ disposent chacune d'un dispositif propre de centralisation des renseignements recueillis.

La CNCTR peut alors procéder, depuis ses locaux, à une analyse détaillée des données recueillies grâce aux applications mises à sa disposition par le GIC ou demander la présentation du dossier lors d'un contrôle *a posteriori* réalisé sur pièces et sur place dans les locaux des services de renseignement. Cette décision est prise, selon les cas, soit par le membre ayant qualité de magistrat qui examine l'affaire, soit par la formation collégiale de la CNCTR.

D'une part, la CNCTR peut subordonner le renouvellement d'une autorisation à la réalisation d'un suivi exhaustif des productions issues de la précédente période d'exploitation de la technique en cause. Les éléments complémentaires d'information recueillis dans le cadre de ce suivi seront soumis à l'appréciation de la commission. Le contrôle *a priori* d'une demande d'autorisation d'une technique de renseignement déclenche ainsi, un contrôle *a posteriori* à distance, mené depuis les locaux de la CNCTR.

D'autre part, la CNCTR peut subordonner la poursuite d'une mesure de surveillance à la réalisation d'un contrôle *a posteriori*, sur pièces et sur place, au sein des locaux des services de renseignement.

Réalisés par un membre de la commission et des chargés de mission présentant des profils à la fois juridique et technique, ces contrôles sont habituellement menés à un rythme de deux, voire trois par semaine, tous services confondus.

Le dossier sera évoqué avec le service, en particulier avec les agents spécifiquement chargés de son suivi, à l'occasion de l'un des déplacements de la commission. La présentation réalisée par le service permettra à la commission d'expliquer les difficultés relevées lors de l'instruction et d'obtenir des éclaircissements ou des informations supplémentaires sur le profil de la cible, son implication dans des activités ou projets en lien avec la finalité invoquée dans la demande ou encore sur les conditions de mise en œuvre de la ou des techniques sollicitées à son encontre.

Ce contrôle qui permettra également d'accéder aux serveurs et aux applications informatiques du service portera sur la mise en œuvre de la technique (date de mise en œuvre, lieu de mise en œuvre ou encore, le

cas échéant, date d'activation ou de désactivation du dispositif technique) ainsi que sur les données recueillies, qu'il s'agisse des renseignements bruts collectés ou des transcriptions et extractions qui doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités prévues par la loi.

Ainsi la CNCTR examine, à intervalles réguliers et avec chacun des services, les dossiers qui portent sur la mise en œuvre des techniques les plus attentatoires à la vie privée, qui font l'objet d'un suivi de longue durée ou qui présentent une complexité particulière.

Enfin, la CNCTR peut organiser, dans ses propres locaux, une présentation de dossiers par le service intéressé. Il s'agira des dossiers les plus complexes, posant une question nouvelle ou sérieuse. Ces présentations ont l'avantage d'associer plus largement les membres du collège.

Ces diverses modalités de contrôle ne sont pas exclusives les unes des autres et peuvent être échelonnées ou cumulées en fonction des durées d'autorisation des techniques.

2.2.3.2 Les constats dressés au cours des contrôles *a posteriori* peuvent éclairer la commission lors de l'instruction des demandes d'autorisation présentées par les services

Chaque contrôle *a posteriori* sur pièces et sur place donne lieu à la rédaction d'un rapport détaillé. Ce document, à usage interne, est diffusé auprès de tous les membres et agents de la CNCTR. Il soulève, le cas échéant, des questions sur lesquelles le collège de la commission devra se prononcer. Lorsqu'un dossier a été abordé en contrôle *a posteriori* à la demande expresse d'un membre de la commission ou de sa formation collégiale, le rapport fait état, de manière exhaustive, des explications ou précisions fournies par le service ainsi que des difficultés demeurant, éventuellement, en suspens.

Ainsi, lorsque la CNCTR est saisie d'une demande tendant à prolonger la surveillance d'une personne ou à mettre en œuvre à son égard une technique de renseignement nouvelle, les membres de la commission sont informés des constats dressés lors des contrôles *a posteriori* portant sur cette surveillance. Il s'agira, selon les cas, de constats liés au contexte

entourant la surveillance, tel que le service le décrit, ou à ses enjeux concrets, d'un point de vue opérationnel, technique et juridique.

Par ailleurs, il arrive régulièrement que les services de renseignement évoquent, de leur propre initiative, des dossiers à l'occasion des contrôles effectués dans leurs locaux. La discussion porte, le plus souvent, sur des demandes ayant donné lieu à un avis favorable assorti d'observations voire de restrictions³⁶, ou à un avis défavorable de la commission. Elle est l'occasion, pour les représentants de la CNCTR, d'explicitier le sens de l'avis rendu et d'exposer le raisonnement sur lequel il se fonde. En retour, le service concerné peut apporter des précisions complémentaires qui ne figuraient pas dans la motivation de sa demande et ainsi donner un éclairage nouveau au dossier. La commission pourra, le cas échéant, en tenir compte au cours de l'instruction des demandes d'autorisation qui seront ultérieurement soumises à son examen, qu'il s'agisse de nouvelles demandes ou de demandes de renouvellement.

Enfin, la CNCTR est parfois informée, lors de ces contrôles, des projets de surveillance des services, avant même que ces derniers ne formulent une demande d'autorisation de mise en œuvre d'une technique de renseignement. Il peut s'agir de dossiers complexes qui donnent lieu à des interrogations de la part des services, notamment sur le caractère approprié de la finalité ou de la technique permettant de réaliser l'opération matérielle envisagée, et qui soulèvent des difficultés, le plus souvent sous l'angle du principe de proportionnalité.

Les représentants de la commission se bornent alors à rappeler le cadre juridique en vigueur ainsi que la doctrine d'application élaborée par la CNCTR depuis 2015. Ils se gardent de toute appréciation de fond tant qu'une demande d'autorisation n'est pas soumise à la CNCTR.


Ces échanges sont, pour la commission comme pour les services de renseignement, une occasion utile de faire le point sur certaines thématiques de renseignement qui nécessitent des explications détaillées. Celles-ci peuvent être fournies le cas échéant par voie écrite ou, dans les

³⁶ - Voir, pour plus de précisions, le point 3.1 du premier rapport d'activité pour la période 2015/2016 de la CNCTR ainsi que le point 2.2.2 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.



cas les plus complexes, lors de présentations aux membres du collège dans les locaux de la CNCTR.

La commission retire ainsi des contrôles *a posteriori* une connaissance approfondie des besoins et des méthodes opérationnelles de chaque service de renseignement. Elle lui permet en retour d'apprécier plus finement la portée concrète de leurs demandes et, en cas d'autorisation délivrée par le Premier ministre, de s'assurer que son exécution ne porte pas d'atteinte excessive aux libertés.



3. Le contrôle *a posteriori* de la mise en œuvre des techniques autorisées : une mission exercée en 2020 dans des conditions adaptées au risque sanitaire

En 2020, en situation de pandémie, la priorité a été donnée au contrôle préalable de l'examen des demandes d'autorisation de mise en œuvre des techniques de renseignement. Le contrôle *a posteriori* de l'exécution des demandes autorisées n'a pas pour autant été délaissé. Mais il a dû être réalisé d'une manière adaptée en fonction des effectifs disponibles et des contraintes liées à la situation sanitaire.

