

N° 4308
ASSEMBLÉE NATIONALE
CONSTITUTION DU 4 OCTOBRE 1958
QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale
le 1^{er} juillet 2021

N° 729
SÉNAT
SESSION ORDINAIRE DE 2012-2013

Enregistré à la Présidence du Sénat
le 1^{er} juillet 2021

RAPPORT PUBLIC

FAIT

AU NOM DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

*relatif à l'activité de la **délégation parlementaire au renseignement**
pour l'année **2020-2021**,*

PAR Mme FRANÇOISE DUMAS,

Députée,

Présidente de la délégation

PAR M. FRANÇOIS-NOËL BUFFET,

Sénateur,

Premier vice-président de la délégation

SOMMAIRE

Pages

CHAPITRE 1^{ER} BILAN D'ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT DE JUIN 2020 À JUIN 2021	11
I. UNE COMPOSITION PARTIELLEMENT RENOUVELÉE	11
II. LA PERMANENCE DU CONTRÔLE PARLEMENTAIRE DU RENSEIGNEMENT, MALGRÉ LA CRISE SANITAIRE	13
A. LES THÈMES DE TRAVAIL DE L'ANNÉE ÉCOULÉE	14
B. LES DOCUMENTS TRANSMIS À LA DÉLÉGATION	15
C. LES PERSONNALITÉS AUDITIONNÉES	16
III. LE RENFORCEMENT DES PRÉROGATIVES DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT	17
IV. LE SUIVI DES RECOMMANDATIONS 2019-2020 DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT	21
A. SUR LE BILAN DES LOIS DE 2015	21
B. SUR LE RENSEIGNEMENT PÉNITENTIAIRE	23
C. SUR LA MAÎTRISE DES RISQUES	24
D. SUR LE RENSEIGNEMENT SPATIAL	26
E. SUR LA CYBERDÉFENSE	27
F. RECOMMANDATIONS GÉNÉRALES DE LA COMMISSION DE VÉRIFICATION DES FONDUS SPÉCIAUX	28
CHAPITRE 2 LES ENJEUX D'ACTUALITÉ LIÉS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT	29
I. ACTIVITÉS ET RESSOURCES DES SERVICES DE RENSEIGNEMENT	29
A. LES FAITS MARQUANTS DE L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT EN 2019	29
B. LES RESSOURCES ALLOUÉES AU RENSEIGNEMENT ONT POURSUIVI LEUR PROGRESSION	30
1. Les ressources budgétaires	30
2. Les ressources humaines	31

C. LES COOPÉRATIONS	31
1. Les coopérations opérationnelles thématiques.....	31
2. Les coopérations techniques	32
II. LA PERSISTANCE D'UNE MENACE TERRORISTE À UN NIVEAU ÉLEVÉ ..	33
A. DEPUIS 2015 : UNE MENACE TERRORISTE QUI A CHANGÉ DE NATURE MAIS QUI NE FAIBLIT PAS	33
1. D'une menace projetée à une menace endogène	33
2. Les attentats commis depuis 2020 confirment l'évolution de la menace	35
B. LES ENSEIGNEMENTS TIRÉS DES ATTENTATS RÉCENTS	36
1. Renforcer les échanges avec le monde psychiatrique et les préfets dans le cadre de la lutte contre la radicalisation.....	36
2. Répondre aux signalements effectués sur les réseaux sociaux	37
C. DE NOUVEAUX DISPOSITIFS JURIDIQUES DE LUTTE CONTRE L'ISLAM POLITIQUE : LES FERMETURES DES LIEUX DE CULTE ET L'EXTENSION À LEURS DÉPENDANCES.....	38
D. DES MOTIFS DE PRÉOCCUPATION PERSISTANTS	39
1. Le suivi en détention et à la sortie de prison.....	39
2. La possible reconstitution d'une menace projetée	41
III. L'EXTENSION DES FICHIERS DE POLICE ET DE GENDARMERIE PAR TROIS DÉCRETS DU 2 DÉCEMBRE 2020.....	43
A. LES PRINCIPALES MODIFICATIONS APPORTÉES PAR LES DÉCRETS	45
B. LES GARANTIES PRÉVUES PAR LES TEXTES.....	45
C. UNE EXTENSION QUI FAIT L'OBJET D'UN RECOURS DEVANT LE CONSEIL D'ÉTAT	45
IV. LA REFONTE DU PLAN NATIONAL D'ORIENTATION DU RENSEIGNEMENT (PNOR).....	47
A. LA VOCATION DU PNOR EN TANT QU'OUTIL DE PILOTAGE	47
B. LES PRINCIPALES MENACES IDENTIFIÉES PAR LE PNOR.....	48
1. Les menaces terroristes	48
2. L'anticipation des crises et risques de ruptures majeures.....	48
3. La défense et la promotion de notre économie :	48
4. Les menaces transversales	48
5. *****	49
C. LES FICHES D'ORIENTATION STRATÉGIQUE.....	49

V. L'IMPACT DE LA JURISPRUDENCE EUROPÉENNE SUR L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT ET LE PROJET DE LOI RELATIF À LA PRÉVENTION D'ACTES DE TERRORISME ET AU RENSEIGNEMENT	51
A. UNE JURISPRUDENCE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME FONDÉE SUR LE RESPECT DE LA VIE PRIVÉE.....	51
B. UN CONTRÔLE DE LA CJUE LIÉ AUX OBLIGATIONS REPOSANT SUR LA CONSERVATION DES DONNÉES PERSONNELLES	52
1. 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, dite <i>ePrivacy</i>	53
2. Le contrôle exercé par la CJUE sur le respect de cette directive et l'arrêt <i>Tele2</i> ...	54
C. UN CADRE NATIONAL CONFORTÉ PAR LA JURISPRUDENCE DU CONSEIL D'ÉTAT ET LES ÉVOLUTIONS APPORTÉES PAR LE PROJET DE LOI RELATIF À LA PRÉVENTION D'ACTES DE TERRORISME ET AU RENSEIGNEMENT, MAIS LA PERMANENCE D'ENJEUX COMPLEXES.....	56
1. Les garanties apportées par le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement	56
2. La nécessité d'anticiper sur les exigences posées par le droit européen.....	57
a. Une action sur le droit de l'Union européenne.....	57
b. La question des échanges d'informations avec les services étrangers.....	57
CHAPITRE III LA CONTINUITÉ DES MISSIONS DE RENSEIGNEMENT PENDANT LA CRISE SANITAIRE	59
I. LE RISQUE PANDÉMIQUE EST CLAIREMENT IDENTIFIÉ, MAIS INSUFFISAMMENT SUIVI PAR LES SERVICES DE RENSEIGNEMENT	59
A. UN RISQUE PRIS EN COMPTE PAR LA REVUE STRATÉGIQUE DE DÉFENSE ET DE SÉCURITÉ NATIONALE DE 2017	59
B. POURTANT, LES SERVICES DE RENSEIGNEMENT N'AVAIENT, JUSQU'ALORS, DÉVELOPPÉ AUCUNE CAPACITÉ D'ANTICIPATION	60
II. MALGRÉ LE CONFINEMENT, LES SERVICES ONT ASSURÉ LA CONTINUITÉ DE LEURS MISSIONS ESSENTIELLES	61
A. LORSQUE LA CRISE SANITAIRE S'EST DÉCLARÉE, TOUS LES SERVICES DE RENSEIGNEMENT NE DISPOSaient PAS D'UN PLAN DE CONTINUITÉ D'ACTIVITÉ ADAPTE	61
1. Un document indispensable pour surmonter une crise nouvelle et soudaine	61
2. Les plans de continuité d'activité des services ont rapidement évolué pour prendre en compte la situation sanitaire.....	61
B. UNE ACTIVITÉ RÉDUITE ET RECENTRÉE SUR LES MISSIONS PRIORITAIRES	62
1. L'organisation interne des services.....	62
2. Une activité concentrée sur les missions jugées essentielles.....	62

3. La coopération internationale a été sensiblement ralentie par la crise, au contraire de la coopération interservices	62
4. Un recours au télétravail très restreint	63
C. DES CONSÉQUENCES SUR LE RECRUTEMENT LIMITÉES	64
III. PENDANT LA CRISE SANITAIRE, LES MENACES PESANT SUR LA FRANCE ET SES INTÉRÊTS N'ONT PAS FLÉCHI	65
A. LA CRISE N'A PAS EU DE CONSÉQUENCE SUR L'ÉVOLUTION DE LA MENACE TERRORISTE, TOUJOURS AUSSI PRÉGNANTE	65
B. LES TENTATIVES D'INGÉRENCE N'ONT PAS CONNU DE RÉELLE ÉVOLUTION, MAIS LES RISQUES SE SONT ACCENTUÉS	65
C. LES TRAFICS ET LES FRAUDES N'ONT PAS BAISSÉ NON PLUS.....	65
D. DES DIFFICULTÉS SE SONT FAIT JOUR AU SEIN DE CERTAINS ÉTABLISSEMENTS PÉNITENTIAIRES.....	66
CHAPITRE IV LE RENSEIGNEMENT TERRITORIAL, MAILLON CLÉ DE LA SÉCURITÉ INTÉRIEURE	67
I. LE RENSEIGNEMENT DE PROXIMITÉ EN PREMIÈRE LIGNE FACE AUX NOUVEAUX RISQUES D'ATTEINTE À L'ORDRE PUBLIC ET À LA PRÉVENTION DU TERRORISME.....	67
A. LA MULTIPLICATION DES PHÉNOMÈNES CONTESTATAIRES	67
1. Des contestations plus nombreuses et plus radicales.....	67
2. ... qui concernent l'ensemble du territoire.....	68
3. ...amplifiées par les réseaux sociaux	69
4. ...et qui s'accompagnent d'une recrudescence des violences	69
B. LES MOUVEMENTS SÉPARATISTES LIÉS AUX DÉRIVES RELIGIEUSES.....	71
C. LA MENACE TERRORISTE ENDOGÈNE	72
II. LONGTEMPS CONSIDÉRÉ COMME LE PARENT PAUVRE DU RENSEIGNEMENT INTÉRIEUR, LE RENSEIGNEMENT TERRITORIAL RESTE EN CONSTRUCTION.....	75
A. LES RÉFORMES DE 2008 ET 2014 ET L'AFFIRMATION PROGRESSIVE DU RENSEIGNEMENT TERRITORIAL	75
B. LE SCRT, UN SERVICE « BAROQUE »	77
C. UNE MONTÉE EN PUISSANCE RAPIDE DEPUIS 2014, ET QUI N'EST PAS ENCORE ACHEVÉE	78
1. Le renforcement des effectifs.....	78
2. Le renforcement des moyens budgétaires.....	81
3. Le renforcement de la filière « recherche et appui »	81
D. DES FRAGILITÉS PERSISTANTES.....	81
1. La difficulté à prioriser les missions.....	81
2. L'absence d'autonomie.....	83