Durant les deux périodes de confinement, les déplacements dans les locaux des services de renseignement ont été en partie suspendus. Le contrôle *a posteriori* exercé depuis les locaux de la commission grâce aux outils informatiques disponibles a, en contrepartie, été développé.

Les déplacements dans les centres territoriaux du GIC ont également dû être limités. Ainsi, 4 déplacements seulement ont été réalisés en 2020, uniquement sur le territoire métropolitain³⁷. En comparaison, 10 visites avaient été effectuées en 2019, dont l'une en Outre-mer. Ces déplacements, conduits par des délégations du GIC et de la CNCTR respectivement composées, d'une part, du directeur du GIC ou de son adjoint et d'un ou deux responsables des cellules de soutien de la zone géographique concernée et, d'autre part, du président de la commission, d'un membre du collège et d'un chargé de mission, permettent de rencontrer les chefs des services de renseignement déconcentrés³⁸ afin de répondre aux interrogations qui leur sont propres et diffuser la doctrine de la commission³⁹.

37 - Trois de ces déplacements ont été réalisés au cours des mois de janvier et février 2020 et le quatrième a été effectué au cours du mois de septembre 2020.

38 - Il peut s'agir des services déconcentrés de la sécurité intérieure, de la police judiciaire, du renseignement territorial, de la gendarmerie nationale ou des enquêtes douanières.

39 - Voir, pour plus de précisions, le point 3.2.1 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

3.1 Une complémentarité renforcée entre les contrôles menés sur pièces et sur place au sein des services de renseignement et ceux réalisés à distance depuis les locaux de la CNCTR

La CNCTR a recours, dans le cadre du contrôle de la mise en œuvre des techniques de renseignement, à deux méthodes pour s'assurer de la conformité du recueil, de la transcription, de l'extraction et de la conservation des renseignements aux dispositions du livre VIII du code de la sécurité intérieure.

La première méthode consiste à opérer des vérifications depuis les locaux de la commission grâce aux outils informatiques mis à sa disposition par le GIC. Ces applications offrent à la CNCTR un accès direct aux données recueillies, voire, pour certaines techniques, aux transcriptions et extractions réalisées à partir de ces données.

La seconde méthode consiste en la réalisation de contrôles sur pièces et sur place au sein des services de renseignement, ces contrôles pouvant porter sur l'intégralité des techniques entrant dans le champ de compétence de la commission.

3.1.1 Le développement de nouvelles modalités de contrôle à distance pour s'adapter aux mesures destinées à limiter la pandémie de Covid-19

Jusqu'à présent, les contrôles sur pièces et sur place au sein des services de renseignement étaient diligentés par une équipe composée le plus souvent d'un membre et de deux ou trois chargés de mission présentant des profils à la fois juridique et technique. Ces contrôles étaient menés à un rythme de deux, voire trois par semaine, tous services confondus. 105 contrôles sur pièces et sur place avaient ainsi été réalisés en 2019.

Les mesures imposées par la situation sanitaire ont conduit la CNCTR à diminuer le nombre de ses déplacements dans les locaux des services de renseignement et même à les suspendre entièrement pendant la première période de confinement. En dépit de ces contraintes et grâce à la forte mobilisation de ses agents, la commission a néanmoins réussi à réaliser 76 contrôles sur pièces et sur place en 2020.

Ces contrôles ont été concentrés sur la période comprise entre les deux confinements. Ils ont, en priorité, concerné les services mettant en œuvre le plus grand nombre de techniques de renseignement, les dossiers d'une sensibilité ou d'une technicité particulière ainsi que les techniques pour lesquelles la CNCTR ne dispose pas encore d'outil de contrôle à distance depuis ses locaux, en particulier les techniques les plus intrusives ou celles utilisées en matière de surveillance des communications électroniques internationales.

Les contrôles ont été réalisés dans un format adapté au risque sanitaire et aux effectifs disponibles. La composition de la délégation de la CNCTR a ainsi été limitée à deux personnes, le plus souvent la personnalité qualifiée accompagnée d'un chargé de mission. Des mesures comparables de réduction du nombre de personnes présentes durant les contrôles ont été appliquées par l'ensemble des services de renseignement de sorte que ces contrôles ont pu se dérouler dans des conditions de sécurité satisfaisantes.

Afin de compenser la baisse du nombre des contrôles sur pièces et sur place et poursuivre l'activité de contrôle de la mise en œuvre des techniques de renseignement, la CNCTR a cherché à développer les contrôles réalisés à distance, depuis ses locaux. Elle a, d'une part, exploité l'ensemble des capacités offertes par les outils informatiques mis à sa disposition par le GIC et d'autre part, mis en place de nouvelles modalités d'échanges avec les services de renseignement à partir des moyens de communication sécurisés disponibles. Ces deux démarches sont complémentaires puisque le constat d'une irrégularité relevée depuis les locaux de la CNCTR donne toujours lieu à un échange, par tous moyens, avec le service concerné.

La CNCTR rappelle, en premier lieu, que les applications développées par le GIC lui offrent un accès exhaustif aux données recueillies par la mise en œuvre des techniques de recueil de données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), de géolocalisation en temps réel (article L. 851-4 du même code), de balisage (article L. 851-5 du même code) et d'interception de correspondances émises par la voie des communications électroniques auprès des opérateurs (I de l'article L. 852-1 du même code). À la toute fin de l'année 2020, elle s'est, en outre, vu doter par le GIC de postes informatiques lui permettant d'avoir accès aux renseignements collectés par la mise en œuvre de la technique de captation de paroles (article L. 853-1 du code) qui commence à faire l'objet d'une centralisation effective par le GIC.

La CNCTR a, ainsi, mis à profit l'ensemble de ses accès à distance pour diligenter des contrôles, parfois exhaustifs, de certains dossiers.

En outre, le recours à la procédure de suivi des « productions » décrite au point 2.2.1 du présent rapport a été généralisé. La sélection des dossiers contrôlés a reposé sur l'application et la combinaison de différents critères tenant, notamment, au profil de la cible surveillée, au caractère incomplet ou imprécis de la motivation de la demande d'autorisation ou encore à la durée des surveillances autorisées.

La CNCTR a, en second lieu, mis en place de nouvelles modalités d'échanges avec les services, utilisant l'ensemble des moyens de communication sécurisés qu'elle partage avec eux.

Cette procédure de contrôle « dématérialisé » est mise en œuvre en deux temps. La première étape a pour objet d'identifier, à partir des outils à la disposition de la commission et des éléments déjà en sa possession depuis l'autorisation initiale, les points sur lesquels des compléments d'information, des vérifications ou des précisions doivent être demandés au service. La seconde consiste à transmettre au service de renseignement, *via* des moyens de communication sécurisés, les questions et demandes d'information pour lesquelles des réponses sont jugées indispensables.

La CNCTR a ainsi été amenée à adresser aux services de renseignement des questions portant sur le fond de certains dossiers, à leur demander des

précisions sur les modalités de mise en œuvre de certaines techniques, à solliciter des informations sur les renseignements collectés (qui peuvent concerner leur nature ou leur volume par exemple) ou sur les données « pertinentes » conservées au-delà des délais légaux. Elle a également, dans certains cas, invité les services à lui transmettre les transcriptions réalisées à partir des techniques de renseignement ainsi que, le cas échéant, les notes ou bulletins de renseignement que ces transcriptions avaient permis d'établir. Enfin, elle a parfois sollicité des éléments ou des éclairages complémentaires sur des thématiques particulières suivies par les services.

Cette procédure n'a cependant pas permis d'obtenir tous les résultats escomptés car peu de services de renseignement ont jusqu'à présent accepté de s'engager dans la démarche initiée par la commission.


3.1.2 Une mise en œuvre à consolider face aux réserves manifestées par les services de renseignement

Pour justifier leurs réserves, plusieurs services de renseignement ont mis en avant des considérations de sécurité liées aux modalités de communication à distance et de transmission dématérialisée de certains documents.

La commission s'est efforcée de prendre en considération les spécificités relatives à la sensibilité de certains dossiers ou de certaines thématiques. Elle a ainsi maintenu certains déplacements dans les locaux des services de renseignements lorsque la communication des éléments nécessaires à l'exercice de sa mission de contrôle était impossible ou inappropriée par voie dématérialisée.

En outre, la mise en œuvre de cette procédure de contrôle a été limitée aux dossiers et thématiques relevant de certaines finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure, jugées les moins sensibles.

Cette procédure, même circonscrite aux dossiers les moins délicats, peine encore aujourd'hui à recueillir l'adhésion des services de renseignement.




Si la majorité d'entre eux n'ont pas expressément refusé de coopérer, les réponses aux sollicitations de la CNCTR ont souvent été partielles et longues à obtenir.

La réticence de certains services de renseignement a, en conséquence, obligé la CNCTR à diligenter des contrôles sur pièces ou place pour obtenir les informations et précisions demandées, en dépit d'un contexte sanitaire dégradé.

Les difficultés d'exercice du contrôle *a posteriori* en situation de pandémie ont permis de dégager des enseignements.

Le principal d'entre eux a trait à la nécessité pour la CNCTR de bénéficier d'un accès sécurisé direct, complet, permanent et immédiat à l'ensemble des données recueillies au moyen des techniques de renseignement ainsi qu'aux outils permettant de les exploiter. Cette exigence vaut tout particulièrement en matière de surveillance des communications électroniques internationales, pour laquelle la commission ne dispose actuellement d'aucun moyen de contrôle à distance.

La poursuite de l'essor des contrôles à distance ne vient cependant pas rendre moins pertinents les contrôles sur pièces et sur place. Ceux-ci donnent l'occasion d'un dialogue fructueux avec les services de renseignement. Ils doivent être poursuivis à un rythme adapté au contexte sanitaire.



3.2 L'approfondissement du contrôle du recueil et de l'exploitation des données issues des techniques de renseignement : une entreprise à long terme qui progresse

Bien que la mise en œuvre des contrôles à distance ait connu un résultat mitigé, la CNCTR dresse, à l'instar des années précédentes, un bilan positif des contrôles sur pièces et sur place et se montre satisfaite des conditions dans lesquelles ses délégations ont été accueillies.

3.2.1 Une application sérieuse du cadre légal : des irrégularités en nombre limité et de faible portée

Qu'il s'agisse des contrôles diligentés en matière de surveillance intérieure comme de ceux portant sur la surveillance des communications électroniques internationales, la CNCTR constate que les services de renseignement s'acquittent de leurs obligations légales avec sérieux bien que certaines irrégularités, de faible portée, soient constatées.

Ces irrégularités ont toutes été rapidement corrigées par les services concernés.

Si, en 2019, la CNCTR avait, à deux reprises, fait usage de son pouvoir de recommander l'interruption d'une technique de renseignement et de détruire les données recueillies, elle n'a, en 2020, pas eu à recourir à cette faculté prévue à l'article L. 833-6 du code de la sécurité intérieure.

Les irrégularités constatées au cours de l'année 2020 se répartissent en plusieurs catégories, de nature et d'importance variables. Elles concernent aussi bien la surveillance intérieure que celle des communications électroniques internationales. Certaines catégories avaient déjà été relevées en 2019⁴⁰, d'autres sont nouvelles.

40 - Voir le point 3.1.1 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

3.2.1.1 Les irrégularités constatées en matière de surveillance intérieure

La **première catégorie d'irrégularités** constatées en 2020 par la CNCTR consiste en des retranscriptions d'interceptions de sécurité ne présentant aucun lien apparent avec l'une des finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure.

La détection de ces irrégularités résulte de la mise en œuvre de la procédure de suivi des « productions » décrite au point 2.2.1 du présent rapport. Cette procédure est notamment utilisée pour la préparation des contrôles sur pièces et sur place dans les locaux des services de renseignement et permet, en outre, de réaliser des contrôles dématérialisés complets de certains dossiers.

Lorsqu'une irrégularité de cette nature est détectée, la CNCTR engage un dialogue approfondi avec le service concerné afin de recueillir ses observations avant de décider du sort de la ou des transcriptions litigieuses.

De la détection à la destruction d'une production irrégulière : une procédure concertée avec les services et le GIC

En complément des vérifications opérées par le GIC⁴¹ sur l'ensemble des transcriptions réalisées par les exploitants des services de renseignement à partir des interceptions de sécurité, les agents de la CNCTR examinent également ces « productions », pour la préparation des contrôles menés sur pièces et sur place ou lorsqu'ils réalisent des contrôles dématérialisés depuis les locaux de la commission, afin d'apprécier leur pertinence au regard des finalités motivant l'autorisation à laquelle elles se rapportent.

La détection d'une production litigieuse donne lieu, après un éventuel échange avec le service concerné au cours du contrôle diligenté dans ses locaux, à l'envoi d'un message sécurisé l'invitant à faire valoir, dans un délai que précise la CNCTR, ses observations sur les motifs susceptibles de justifier la conservation des transcriptions concernées. À défaut, il lui est demandé de procéder à la destruction des données irrégulièrement conservées et d'en rendre compte à la commission.

Le GIC est systématiquement informé de ces échanges et associé à la mise en œuvre de cette procédure. Toute destruction de productions par le service donne lieu à la rédaction d'un procès verbal et à la transmission de celui-ci au GIC. Ce dernier procédera à la suppression, dans ses applications informatiques, de la ou des productions concernées.

Les observations formulées par un service de renseignement souhaitant conserver les données contestées sont examinées par la CNCTR qui détermine si, à la lumière de ces précisions, une telle conservation apparaît justifiée ou si lesdites données doivent, au contraire, être détruites. Si cela s'avère nécessaire, la commission peut exercer son pouvoir de recommander que les transcriptions effectuées soient détruites, en application de l'article L. 833-6 du code de la sécurité intérieure.

41 - Voir le point 3.2.2 du quatrième rapport d'activité pour l'année 2019 de la CNCTR et le point 2.2.1 du présent rapport.

Au cours de l'année écoulée, la CNCTR a vérifié la pertinence d'une quarantaine de productions concernant seize cibles différentes. Cela a conduit à la destruction de certaines données par les services concernés, laquelle a été opérée dans des délais jugés satisfaisants par la commission.

La **deuxième catégorie d'irrégularités** constatées concerne des extractions ou des transcriptions de données ne présentant aucun lien avec la cible faisant l'objet de la technique de renseignement.

Alors qu'aucune irrégularité de cette nature n'avait été identifiée en 2019 trois cas ont été identifiés au cours de l'année 2020. Les données irrégulièrement conservées ont été détruites dans les plus brefs délais.