3. Des freins techniques	84
4. Des prérogatives juridiques encore limitées	86
a. Un accès aux techniques de renseignement limité à certaines finalités	86
b. Un accès restreint aux fichiers de souveraineté.....	86
c. Le cloisonnement avec les informations de nature judiciaire	87
III. PLUTÔT QU'UNE NOUVELLE REFORME, LE RENSEIGNEMENT TERRITORIAL A SURTOUT BESOIN DE MOYENS OPÉRATIONNELS PLUS ADAPTÉS À L'EXERCICE DE SES MISSIONS.....	87
1. Créer au sein du ministère de l'intérieur une direction générale réunissant le SCRT, la SDAO et la DRPP.	88
2. Doter le renseignement territorial de budgets opérationnels de programme « BOP » dédiés.....	88
3. Confier au renseignement territorial le chef de filât sur la prévention et le suivi des subversions violentes.	88
4. Promouvoir la mobilité des agents.....	89
5. Renforcer les compétences du renseignement territorial par un recrutement plus diversifié et des formations adaptées aux besoins des missions de renseignement.	89
6. Faire du dialogue avec les élus des territoires un critère d'évaluation des cadres du renseignement territorial.	90
7. Doter le SCRT d'un réseau classifié sécurisé.....	90
8. Prévoir un plan pluriannuel de modernisation des matériels.....	90
9. Donner à la filière « recherche et appui » du SCRT les moyens humains et matériels de sa montée en puissance.....	91
10. Autoriser l'accès du renseignement territorial aux techniques de renseignement pour la finalité 5c « subversions violentes »	91
11. Autoriser l'accès du renseignement territorial aux informations judiciairisées....	92
12. Envisager la création d'un fichier commun dédié renseignement territorial (SCRT, SDAO et DRPP)	92
CHAPITRE V RAPPORT GÉNÉRAL DE LA CVFS	93
I. PRÉSENTATION GÉNÉRALE DES FONDS SPÉCIAUX EN 2019	95
A. *****	95
B. *****	95
II. OBSERVATIONS COMMUNES À L'ENSEMBLE DES SERVICES	97
A. LE PÉRIMÈTRE D'EMPLOI DES FONDS SPÉCIAUX	97
1. Des marges de manœuvre qui persistent pour la normalisation de certaines dépenses	97
a. La bascule progressive de certaines dépenses en fonds normaux	97
b. *****	98
c. Étudier les possibilités d'anonymisation dans l'application Chorus	98

2. *****	98
B. LE NECESSAIRE RENFORCEMENT DU CONTRÔLE INTERNE	98
C. L'ACCÈS DE LA CVFS À UNE INFORMATION FIABLE ET EXHAUSTIVE	99
D. LE SUIVI DES RECOMMANDATIONS	99
III. RECOMMANDATIONS GENERALES 2019 EMISES PAR LA CVFS	103
RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU TITRE DE SON RAPPORT ANNUEL D'ACTIVITÉ 2020-2021	105
EXAMEN PAR LA DÉLÉGATION	109

AVANT-PROPOS

Mesdames, Messieurs,

L'année écoulée a une nouvelle fois montré combien les enjeux liés au renseignement prennent une place de plus en plus importante, non seulement pour notre sécurité et la défense de notre souveraineté mais aussi dans le fonctionnement de nos sociétés démocratiques.

Loin de faiblir, les menaces, omniprésentes, prennent des formes de plus en plus variées, s'affranchissent des frontières et se nourrissent du progrès technologique. Espionnage, cyberattaques, terrorisme, séparatisme, contestations violentes : les dangers des temps modernes appellent à de l'anticipation et à des réponses rapides, efficaces et proportionnées qui, dans un État de droit, se doivent d'être nécessairement respectueuses des principes démocratiques.

L'onde de choc de la pandémie de la Covid-19 a également impacté la communauté du renseignement qui a dû s'organiser pour assurer la continuité de ses missions. Mais cette année singulière ne fut en aucun cas une année blanche pour le contrôle parlementaire de la politique publique du renseignement.

Au cours des douze derniers mois, la Délégation parlementaire au renseignement a en effet connu une activité soutenue dans un contexte marqué par de nouveaux attentats meurtriers et le traumatisme de l'assassinat de Samuel Paty, la résurgence d'actions violentes sur la voie publique, la multiplication d'attaques cyber contre des systèmes informatiques stratégiques ou encore des révélations d'espionnage d'État.

Cette année fut également marquée par la révision du cadre légal du renseignement. Six ans après la loi fondatrice du 24 juillet 2015, la révision de la loi renseignement est une réponse à une triple évolution :

D'abord, l'évolution de la menace terroriste, de plus en plus endogène, qui appelle à détecter le mieux possible ces signaux faibles qui alertent d'un possible passage à l'acte ; le suivi du « bas du spectre » est un défi lancé au renseignement territorial, de plus en plus souvent en première ligne.

Il y a ensuite les évolutions technologiques qui sont autant d'opportunités nouvelles pour les terroristes et les trafiquants. Qu'il s'agisse par exemple de la 5G ou de la massification à venir des communications satellitaires, la course aux technologies est une véritable course contre la montre qui ne doit souffrir aucun vide juridique ; l'enjeu pour la communauté du renseignement étant de conserver son temps d'avance.

Il était enfin nécessaire de transcrire, dans notre droit, les conséquences de la jurisprudence « Télé 2 » de la Cour de justice de l'Union européenne quant aux règles applicables à la conservation des données. La loi a tiré les enseignements de l'arrêt du Conseil d'État du 21 avril 2021 qui définit les obligations nouvelles liées

au respect du droit européen sans pour autant contraindre la puissance publique à renoncer aux outils juridiques dont elle a besoin pour nous protéger face à des menaces graves et persistantes pour la sécurité nationale.

Le débat parlementaire sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement a également permis, par voie d'amendement, de franchir une nouvelle étape dans le renforcement du contrôle parlementaire du renseignement. La Délégation parlementaire au renseignement voit en effet son rôle conforté et ses prérogatives élargies en matière de droit à l'information et de pouvoir d'audition.

Ces différents sujets, qui ont marqué l'année écoulée, ont fait l'objet de réunions, d'auditions et de déplacements de la DPR dont la synthèse des travaux figure dans le présent rapport, composé de cinq chapitres :

- Le bilan d'activité de la délégation de juillet 2020 à juin 2021 (I)
- Les enjeux d'actualité liés à la politique publique du renseignement (II)
- La continuité des missions de renseignement pendant la crise sanitaire (III)
- Le renseignement territorial (IV)
- La présentation des travaux de la Commission de vérification des fonds spéciaux (CVFS) portant sur l'exercice budgétaire 2019 (V)

À la date de l'adoption du présent rapport, le débat parlementaire sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement n'était pas achevé. Dans un souci de clarté rédactionnelle, il a été décidé, postérieurement à l'adoption du présent rapport de faire référence non plus au projet de loi, mais à la loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, définitivement adoptée par le Parlement.

Nonobstant son souci de répondre aux légitimes attentes de transparence des citoyens, les membres de la DPR ont également conscience que certaines informations portées à leur connaissance doivent être soustraites à la curiosité de nos rivaux comme de nos adversaires. C'est pour parvenir à concilier ces deux impératifs antagonistes qu'il a été décidé de masquer quelques passages sensibles au moyen d'un signe typographique (****), invariable quelle que soit l'ampleur des informations rendues ainsi illisibles.