La **troisième catégorie d'irrégularités** constatées en matière de surveillance intérieure concerne la traçabilité de l'exploitation des données recueillies.

En 2019, la CNCTR avait relevé plusieurs anomalies relatives à la traçabilité de l'exécution des techniques de renseignement autorisées. La commission rappelle qu'en application de l'article L. 822-1 du code de la sécurité intérieure, un relevé de mise en œuvre de chaque technique de renseignement, mentionnant les dates de début et de fin de mise en œuvre ainsi que la nature des renseignements collectés, doit être établi. Ce relevé, plus couramment désigné « fiche de traçabilité », est tenu à la disposition de la commission qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement.

Contrairement à l'année précédente, aucune divergence entre les mentions portées dans une fiche de traçabilité et la mise en œuvre effective de la technique correspondante n'a été constatée en 2020. De même, aucune carence dans la production de ces fiches n'est à signaler. Des retards persistent mais se raréfient.

La CNCTR a, en revanche, décelé plusieurs anomalies en matière de traçabilité de l'exploitation des données recueillies au cours de l'année 2020. Dans une dizaine de cas, elle a été informée par les exploitants des services de renseignement rencontrés au cours des contrôles sur pièces et sur place de l'existence de transcriptions issues de techniques de renseignement. Lorsque la CNCTR a souhaité les consulter sur

les applications informatiques des services concernés, celles-ci ne s'y trouvaient pas. La CNCTR a exigé que les transcriptions manquantes lui soient communiquées dans les plus brefs délais et qu'elles soient, en outre, intégrées dans les applications informatiques dédiées.

La CNCTR n'a cependant pas détecté de volonté délibérée de dissimulation ou de contournement du cadre légal. Elle estime que ces anomalies témoignent plutôt des difficultés d'appropriation des bonnes pratiques par les agents des services de renseignement. En dépit des efforts déployés par les équipes juridiques de ces services pour formaliser, expliquer et diffuser le cadre d'emploi des techniques de renseignement⁴², les procédures internes visant à centraliser l'ensemble des extractions et transcriptions réalisées dans des applications informatiques accessibles à la CNCTR ne sont pas encore correctement appliquées.

La CNCTR souligne, néanmoins, que les démarches initiées par les services en 2017 et poursuivies depuis lors ont permis le développement d'outils informatiques désormais fonctionnels qui lui permettent d'assurer un contrôle efficace de l'exploitation des renseignements collectés.

Dans un seul cas, constitutif de la **quatrième catégorie d'irrégularité**, la CNCTR a constaté que la technique de recueil de données de connexion par *IMSI catcher* prévue par l'article L. 851-6 du code de la sécurité intérieure avait été mise en œuvre au moyen d'un dispositif technique ne figurant pas dans le registre spécial mentionné au II du même article. Cette irrégularité a révélé que le service concerné avait omis de mettre à jour son registre. Cette mise à jour a été effectuée dans les jours suivant le contrôle.

Deux dernières catégories d'irrégularités, déjà été décrites en 2019, ont à nouveau été constatées en 2020.

D'une part, la commission a identifié, à une seule reprise en 2020, un court dépassement du délai légal de conservation des renseignements bruts collectés. Par comparaison, huit cas de ce type avaient été relevés en 2019.

42 - Voir le point 3.1.3.2 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

D'autre part, la commission a relevé, à une seule reprise en 2020 (trois fois en 2019), un dépassement de la durée d'autorisation d'une technique de renseignement. Ce dépassement, utilisé pour procéder au retrait d'un dispositif technique de surveillance installé dans un lieu privé, était de très courte durée et a été spontanément signalé par le service concerné.

3.2.1.2 Les irrégularités constatées en matière de surveillance des communications électroniques internationales

Comme en matière de surveillance intérieure, la CNCTR réalise des contrôles réguliers des conditions de recueil, de conservation et d'exploitation des données issues de la surveillance des communications électroniques internationales, en application de l'article L. 854-9 du code de la sécurité intérieure.

En l'absence d'accès direct, depuis ses locaux, à ces données, l'essentiel des contrôles est réalisé sur pièces et sur place, au sein des services de renseignement. Ces contrôles mettent en évidence, depuis 2015, une appropriation progressive et désormais solide par ces services, du cadre légal applicable en matière de surveillance dite « internationale », en dépit de sa complexité.

En outre, de récents développements informatiques déployés par les services de renseignement, en concertation avec la CNCTR, ont permis d'améliorer la traçabilité des actions effectuées par les exploitants et, ce faisant, d'approfondir et faciliter les contrôles de la commission.

La CNCTR a pu relever, au cours de l'année 2020, des irrégularités se répartissant en deux grandes catégories. La plupart d'entre elles ont été signalées aux services concernés au cours des contrôles et rapidement corrigées.

La **première catégorie d'irrégularités** concerne des exploitations réalisées sur le fondement d'une autorisation inappropriée. La CNCTR rappelle qu'aux termes de l'article L. 854-2 du code de la sécurité intérieure, le Premier ministre peut délivrer différents types d'autorisation d'exploitation des données (de connexion ou de contenu) interceptées par les réseaux de communications électroniques internationales. Ainsi, il

peut autoriser l'exploitation non individualisée des données de connexion interceptées (II du même article), l'exploitation des communications ou des seules données de connexion, relatives à des zones géographiques, à des organisations, à des groupes de personnes ou à des personnes (III) ou encore l'exploitation des communications ou des seules données de connexion, de numéros d'abonnement ou d'identifiants techniques rattachables au territoire national dont l'utilisateur communique depuis ce territoire (V).

L'exploitation de ces données est réalisée par des agents spécialisés, à partir d'applications informatiques spécifiques dont les droits et les conditions matérielles d'accès sont strictement limités et contrôlés.

La CNCTR a découvert, à quelques reprises, que des exploitations de données avaient été informatiquement rattachées non à l'autorisation pertinente mais à une autre autorisation en cours de validité. Au regard des explications fournies par les services, la commission a constaté que ces irrégularités résultaient d'erreurs de manipulation de l'outil informatique ou d'inattention et ont été rapidement corrigées. Les formations dispensées aux agents ainsi que les nombreux rappels effectués par les équipes juridiques des services de renseignement portent leurs fruits et permettent de faire progressivement diminuer ces irrégularités.

La **seconde catégorie d'irrégularités** concerne des transcriptions réalisées dans le cadre de l'exploitation de communications utilisant un identifiant technique rattachable au territoire national, au titre d'une finalité légale non autorisée pour cette autorisation. L'autorisation prévue au V de l'article L. 854-2 du code de la sécurité intérieure ne peut être délivrée que pour la défense ou la promotion d'un nombre limité de finalités. Il s'agit de celles mentionnées aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du même code. À deux reprises au cours de l'année 2020, la CNCTR a toutefois constaté que les éléments transcrits et conservés par le service concerné se rattachaient à une finalité différente, non prévue dans cette liste, de celle ayant servi de fondement à l'autorisation délivrée par le Premier ministre. Le service concerné a admis le caractère irrégulier des deux transcriptions, lesquelles ont été détruites dans les jours suivant les contrôles au cours desquels elles ont été détectées.

Comme elle l'indiquait dans son rapport d'activité pour l'année 2019, le constat d'une irrégularité, quelle que soit la suite que la CNCTR entend lui réserver, donne systématiquement lieu à un échange approfondi entre la commission et le service concerné. Il permet d'identifier précisément la ou les étapes des processus internes au cours desquels est survenue l'irrégularité afin de déterminer les éventuels ajustements à apporter pour prévenir toute réitération.

La commission estime en effet que, si l'article L.833-6 du code de la sécurité intérieure lui accorde la faculté d'adresser une recommandation au service concerné tendant à l'interruption d'une technique de renseignement et à la destruction de renseignements indûment collectés, sa mission ne se limite pas à cette démarche. Elle cherche ainsi à accompagner et, dans certains cas, à guider la mise en œuvre de bonnes pratiques au sein des services de renseignement pour assurer le plein respect du cadre légal.

3.2.2 Un contrôle *a posteriori* qui doit encore être facilité et perfectionné : des évolutions toujours attendues en matière d'accès, de centralisation et de traçabilité de l'exploitation des données recueillies

3.2.2.1 Un approfondissement continu et progressif du contrôle *a posteriori* à l'épreuve des réserves des services de renseignement

La CNCTR s'efforce, d'année en année, d'approfondir et de perfectionner son contrôle *a posteriori* conformément à la mission qui lui a été confiée par la loi.

Dans un premier temps, la CNCTR avait en priorité fait porter ses contrôles *a posteriori* sur le respect des dispositions régissant le recueil et la conservation des données collectées. Consciente des difficultés rencontrées par les services de renseignement pour saisir et respecter l'ensemble des exigences imposées par le nouveau cadre légal établi en 2015, la commission a accompagné ces services dans leurs efforts d'appropriation des règles juridiques, d'adaptation de leurs méthodes et de leurs outils de travail ainsi que de formation de leur personnel.

À partir de l'année 2018, la commission a souhaité, en outre, renforcer son contrôle sur la phase d'exploitation des données recueillies, en particulier sur la réalisation, la diffusion et la conservation des transcriptions et des extractions de ces données⁴³. Les renseignements bruts collectés par la mise en œuvre d'une technique de renseignement sont, en effet, exploités afin d'en tirer les informations pertinentes, qui seront ensuite intégrées dans les documents d'analyse produits par les services de renseignement. Cette exploitation, qui consiste à examiner et à trier les données brutes recueillies, peut prendre la forme d'extractions ou de transcriptions qui pourront être conservées tant qu'elles demeurent indispensables à la poursuite des finalités qui ont motivé leur réalisation.

La CNCTR avait alors demandé aux services contrôlés de répertorier, pour les dossiers qu'elle avait prévu d'aborder au cours de ses contrôles *a posteriori*, toutes les transcriptions et les extractions réalisées à partir de données recueillies au moyen de techniques de renseignement. Ce recensement devait faire apparaître tous les lieux de conservation de ces transcriptions et extractions et indiquer les entités ou les agents disposant d'accès aux informations ainsi que les modalités de traçabilité de ces accès.

Pour assurer son contrôle, la CNCTR dispose, en application du 2° de l'article L. 833-2 du code de la sécurité intérieure, d'un accès permanent, complet, direct et, pour certaines techniques, immédiat, aux relevés, registres, renseignements collectés, transcriptions et extractions. Cet accès est garanti par la loi, où que ces éléments se trouvent.

Dans l'hypothèse où un service de renseignement refuserait à la CNCTR l'accès à certains lieux, physiques ou logiciels, de conservation des transcriptions et des extractions, l'article L. 833-2 du code de la sécurité intérieure permet à celle-ci de demander ces éléments au Premier ministre, à l'exclusion de ceux communiqués par des services étrangers ou qui donneraient connaissance à la commission, directement ou indirectement, de l'identité des sources des services de renseignement. L'article L. 833-3 du même code punit d'un an d'emprisonnement et de

43 - Cette démarche s'est matérialisée par un courrier du 12 juillet 2018 par lequel le président de la CNCTR a rappelé, à tous les chefs de service, les dispositions légales applicables et a annoncé l'approfondissement du contrôle *a posteriori*.

15 000 euros d'amende le fait d'entraver l'action de la CNCTR en refusant de lui communiquer les documents qu'elle a sollicités en application de l'article L. 833-2, en dissimulant ces documents ou en les faisant disparaître.

En pratique, d'importants progrès restent à accomplir en matière d'identification et de localisation des données recueillies par les techniques de renseignement.

En ce domaine, comme elle l'indiquait dans son rapport d'activité pour l'année 2019, la commission continue à se heurter au refus, presque unanime, des services de renseignement de lui permettre d'accéder aux données contenues dans les fichiers intéressant la sûreté de l'État au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, communément dénommés « fichiers de souveraineté »⁴⁴.

Ces services justifient leur position par le fait qu'outre les données issues de techniques de renseignement, figureraient, dans ces fichiers, des données de provenances différentes, incluant des données communiquées par des services étrangers ou des éléments susceptibles de dévoiler, directement ou indirectement, l'identité des sources des services de renseignement, non soumis au contrôle de la CNCTR⁴⁵.

Au cours de l'année 2019, des solutions alternatives à l'accès aux fichiers de souveraineté ont été proposées à la CNCTR afin qu'elle puisse exercer son contrôle sur les données issues de techniques de renseignement susceptibles de venir alimenter les notes, bulletins de renseignement et fichiers de souveraineté.

Ces propositions, jugées constructives, avaient été accueillies favorablement par la commission dans la mesure où leur mise en œuvre pouvait faire escompter des progrès en matière de centralisation des données et contribuer ainsi à améliorer l'efficacité des contrôles.

Le constat de leur mise en œuvre est cependant décevant. Les résultats initialement annoncés par les services de renseignement n'ont pas

44 - Voir notamment l'article R. 841-2 du code de la sécurité intérieure.

45 - Voir le 4° de l'article L. 833-2 du code de la sécurité intérieure.

été atteints au cours de l'année 2020. D'une part, les développements informatiques engagés ont été ralentis sous l'effet de la crise sanitaire. D'autre part, la diffusion des nouvelles consignes méthodologiques élaborées par les services pour l'exploitation des données issues des techniques de renseignement a nécessité un délai important, reportant ainsi leur application complète par les agents concernés.

3.2.2.2 Une centralisation croissante des données recueillies par la mise en œuvre des techniques de renseignement mais encore incomplète

Comme la CNCTR l'a déjà souligné dans ses précédents rapports d'activité, deux exigences légales, distinctes mais liées, conditionnent l'efficacité et la pertinence des contrôles *a posteriori* : la **centralisation** du recueil et de l'exploitation des données issues des techniques de renseignement, d'une part, la **traçabilité** de la mise en œuvre des techniques de renseignement et de l'exploitation des données recueillies, d'autre part.

La centralisation des données recueillies est indispensable à l'exercice du contrôle *a posteriori* dont la commission a été chargée par la loi. De nouvelles avancées ont eu lieu à cet égard en 2020.

Dans son rapport d'activité pour l'année 2019, la CNCTR rappelait les développements engagés par le GIC en matière de centralisation, dans son système d'information, des paroles et des images captées sur le fondement des dispositions de l'article L. 853-1 du code de la sécurité intérieure⁴⁶.

La centralisation de la technique de captation de paroles avait été officiellement lancée et généralisée⁴⁷ à l'automne 2019. Elle est devenue pleinement opérationnelle au cours de l'année 2020 en dépit de quelques dysfonctionnements, parfois récurrents, rencontrés par certains services. Des ajustements opérés par le GIC devraient permettre de surmonter ces difficultés.