Employé par le parlement britannique, ce procédé permet une synthèse entre des logiques ambivalentes. Nos concitoyens pourront ainsi apprécier le raisonnement déployé, sa cohérence, ses principales conclusions, tandis que certains détails resteront protégés sans que l'on puisse critiquer la vacuité du propos ou un « caviardage » excessif.

CHAPITRE I^{ER} BILAN D'ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT DE JUIN 2020 À JUIN 2021

I. UNE COMPOSITION PARTIELLEMENT RENOUVELÉE

Au cours de l'année écoulée, la composition de la délégation parlementaire au renseignement a été partiellement renouvelée à la suite, d'une part, de la démission le 17 juin 2020 de Patrice Verchère de son mandat de député et, d'autre part, des élections sénatoriales du 27 septembre 2020.

Claude de Ganay, député (LR) du Loiret a ainsi succédé à Patrice Verchère, désormais ancien député (LR) du Rhône.

Deux nouveaux sénateurs ont été désignés par le Président du Sénat pour siéger à la DPR : Agnès Canayer, sénatrice (LR) de la Seine-Maritime et Yannick Vaugrenard, sénateur (SER) de la Loire-Atlantique.

Le sénateur (LR – Rhône) François-Noël Buffet, président de la Commission des lois du Sénat, déjà membre de la DPR depuis 2015, y siège désormais en tant que membre de droit (en remplacement de Philippe Bas, sénateur (LR) de la Manche), au même titre que le sénateur Christian Cambon (LR – Val-de-Marne), Président de la Commission des affaires étrangères et des forces armées du Sénat.

Conformément à la loi, la composition de la DPR est le reflet d'une représentation pluraliste des sensibilités politiques :

- le groupe LREM est représenté par 2 membres ;
- le groupe LR est représenté par 4 membres ;
- le groupe AGIR est représenté par 1 membre ;
- le groupe SER est représenté par 1 membre.

Il est à noter que du fait des équilibres politiques différents à l'Assemblée nationale et au Sénat, l'opposition est davantage représentée au sein de la DPR que ne l'est la majorité présidentielle. Le mode de fonctionnement de la délégation, qui n'intervient pas en tant que telle dans la procédure législative, relativise cette singularité.

II. LA PERMANENCE DU CONTRÔLE PARLEMENTAIRE DU RENSEIGNEMENT, MALGRÉ LA CRISE SANITAIRE

Malgré les contraintes liées à la crise sanitaire, la délégation parlementaire au renseignement a maintenu une activité soutenue au cours de l'année écoulée. Sous la présidence de Françoise Dumas, la DPR a tenu une quinzaine de réunions et effectué cinq déplacements.

En raison de la nature de ses missions et de l'accès de ses membres à des informations classifiées, la délégation a tenu ses réunions en présentiel, dans sa salle de réunion sécurisée à l'Assemblée nationale ou directement dans les locaux des services visités.

Réunions plénières de la DPR de juin 2020 à juin 2021

Judi 25 juin 2020 :

Audition de M. Pierre de Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme

Judi 9 juillet 2020 :

Déplacement à la préfecture de Police de Paris

Audition de M. Didier Lallement, préfet de Police de Paris

Audition de Mme Françoise Bilancini, directrice du renseignement de la préfecture de Police de Paris

Judi 26 novembre 2020 :

Reconstitution du Bureau de la DPR

Reconstitution de la CVFS

Audition de M. Laurent Nunez, coordonnateur national du renseignement et de la lutte contre le terrorisme

Judi 5 décembre 2020 :

Audition de M. Jean-Jacques Brot, préfet des Yvelines

Audition de M. Pierre de Bousquet de Florian, directeur de cabinet du ministre de l'Intérieur

Judi 14 janvier 2021 :

Déplacement à la Direction du renseignement militaire (DRM) sur la base aérienne de Creil

Judi 28 janvier 2021 :

Adoption du rapport de la Commission de vérification des fonds spéciaux (CVFS)

Reconstitution de la CVFS

Déplacement à l'Office de lutte contre la criminalité liée aux technologies de l'information et de la communication – visite de la plateforme Pharos

Jeudi 11 février 2021 :

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

Jeudi 25 mars 2021 :

Déplacement à la Direction générale de la sécurité intérieure (DGSI)

Jeudi 8 avril 2021 :

Audition conjointe de M. Laurent Nunez, coordonnateur national du renseignement et de la lutte contre le terrorisme et M. Franck Robine, conseiller « affaires intérieures » au cabinet du Premier ministre

Audition du Général Patrick Henry, sous-directeur de l'anticipation opérationnelle à la Direction générale de la gendarmerie nationale (SDAO)

Jeudi 15 avril 2021 :

Audition de M. Francis Delon, président de la CNCTR

Audition conjointe de Mme Lucile Rolland, directrice du Service central du renseignement territorial (SCRT) et M. Arnaud Verhille, chef du service départemental du renseignement territorial des Yvelines

Mercredi 5 mai 2021 :

Audition de M. Laurent Nunez, coordonnateur national du renseignement et de la lutte contre le terrorisme

Jeudi 17 juin 2021 :

Audition de M. Laurent Nunez, coordonnateur national du renseignement et de la lutte contre le terrorisme

Jeudi 24 juin 2021 :

Audition de M. Jérôme Leonnet, Directeur général adjoint de la Police nationale.

Jeudi 1^{er} juillet 2021 :

Adoption du rapport annuel d'activité et renouvellement du Bureau de la Délégation.

A. LES THÈMES DE TRAVAIL DE L'ANNÉE ÉCOULÉE

Dans le cadre de sa mission de suivi et d'évaluation de la politique publique du renseignement, la délégation a consacré une part importante de ses travaux au suivi des enjeux d'actualité en lien avec le renseignement. Cela s'est traduit par des auditions très régulières du coordonnateur national du renseignement et de la lutte contre le terrorisme qui a été entendu à cinq reprises. Ces auditions ont notamment porté sur un retex de l'attentat commis contre Samuel Paty, sur la présentation du projet de loi relatif à la prévention des actes de terrorisme et au renseignement ainsi que sur une présentation de la refonte du plan national d'orientation du renseignement (PNOR).