46 - Voir le point 3.1.3.1 du quatrième rapport d'activité pour l'année 2019 de la CNCTR.

47 - Tous les services de renseignement sont tenus de recourir au dispositif géré par le GIC, hormis la DGSE et la DGSI, qui en ont la faculté mais non l'obligation. Ces deux services disposent, en effet, d'un dispositif propre de centralisation des renseignements recueillis.

Le dispositif mis en place par le GIC permet aux services d'exploiter dans ses centres territoriaux les renseignements collectés. Il permet à la CNCTR d'accéder, depuis ses locaux, aux renseignements collectés ainsi qu'aux transcriptions et extractions réalisées par les agents des services. Cet accès n'a cependant commencé à être pleinement effectif qu'à la fin de l'année 2020.

La centralisation de la technique de captation d'images était en cours de finalisation à la fin de l'année 2020. Quelques adaptations techniques devaient encore être apportées avant de procéder au déploiement du dispositif au début de l'année 2021. Les formations dispensées aux personnels des services de renseignement ont toutefois été retardées par la crise sanitaire.

La majorité des techniques de renseignement sont ainsi couvertes par le dispositif de centralisation du GIC, à l'exception encore des techniques de recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) et de celles de recueil et de captation de données informatiques (article L. 853-2 du même code), toutes deux caractérisées par une collecte décentralisée et des modalités diverses de stockage des données recueillies.

Les projets de développements de réseaux informatiques sécurisés capables d'acheminer des données volumineuses ont connu peu de développements au cours de l'année écoulée, laissant parfois subsister un stockage décentralisé au sein d'échelons territoriaux de certains services.

Enfin, les dispositifs propres de centralisation des données de la DGSE et de la DGSI ont connu, en 2020, des développements significatifs permettant de faciliter les contrôles de la CNCTR.

3.2.2.3 Des évolutions contrastées en matière de traçabilité de la mise en œuvre des techniques de renseignement et d'exploitation des données recueillies

L'efficacité et la pertinence des contrôles *a posteriori* dépendent aussi de la traçabilité de la mise en œuvre et de l'exploitation des techniques de renseignement.

S'agissant de la traçabilité de la mise en œuvre des techniques de renseignement, la CNCTR constate que la tendance positive constatée depuis 2017 n'a cessé de progresser depuis lors.

Un relevé de chaque mise en œuvre d'une technique de renseignement mentionnant les dates de début et de fin de mise en œuvre ainsi que la nature des renseignements collectés doit être établi. Ce relevé, plus couramment désigné « fiche de traçabilité », est tenu à la disposition de la commission qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement.

Ces fiches sont en principe rédigées dès la fin de la mise en œuvre d'une technique ou, en l'absence de mise en œuvre, dès l'arrivée à échéance de l'autorisation. Grâce aux applications mises à sa disposition par le GIC, la commission peut vérifier de façon immédiate l'existence et le contenu des relevés de mise en œuvre, qui contribuent à la préparation des contrôles sur pièces et sur place au sein des services de renseignement mais peuvent être aussi l'occasion d'échanges entre la commission et les services destinés à préciser l'état d'une technique.

Si la commission avait salué, dans son rapport portant sur l'année 2019, la diligence avec laquelle la plupart des services s'efforçaient de renseigner ces fiches de traçabilité, elle avait néanmoins constaté un certain nombre de retards voire de carences pour certains services de renseignement.

Des efforts importants ont été consentis en 2020 pour remédier à cette situation. Les procédures internes de rédaction, de révision et de transmission de ces fiches ont été revues et améliorées par les services concernés. Ainsi, aucune carence dans la production de ces fiches n'a été relevée en 2020 et les retards se raréfient.

Le GIC a, en outre, lancé une consultation associant tous les services et autorités intéressés, au titre de laquelle la CNCTR a été interrogée, en vue de clarifier et simplifier la production des fiches de traçabilité. Les évolutions retenues devraient être mises en œuvre dans le courant de l'année 2021.

S'agissant de la traçabilité de l'exploitation des données recueillies, quelques avancées ont été réalisées mais la situation n'est pas satisfaisante.

Plusieurs services de renseignement avaient développé, en 2017 et 2018, des outils de traçabilité ambitieux. Ils ont, depuis lors, été constamment corrigés et améliorés et se révèlent particulièrement utiles lors des contrôles *a posteriori* menés par la CNCTR. La traçabilité de l'exploitation des mesures de surveillance des communications électroniques internationales en est un exemple réussi. Celle-ci n'a cessé de progresser. Elle facilite et renforce notablement les possibilités de contrôle de la commission.

Ces outils sont désormais utilisés dans certains services pour tracer l'exploitation des renseignements recueillis en matière de surveillance intérieure. Dans d'autres services, le contrôle informatisé des consultations, transcriptions et extractions de données recueillies demeure toujours à construire et le développement des outils informatiques assurant la traçabilité des consultations, transcriptions et extractions des données recueillies a peu évolué depuis 2019.

4. Un usage modéré des recours contre la mise en œuvre des techniques de renseignement

4.1 Une légère diminution du nombre de réclamations adressées à la CNCTR

La CNCTR peut être saisie par toute personne qui souhaite vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Cette procédure de réclamation préalable est prévue par les dispositions de l'article L. 833-4 du code de la sécurité intérieure, en ce qui concerne la surveillance nationale, et par celles de l'article L. 854-9 du même code, en ce qui concerne la surveillance des communications électroniques internationales.

Comme la CNCTR le précisait dans ses précédents rapports d'activité, le pouvoir de vérification que la loi lui a confié porte sur les seules techniques de renseignement prévues au livre VIII du code de la sécurité intérieure, à savoir des techniques mises en œuvre par des services de renseignement pour des finalités administratives. Cette compétence n'inclut donc ni les mesures de surveillance ordonnées par l'autorité judiciaire ni celles, au demeurant illégales, que pratiqueraient des personnes privées.

La CNCTR souligne, par ailleurs, une nouvelle fois⁴⁸ que, pour des motifs de sécurité nationale, et en application des dispositions du décret n° 2015-1405 du 5 novembre 2015 relatif aux exceptions à l'application du droit des usagers de saisir l'administration par voie électronique, elle ne peut valablement être saisie que par lettre envoyée par voie postale.

48 - Cette obligation était précisée au point 5.1.1 du premier rapport d'activité pour la période 2015/2016 de la CNCTR.

La réclamation doit être présentée par la personne concernée, justifiant son identité, et mentionner, le cas échéant, les éléments techniques à partir desquels elle souhaite que les vérifications soient conduites. Ces éléments techniques, notamment des numéros de téléphone ou des adresses de messagerie électronique, doivent être assortis de justificatifs, tels qu'un contrat d'abonnement ou une facture. Les vérifications ne peuvent avoir lieu que lorsque l'ensemble de ces informations et justificatifs a été communiqué à la commission.

La CNCTR instruit les réclamations qui lui sont adressées de la même manière et en utilisant les mêmes outils que lorsqu'elle effectue un contrôle *a posteriori* depuis ses locaux de sa propre initiative.

Le nombre de réclamations reçues par la CNCTR, en 2020, est en baisse par rapport à 2019 et se rapproche des chiffres enregistrés en 2018. Cette diminution est, probablement, à mettre en relation avec la situation sanitaire. La commission relève cependant que le volume des réclamations dont elle est saisie relève du même ordre de grandeur depuis cinq ans, sans que les différences constatées d'une année sur l'autre puissent être regardées comme significatives.

	2016	2017	2018	2019	2020	Évolution 2019/ 2020	Évolution 2016/ 2020
Nombre de réclamations	49	54	30	47	33	- 29,8 %	- 32,7 %

Aucune personne n'a présenté plus d'une réclamation au cours de l'année 2020. En revanche, cinq réclamations ont été présentées par des personnes ayant déjà saisi la CNCTR au cours des années antérieures et souhaitant que des vérifications soient à nouveau conduites à leur sujet.

Le délai de réponse aux réclamations contenant toutes les informations nécessaires à leur traitement a été inférieur à deux mois⁴⁹.

Aucune réclamation n'a conduit la CNCTR à envoyer de recommandation au chef du service de renseignement concerné, au ministre dont il relève ou au Premier ministre pour que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits, conformément à l'article L. 833-6 du code de la sécurité intérieure. En conséquence, la CNCTR ne s'est pas non plus trouvée dans la situation de devoir saisir le Conseil d'État d'un recours contentieux sur le fondement de l'article L. 833-8 du code, cette voie de recours étant ouverte lorsque le Premier ministre ne donne pas suite aux recommandations de la commission.

49 - Ce délai court à compter de la date à laquelle la réclamation est en état d'être instruite. Lorsqu'une demande de pièces complémentaires (justificatifs d'identité, justificatifs d'abonnement...) a été adressée à l'auteur de la réclamation, ce délai ne commence à courir qu'à compter de la réception de ces pièces.

Le dispositif propre aux « lanceurs d’alerte »

Pour garantir qu’il soit mis fin aux éventuelles violations manifestes du cadre juridique applicable aux techniques de renseignement, l’article L. 861-3 du code de la sécurité intérieure prévoit que les agents des services de renseignement ayant connaissance, dans l’exercice de leurs fonctions, d’une telle violation, peuvent porter ces faits à la connaissance de la seule CNCTR. Il appartient alors à la commission, au vu des éléments qui lui ont été transmis, de faire usage, le cas échéant, des pouvoirs de contrôle que lui attribue la loi.

En 2020, la CNCTR n’a pas été saisie sur le fondement de l’article L. 861-3 du code de la sécurité intérieure. Ces dispositions n’ont pas reçu d’application depuis l’entrée en vigueur du cadre légal en 2015.

4.2 Une augmentation limitée du nombre de requêtes introduites devant le Conseil d'État

La procédure contentieuse spéciale prévue aux articles L.773-1 et suivants du code de justice administrative permet de demander à une formation spécialisée du Conseil d'État de vérifier qu'une technique de renseignement n'est ou n'a pas été irrégulièrement mise en œuvre à l'encontre d'une personne. Les membres et le rapporteur public de la formation spécialisée sont habilités à connaître d'informations couvertes par le secret de la défense nationale.

En ce qui concerne les techniques de renseignement relevant de la surveillance intérieure, la formation spécialisée du Conseil d'État peut être saisie, sur le fondement de l'article L. 841-1 du code de la sécurité intérieure, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR.

En ce qui concerne la surveillance des communications électroniques internationales, seul le président ou trois membres au moins de la commission peuvent présenter une requête au Conseil d'État, sauf s'il s'agit de vérifier la légalité de l'exploitation des communications de personnes utilisant des identifiants rattachables au territoire national et communiquant depuis la France. Dans ce dernier cas, toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR peut saisir le Conseil d'État, sur le fondement de l'article L. 854-9 du code de la sécurité intérieure.

En 2016, 2017, 2018 et 2019 le Conseil d'État avait respectivement été saisi de neuf, six, neuf et six requêtes concernant la mise en œuvre de techniques de renseignement. Six décisions avaient été rendues en 2016, trois en 2017, dix en 2018 et sept en 2019.

En 2020, huit nouvelles requêtes ont été enregistrées devant le Conseil d'État sur le fondement de l'article L. 841-1 du code de la sécurité intérieure. Celui-ci a statué sur sept requêtes au cours de l'année 2020,

quatre d'entre elles ayant été enregistrées en 2018 et en 2019. Plusieurs renvois d'audience ont été décidés en raison, notamment, de la situation sanitaire.

Au 31 décembre 2020, huit affaires demeuraient en instance, dont deux enregistrées en 2018 et une en 2019.

En application de l'article L. 773-3 du code de justice administrative, la CNCTR est informée de toute requête introduite sur le fondement de l'article L. 841-1 du code de la sécurité intérieure et est invitée à présenter, le cas échéant, des observations écrites ou orales. Elle a, ainsi, le statut d'observateur devant le Conseil d'État. En tant qu'autorité décisionnaire en matière d'autorisations de mise en œuvre des techniques de renseignement, le Premier ministre, représenté par le GIC, a la qualité de défendeur.

Comme les années précédentes, la CNCTR a produit des observations sur tous les recours qui lui ont été communiqués par le Conseil d'État.

Pour la première fois, la CNCTR s'est, en outre, trouvée en position de défendeur devant le Conseil d'État. Saisie de conclusions tendant, notamment, à l'annulation de la décision par laquelle la CNCTR avait refusé de procéder à une nouvelle instruction de la demande présentée par un requérant sur le fondement de l'article L. 833-4 du code de la sécurité intérieure, la formation spécialisée du Conseil d'État s'est estimée compétente pour en connaître.

Dans cette affaire, le requérant avait, préalablement à la demande en litige, saisi la CNCTR de deux précédentes réclamations tendant à vérifier qu'aucune technique de renseignement n'était ou n'avait été irrégulièrement mise en œuvre à son égard. À peine plus de deux mois s'étaient écoulés entre la réponse apportée à la deuxième réclamation et l'introduction de la troisième. Les trois demandes portaient sur des identifiants identiques. En outre, la réclamation en litige était la sixième adressée à la commission depuis 2017.

Dans ces conditions, la CNCTR avait répondu au requérant que les vérifications qu'il sollicitait avaient déjà été conduites et que la demande en litige, qui ne faisait état d'aucun changement de circonstances, ne

nécessitait pas de nouvelle instruction. La CNCTR estimait que cette demande, qui faisait suite à deux précédentes réclamations introduites à intervalle rapproché et portant sur des identifiants identiques, présentait à la fois un caractère répétitif et systématique et pouvait, dès lors, être regardée comme abusive.


L'article L. 311-2 du code des relations entre le public et l'administration prévoit, en matière de droit à communication des documents administratifs, que l'administration n'est pas tenue de donner suite aux « *demandes abusives, en particulier par leur nombre ou leur caractère répétitif ou systématique* ». Cette faculté n'est pas expressément offerte à la CNCTR s'agissant des réclamations dont elle est saisie sur le fondement de l'article L. 833-4 du code de la sécurité intérieure.

Le Conseil d'État a toutefois jugé que la Commission nationale informatique et libertés (CNIL) dispose, dans le cadre de la mission qui lui est confiée, de la faculté, ouverte même sans texte, de rejeter, sous le contrôle du juge, les plaintes dont elle est saisie qui présentent un caractère abusif⁵⁰.