Outre le suivi des enjeux d'actualité liés au renseignement, la délégation a, au cours de l'année écoulée, orienté ses travaux autour de deux thèmes :

- Les conséquences de la crise sanitaire sur l'activité des services de renseignement ;
- Le renseignement territorial.

S'agissant des conséquences de la crise sanitaire, un questionnaire a été adressé à l'ensemble des services spécialisés ainsi qu'au GIC.

En ce qui concerne le sujet du renseignement territorial, la délégation a procédé à plusieurs auditions tant au niveau central que territorial, a effectué un déplacement à la DRPP et a adressé un questionnaire au SCRT.

B. LES DOCUMENTS TRANSMIS À LA DÉLÉGATION

En application de la loi, la délégation a été destinataire comme chaque année du rapport annuel d'activité des services spécialisés de renseignement et des services mentionnés à l'article L. 811-4 du code de la sécurité intérieure, ainsi que du rapport annuel de synthèse exhaustif des crédits consacrés au renseignement.

Ce rapport est très utile à la délégation pour l'exercice de sa mission de contrôle. Il reste néanmoins transmis tardivement puisqu'il n'a été adressé que fin décembre 2020 pour des données portant sur l'année 2019. Si le contexte sanitaire particulier de l'année 2020 peut expliquer cet envoi tardif, il est nécessaire qu'à l'avenir ce rapport puisse être transmis au plus tard le 1^{er} juillet de l'année n+1.

Par ailleurs, ce rapport pourrait également utilement faire état de la mise en œuvre des recommandations de la DPR [*Recommandation n° 1*].

Au cours de l'année 2020, la délégation a également été destinataire d'un rapport classifié sur la mise en œuvre expérimentale de la technique de l'algorithme. La DPR se félicite de la transmission de ce rapport réalisé spécifiquement pour la DPR alors qu'aucune obligation législative ou réglementaire n'imposait à l'exécutif de le faire. Ce rapport classifié est venu en complément du rapport d'évaluation – celui-ci non classifié – transmis au Parlement en application de la loi de 2015.

La délégation a également sollicité de la CNCTR la présentation, par technique et par finalité, des éléments statistiques figurant dans son rapport d'activité. Au cours de l'année 2020, la CNCTR n'a pas formulé d'observation au Premier ministre en application de l'article L. 855-1 du code de la sécurité intérieure.

Enfin, à sa demande, la liste des rapports de l'inspection des services de renseignement a été transmise à la DPR pour la période allant de juillet 2020 à juin 2021. Trois rapports ont été réalisés :

- Rapport n°06/CD/ISR du 31 août 2020 sur les problèmes de contrôle interne et d'organisation à la DGSE et à la DGSI révélés par les agissements de trois militaires du centre parachutiste d'entraînement spécialisé ;
- Rapport n°07/CD/ISR du 31 août 2020 sur les dispositifs de contrôle des agents des services de renseignement ;
- Rapport n°08/CD/ISR du 10 décembre 2020 sur le renseignement économique.

C. LES PERSONNALITÉS AUDITIONNÉES

Au cours de l'année écoulée, la délégation aura auditionné, soit lors de ses réunions plénières, soit dans le cadre des contrôles opérés par les commissions de vérification des fonds spéciaux (CVFS), l'ensemble des directeurs des services spécialisés du 1^{er} cercle, ceux du second cercle pouvant bénéficier de techniques de renseignement (SCRT, DRPP, SNRP) ainsi que le Groupement interministériel de contrôle (GIC).

Comme la loi l'y autorise, la délégation a également auditionné :

- le président de la CNCTR ;
- le conseiller du Premier ministre disposant d'un pouvoir de délégation pour délivrer des autorisations de mise en œuvre des techniques de renseignement.

III. LE RENFORCEMENT DES PRÉROGATIVES DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

La DPR a été créée par la loi du 9 octobre 2007 après de multiples tentatives avortées de création d'un organe parlementaire de contrôle des services de renseignement.

Après une décennie d'existence, une relation de confiance s'est établie entre la DPR et la communauté du renseignement.

Un premier renforcement des compétences de la DPR s'est opéré avec l'entrée en vigueur de la LPM 2014-2019.

En 2018, lors du débat parlementaire sur la LPM 2019-2025, le sénateur Philippe Bas avait déposé un amendement visant à franchir une nouvelle étape dans le contrôle parlementaire de la politique publique du renseignement. Le Gouvernement s'y était opposé et, lors de la commission mixte paritaire sur la LPM, le Sénat avait accepté de retirer cette disposition moyennant un engagement du Gouvernement à remettre l'ouvrage sur le métier au moment de la révision de la loi renseignement de 2015.

À l'occasion du colloque organisé en novembre 2018 au Palais Bourbon et auquel avaient participé ensemble les présidents du Sénat et de l'Assemblée nationale, en présence des principaux acteurs de la communauté du renseignement, le Gouvernement avait, par la voix du coordonnateur national du renseignement et de la lutte contre le terrorisme, indiqué ses « lignes rouges » quant aux possibilités de renforcement du contrôle parlementaire.

La lente montée en puissance du contrôle parlementaire de la politique publique du renseignement

Jusqu'au début des années 1970, le contrôle parlementaire de la politique publique du renseignement était, en dehors de quelques commissions d'enquête, quasi-inexistant. On avançait alors une contradiction supposée entre la publicité des travaux parlementaires et l'existence du « secret défense ».

De 1971 à 1999, en revanche, concomitamment avec la montée en puissance des fonctions de contrôle du Parlement, ce ne sont pas moins de 14 propositions de création d'un organe de contrôle de services de renseignement qui ont été déposées, sans succès, au Parlement.

Ce n'est qu'à la quinzième tentative, en 2005, que la procédure arriva à son terme, à l'initiative du député Alain Marsaud à l'occasion de l'examen d'un projet de loi anti-terroriste. Il constatait alors que la France était le seul pays occidental, avec le Portugal, à ne pas disposer d'un organe parlementaire de contrôle permanent.

Le ministre de l'Intérieur d'alors, Nicolas Sarkozy, se déclara favorable à cette initiative mais proposa la création d'un groupe de travail chargé de réfléchir à cette question. Divers amendements furent donc rejetés lors de l'examen du projet de loi anti-terroriste, à l'automne 2005, mais le groupe de travail ne vit jamais le jour. C'est le Gouvernement Villepin qui déposa un projet de loi en mars 2006 à l'Assemblée nationale, projet qui ne fût jamais discuté.

Le projet fût finalement redéposé par le Gouvernement Fillon en 2007 et déboucha sur l'adoption de la loi du 9 octobre 2007.

La délégation avait initialement pour mission « *de suivre l'activité générale et les moyens des services spécialisés* » des ministères de la Défense, de l'Intérieur et des Finances. Le terme de « *contrôle* » n'est alors volontairement pas utilisé dans la loi car celui-ci aurait eu, selon le rapporteur du texte à l'Assemblée nationale, Bernard Carayon, « *une connotation trop intrusive* ».

Si la mission de la délégation est alors définie en des termes très généraux, la liste de ses prérogatives l'est en revanche avec beaucoup plus de précision.

La loi de 2007 prévoyait ainsi que, dans le cadre de ses fonctions, la DPR était informée des éléments relatifs « *au budget, à l'activité générale et à l'organisation des services de renseignement* » mais elle précisait que ces éléments ne pouvaient porter « *ni sur les activités opérationnelles de ces services* » et leur financement, « *ni sur les échanges avec des services étrangers* ».

De fait, de 2008 à 2013, l'activité de la DPR se limitait à moins d'une dizaine d'auditions par an et à la publication d'un rapport d'activité très succinct. Cette période n'en fut pas moins fructueuse car elle a permis aux parlementaires de tisser des liens de confiance avec la communauté du renseignement.

L'adoption, à l'automne 2013, de la LPM 2014-2019, consécutif à plusieurs travaux parlementaires consacrés au renseignement – notamment la mission d'information Urvoas-Verchère sur le cadre juridique applicable aux services de renseignement de mai 2013 – marque incontestablement une rupture.

Alors qu'elle était cantonnée jusque-là au « *suivi de l'activité générale et des moyens des services spécialisés* », la DPR s'est vue reconnaître une mission de « *contrôle et d'évaluation de l'action du Gouvernement en matière de renseignement* », ce qui constituait alors une véritable mutation philosophique.

Pour lui permettre d'exercer au mieux sa mission nouvelle de contrôle et d'évaluation, la liste des documents qui lui sont transmis a été enrichie.

La liste des personnes qu'elle peut entendre a également été élargie en 2013 puis complétée à nouveau par la loi relative au renseignement du 24 juillet 2015 qui a également prévu la possibilité pour la délégation parlementaire au renseignement d'entendre chaque semestre le Premier ministre sur son application ainsi que les personnes spécialement déléguées par lui pour délivrer les autorisations de mise en œuvre des techniques de renseignement mentionnées par la loi.

Celle-ci peut également inviter le président de la CNCTR à lui présenter le rapport d'activité de la commission, tout comme le président de la Commission consultative du secret de la défense nationale. Elle entend enfin très régulièrement le coordinateur national du renseignement et de la lutte contre le terrorisme mais aussi des personnalités dont l'audition n'est pas expressément prévue par la loi comme des universitaires ou autres personnalités qu'elle juge utile d'entendre.

Le dépôt par le Gouvernement du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement est apparu comme étant le moment opportun pour procéder à une évolution du cadre législatif de la DPR.

A l'initiative des députés membres de la DPR, un amendement renforçant les prérogatives de la DPR a été adopté en première lecture à l'Assemblée nationale, puis a obtenu le vote favorable du Sénat. Au terme de la loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, les principales modifications apportées à l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 sont les suivantes :

- Le champ de compétence de la DPR est élargi au suivi des enjeux d'actualité et des défis à venir qui concernent la politique publique du renseignement.
- La DPR sera dorénavant destinataire, chaque semestre, de la liste des rapports d'inspection portant sur les services de renseignement.
- La DPR pourra également demander communication de tout document, information et élément d'appréciation nécessaire à l'accomplissement de sa mission. Il s'agit d'une avancée significative car jusqu'à présent, la DPR n'est destinataire que d'une liste limitative de documents. En revanche, ce droit à l'information élargi reste limité au besoin d'en connaître de la DPR, ce qui exclut les opérations en cours, les méthodes opérationnelles et les relations des services avec leurs partenaires étrangers.
- Au-delà de la liste limitative jusqu'à présent prévue par la loi, la DPR pourra désormais auditionner « toute personne exerçant des fonctions de direction » au sein des services de renseignement. Jusqu'à présent, seuls les directeurs des services et les personnes placées auprès de ces directeurs et occupant un emploi pourvu en conseil des ministres pouvaient être auditionnées.

- Enfin, la DPR aura la possibilité de demander chaque année au coordonnateur national du renseignement et de la lutte contre le terrorisme de lui présenter le plan national d'orientation du renseignement (PNOR).

Cet amendement, porté à l'Assemblée nationale par les quatre députés membres de la délégation parlementaire au renseignement, puis soutenu au Sénat, reprend l'esprit de la proposition de loi de Philippe Bas de 2018, tout en encadrant rigoureusement les nouvelles prérogatives accordées à la DPR. Un point d'équilibre a été atteint qui permet de franchir une nouvelle étape dans le renforcement du contrôle parlementaire de la politique publique du renseignement au moment où la révision des lois de 2015 et 2017 offre de nouveaux outils juridiques et techniques aux services de renseignement.