Par une décision n° 437571 du 21 décembre 2020, la formation spécialisée du Conseil d'État, après avoir relevé que la réclamation préalable adressée à la CNCTR par le requérant « *faisait suite à plusieurs vérifications relatives à des identifiants différents* », « *portait sur le même identifiant que celui ayant déjà fait l'objet de vérifications successives par la Commission au cours de mois précédents* » et « *n'était assortie d'aucun élément nouveau* », a estimé que la commission n'avait commis ni erreur de droit, ni erreur d'appréciation et ni détournement de pouvoir en retenant que cette demande présentait un caractère abusif.

La CNCTR ne s'est pas trouvée dans la situation d'exercer elle-même un recours contentieux devant le Conseil d'État sur le fondement des articles L. 833-8 ou L. 854-9 du code de la sécurité intérieure. Cette voie de recours est ouverte au président de la commission ou à trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission.

50 - Voir la décision CE, 10/9 SSR, 10 avril 2015, M. Houvet, n°3



En 2020, le Premier ministre a suivi tous les avis *a priori* défavorables émis par la CNCTR et les contrôles *a posteriori* effectués par la commission n'ont pas révélé d'irrégularité justifiant l'envoi d'une recommandation au Premier ministre.



Le dialogue institutionnel avec le Parlement, l'information du public et les relations internationales

Au sein de la chaîne opérationnelle conduisant au recueil et à l'exploitation du renseignement, la CNCTR se voit confier par la loi une mission de contrôle qui ne peut, en application du principe de la séparation des pouvoirs et eu égard aux exigences du secret de la défense nationale, être accomplie que par un organisme distinct non seulement du Gouvernement mais également du Parlement et du public. La CNCTR se présente, dès lors, comme un « tiers de confiance », auquel le législateur a attribué une compétence spécialisée qu'il ne peut assurer directement. En retour, la CNCTR rend compte tout au long de l'année de ses activités au Parlement et au public, dans le respect du secret de la défense nationale qui couvre ses travaux en application de l'article L. 832-5 du code de la sécurité intérieure.

La commission conduit, par ailleurs, une action internationale destinée à faire connaître le cadre légal français applicable aux activités de renseignement et à recueillir les bonnes pratiques mises en œuvre par les institutions nationales de contrôle des pays partenaires de la France.

Dans le cadre du dialogue institutionnel avec le Parlement, le président de la CNCTR a été auditionné en janvier 2020 par la mission d'information commune aux commissions des lois et de la défense de l'Assemblée nationale sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement.

En janvier 2020, il a également été entendu par la commission d'enquête chargée de faire la lumière sur les dysfonctionnements ayant conduit aux attaques commises à la préfecture de police de Paris le jeudi 3 octobre 2019.

Le président de la CNCTR a été auditionné, en février 2020, par la délégation parlementaire au renseignement.

En juin 2020, il a été reçu, aux côtés des deux membres de la CNCTR désignés en qualité de sénateurs, par le président du Sénat pour une

présentation du quatrième rapport d'activité de la commission pour l'année 2019.

Le président de la CNCTR a été auditionné, lors de l'examen au Sénat du projet de loi de finances pour l'année 2021, par le rapporteur de la commission des lois saisie pour avis concernant les moyens financiers et humains alloués à la commission pour remplir sa mission.

Outre la publication de son rapport annuel d'activité, la CNCTR entend faire connaître aux professionnels du droit, aux universitaires et à des associations de défense des libertés le cadre juridique applicable aux activités de renseignement.

En juillet 2020, invité par l'ordre des avocats de Paris à intervenir lors d'un évènement consacré à la formation continue des membres de cette profession, le président de la CNCTR a présenté le régime juridique applicable aux techniques de renseignement et a décrit le fonctionnement de la commission.

S'agissant des relations internationales, la CNCTR entretient un dialogue avec ses homologues européens dans le cadre de réunions bilatérales mais également multilatérales depuis la première rencontre des autorités nationales de contrôle en Europe organisée à Paris en décembre 2018. Cette activité a connu un net ralentissement en 2020 en raison de la situation créée par la pandémie de Covid-19. Une troisième réunion multilatérale de ce type prévue à Rome à la fin de l'année 2020, après celles organisées à Paris puis à La Haye, en décembre 2019, a ainsi dû être reportée à une date postérieure à la publication de ce rapport.

Annexe

Annexe

Délibération de la CNCTR n° 1/2020 du 20 mai 2020

Saisie pour avis le 18 mai 2020 par le ministre de l'intérieur, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a examiné deux articles d'un projet de loi relatif à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure. L'article 2 du projet vise à proroger d'un an l'expérimentation de la technique de renseignement dite « algorithmique » prévue par l'article L. 851-3 du code de la sécurité intérieure. L'article 3 rend cette disposition applicable dans les collectivités de l'article 74 de la Constitution ainsi qu'en Nouvelle-Calédonie.

L'expérimentation de la technique prévue par l'article L. 851-3 du code de la sécurité intérieure a été initialement autorisée jusqu'au 31 décembre 2018 par l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Cette échéance a été reportée, à la demande du Gouvernement, au 31 décembre 2020 par l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. En application de ce texte, le Gouvernement doit adresser un rapport au Parlement sur l'application de l'article L. 851-3 au plus tard le 30 juin 2020.

Le ministre de l'intérieur fait valoir que les conditions sanitaires exceptionnelles résultant de l'épidémie de Covid-19 rendent difficiles l'examen par le Parlement en temps utile et dans des conditions de débat appropriées d'un projet de loi spécifique portant sur les conditions de la pérennisation ou de la suppression de cette disposition. Le projet de loi propose en conséquence de proroger d'un an la durée de l'expérimentation.

L'étude d'impact accompagnant le projet de loi dresse un état des lieux du cadre juridique en vigueur et rappelle les enjeux de lutte contre le terrorisme dans lesquels s'inscrit la technique de « l'algorithme ».

La commission rappelle que l'article L. 851-3 du code de la sécurité intérieure prévoit que le Premier ministre peut, après avis de la CNCTR, imposer aux opérateurs de communications électroniques et aux fournisseurs de services sur internet la mise en œuvre sur leurs réseaux de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste. Les algorithmes, qui ne peuvent porter que sur des données de connexion, ne doivent pas permettre d'identifier les personnes auxquelles se rapportent les données qu'ils traitent. Ce n'est que lorsque des données susceptibles de révéler une menace terroriste ont été détectées que le Premier ministre peut, après un nouvel avis de la CNCTR, autoriser le recueil par les services de renseignement de ces seules données détectées ainsi que l'identification des personnes auxquelles elles se rapportent. Dans une décision classifiée du 27 avril 2017, le Premier ministre a fixé les règles générales de mise en œuvre des algorithmes, en reprenant l'ensemble des observations et recommandations formulées par la CNCTR dans une délibération classifiée du 28 juillet 2016. Trois traitements automatisés sont aujourd'hui en œuvre. Le premier a été autorisé en 2017, les deux autres en 2018.

Eu égard au contrôle étroit qu'elle exerce sur la technique prévue par l'article L. 851-3 du code de la sécurité intérieure et aux considérations développées par le ministre de l'intérieur tenant au contexte sanitaire exceptionnel, aux incertitudes pesant sur l'issue de la crise ainsi qu'au bouleversement du calendrier parlementaire, la prorogation pour un an de l'expérimentation en cours n'appelle pas d'observations de la part de la CNCTR.



Hôtel de Cassini - 32 rue de Babylone - 75007 Paris