IV. LE SUIVI DES RECOMMANDATIONS 2019-2020 DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

A. SUR LE BILAN DES LOIS DE 2015

N°	RECOMMANDATION	ETAT D'AVANCEMENT	COMMENTAIRE
1	Modifier l'article L. 853-3 du code de la sécurité intérieure afin de renvoyer à la procédure d'avis de droit commun l'examen, par la CNCTR, des demandes de renouvellement des autorisations d'introduction d'habitation à des fins de maintenance ou de retrait de dispositifs techniques de surveillance.	Complètement prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement prend en compte cette recommandation.
2	Allonger : - à 4 mois la durée maximale d'autorisation de la technique de recueil de données de connexion par un dispositif de proximité prévue par l'article L.851-6 du code de la sécurité intérieure ; - à 6 mois la durée maximale d'autorisation d'exploitation des données recueillies dans le cadre d'une surveillance internationale, à l'exception des autorisations d'exploitation données à des fins de surveillance d'une personne située sur le territoire national.	Non prise en compte	
3	Confier à l'inspection des services de renseignement une mission de contrôle de la mise en œuvre, par les services du premier cercle ainsi que les services listés par décret en application de l'article L. 811-4 du code de la sécurité intérieure, de l'exigence de traçabilité définie par le législateur et, plus globalement, des dispositifs de contrôle interne instaurés pour sécuriser les procédures de demande et de traitement des techniques de renseignement. Communiquer à la délégation parlementaire au renseignement les résultats de cette inspection.	Non prise en compte	
4	Favoriser les mutualisations et les partages d'expérience sur la mise en œuvre de dispositifs de traçabilité. Étudier la possibilité de déployer le dispositif informatique de traitement des techniques de renseignement de la DGGI au sein des services du second cercle.	En cours de prise en compte	*****
5	Modifier l'article L. 853-2 du code de la sécurité intérieure afin de prévoir une modalité unique de collecte de données informatiques, plus conforme aux besoins opérationnels des services.	Complètement prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement prend en compte cette recommandation.
6	Proroger, à titre expérimental, la technique dite de l'algorithme prévue par l'article L. 851-3 du code de la sécurité intérieure. N'envisager son extension aux données de navigation sur Internet, et en particulier aux URL, que sous réserve d'un renforcement conséquent des garanties entourant la mesure et de la mise en place d'un contrôle parlementaire renforcé.	Complètement prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement prévoit : 1° la péremission de la technique de l'algorithme; 2° la remise d'un rapport au Parlement au plus tard le 31 juillet 2024; 3° l'extension des pouvoirs de contrôle de la DPR.
7	Engager des négociations en vue de la conclusion d'un protocole d'assistance entre la DGGI et le SCRT dans la mise en œuvre de certaines techniques de renseignement. Envisager, à terme, la mise en place d'une unité de mutualisation commune à plusieurs services.	Complètement prise en compte	Il existe actuellement deux axes d'assistance : les DTR (y compris pour la DRPP) et l'OGINT. Par ailleurs, la DGGI est prête à concrétiser son assistance sur d'autres TR.
8	*****	Complètement prise en compte	*****
9	Étendre à la finalité de préservation et de promotion des intérêts économiques, industriels et scientifiques majeurs de la Nation le champ de l'autorisation d'exploitation de données collectées dans le cadre d'une surveillance internationale, à des fins de surveillance d'une personne située sur le territoire national.	Non prise en compte	
10	Réviser l'échelle des durées de conservation des données collectées dans le cadre des techniques de renseignement afin de tenir compte des contraintes opérationnelles liées à l'exploitation des données, sans toutefois remettre en cause le principe de graduation prévu par le législateur en 2015.	Complètement prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, en alignant la durée de conservation des images et des parois captées, prend en compte cette recommandation.

11	Étendre la technique de géolocalisation en temps réel, définie à l'article L. 851-4 du code de la sécurité intérieure, à l'entourage des personnes surveillées, sous réserve de l'application d'un contingent maximal d'autorisations délivrées simultanément.	Non prise en compte	
12	-----	Non prise en compte	
13	Encadrer législativement la conduite de tests par le GIC et les services de renseignement du premier cercle sur les matériels de collecte de renseignement, à l'instar du régime prévu par l'article L. 2371-2 du code de la défense.	Non prise en compte	
14	Créer une nouvelle interception de sécurité pour couvrir la surveillance des correspondances physiques (lettres, paquets, etc.), susceptible, selon les besoins opérationnels, d'être associée à une introduction dans un lieu privé.	Non prise en compte	
15	Donner un cadre légal aux conditions dans lesquelles les renseignements collectés par le biais de techniques de renseignement peuvent être partagés entre services de renseignement. Modifier, en conséquence, l'article L. 863-2 du code de la sécurité intérieure.	Complètement prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement prend en compte cette recommandation.
16	Engager une réflexion sur le statut des renseignements techniques recueillis ou exploités grâce à l'assistance d'un service de renseignement étranger et sur le niveau de protection qui les entoure.	Non prise en compte	Cette recommandation fait actuellement l'objet de discussions exploratoires, comme suite à l'arrêt Big Brother Watch contre Royaume-Uni de la CEDH du 25/05/2021.
17	Engager une réflexion en vue d'ouvrir un droit d'accès ponctuel aux fichiers de souveraineté à la CNCTR, lorsqu'elle est saisie de réclamations sur le fondement de l'article L. 833-4 du code de la sécurité intérieure, à l'instar des droits actuellement reconnus à la CNIL.	Non prise en compte	
18	Conférer à la formation spécialisée du Conseil d'Etat la possibilité de s'adjoindre le concours de personnels techniques, soit par la voie d'un recrutement, soit par la voie d'un appui technique des équipes, selon les cas, de la CNCTR ou de la CNIL, dans le cadre de l'instruction des recours dont elle est saisie.	Non prise en compte	
19	Adapter, pour les décisions rendues par la formation spécialisée, la procédure d'exécution de droit commun : - en confiant à la formation spécialisée le soin d'instruire les requêtes tendant à assurer l'exécution des décisions qu'elle rend et en lui autorisant à se saisir d'office ; - en permettant à la CNCTR ou à la CNIL, en cas d'inexécution constatée d'une décision du Conseil d'Etat, de saisir la formation spécialisée en vue d'engager une procédure d'exécution.	Non prise en compte	

B. SUR LE RENSEIGNEMENT PÉNITENTIAIRE

N°	RECOMMANDATION	ETAT D'AVANCEMENT	COMMENTAIRE
20	Inscrire à l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 l'obligation pour le Gouvernement de respecter le délai maximum d'un mois pour répondre à une demande de transmission d'un document par la DPR et de motiver sa décision en cas de refus.	Non prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement étend les prérogatives de la DPR (notamment en matière de droit de communication et d'audition), mais ne prévoit pas d'obligation, pour le gouvernement, de répondre aux demandes de la DPR dans un délai déterminé.
21	Expertiser la possibilité de créer un régime indemnitaire dédié aux métiers du renseignement pénitentiaire.	En cours de prise de compte	Le SNRP entretient un dialogue constructif en ce sens avec la sous-direction des ressources humaines et des relations sociales de la Direction de l'administration pénitentiaire (DAP). La nomenclature des postes et le régime indemnitaire sont deux sujets centraux de ces échanges.
22	*****	En cours de prise de compte	*****
23	Élargir aux agents du renseignement pénitentiaire la possibilité de recourir à une identité d'emprunt dans l'exercice de leur mission.	En cours de prise de compte	*****
24	Allonger la durée de conservation des enregistrements de téléphonie légale (article 727-1 du code de procédure pénale) et recourir à des outils de traduction et de transcription automatique de la parole pour améliorer l'exploitation des données conservées.	Partiellement prise en compte	La question de la durée de conservation comme celle de l'automatisation du traitement ne relèvent pas du SNRP. Des expérimentations concernant les outils d'aide à l'exploitation des données sont néanmoins bien actuellement menées par la Direction de l'administration pénitentiaire (DAP).
25	Expertiser la possibilité pour le SNRP de recourir à la technique de l'algorithme si elle venait à être pérennisée par la loi.	Non prise en compte	Cette technique ne serait pas pertinente pour le SNRP. De plus, le projet de loi SILT/Rens actuellement en débat prévoit de restreindre l'utilisation des algorithmes aux seuls services du premier cercle.
26	Ouvrir un quartier d'évaluation de la radicalisation (QER) et un quartier de prévention de la radicalisation (QPR) dédié aux femmes.	En cours de prise de compte	Action en cours au ministère de la Justice.
27	Autoriser les procureurs de la République à accéder au FSPRT.	Non cotée	Il s'agit d'un fichier de suivi en renseignement.
28	Instaurer un régime de sûreté ad hoc pour les sortants de prison.	Complètement prise en compte	La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement prend en compte cette recommandation.

C. SUR LA MAÎTRISE DES RISQUES

N°	RECOMMANDATION	ETAT D'AVANCEMENT	COMMENTAIRE
29	Harmoniser les procédures d'habilitation des agents des services de renseignement, en systématisant l'entretien de sécurité et l'entretien avec un psychologue.	Complètement prise en compte	Les services ont tous pris en compte cette recommandation et l'entretien avec un psychologue est dorénavant systématisé, notamment dans le processus de recrutement.
30	Rationaliser le nombre de services enquêteurs placés respectivement auprès du ministère de l'Intérieur et du ministère des armées, en mutualisant leurs ressources humaines et techniques. Ces services devront conduire leurs enquêtes suivant une méthodologie homogène, établie par le SGDSN, en y associant Tractin. Les effectifs du SGDSN chargés du pilotage de la politique de protection du secret devront être augmentés afin, notamment, de conduire des audits qualité réguliers en ce domaine.	Non prise en compte	Il a été décidé à ce stade d'écartier l'idée d'un service unique d'habilitation MinInt/MinArm, afin de garantir la qualité et l'adéquation des enquêtes aux besoins spécifiques des services et statuts concernés.
31	Informar les personnes habilitées des devoirs qui leur incombent à travers la remise d'un fascicule, concomitamment à leur décision d'habilitation.	Complètement prise en compte	Les services ont pris en compte cette recommandation (sensibilisation systématique, formation, signature d'un engagement de responsabilité, communication des obligations liées à l'habilitation).
32	Enrichir le rapport d'activités visé à l'article 12 de l'IGI 1300 afin de renforcer le dialogue entre les HFDS, le SGDSN et les services enquêteurs, et ainsi mieux identifier les risques liés aux habilitations.	Non cotée	Ne relève pas de la compétence de la CNRLT mais du SGDSN.
33	Formaliser les délégations accordées par les ministres aux services de renseignement en matière d'habilitation de leurs agents, en évitant de cumuler les fonctions d'autorité d'habilitation et d'officier de sécurité. Cette faculté devra être prévue par l'IGI 1300 dans sa nouvelle rédaction.	Non prise en compte	Le principe de délégation aux SR des décisions d'habilitation pour les agents du MinInt, du MinJus et de Bercy a été rejeté.
34	Notifier aux agents des services du second cercle leur obligation en matière de déclaration de changement de situation personnelle auprès de l'officier de sécurité dont ils relèvent. L'officier devra quant à lui saisir l'autorité d'habilitation de ces nouvelles informations (notice 94 A révisée), qui les transmettra au service enquêteur compétent en vue de l'émission d'un nouvel avis de sécurité.	Complètement prise en compte	Dans les services du second cercle, les agents sont informés de la nécessité de mettre à jour leur situation en cas de changement. Les instructions en ce sens ont été rappelées.
35	Engager l'actualisation du cadre réglementaire relatif à la protection du secret de la défense nationale, avec pour objectif d'homogénéiser les procédures qui l'entourent, en particulier en matière d'enquêtes administratives.	Complètement prise en compte	Ne relève pas de la compétence de la CNRLT. Action engagée par le SGDSN (groupe de travail "standardisation des enquêtes administratives" et actualisation du cadre réglementaire).
36	Confier à l'Académie du renseignement la conception d'outils de formation et de sensibilisation aux enjeux de lutte contre la radicalisation, en lien avec les services compétents.	Complètement prise en compte	Organisation d'un séminaire récurrent sur la sécurité dans les services de renseignement.
37	Mettre en place un audit externe des dispositifs de détection et de lutte contre la radicalisation mis en place dans les services de renseignement.	Complètement prise en compte	Rapport de l'ISR sur le traitement des signaux de radicalisation dans les SR.
38	Mettre en place sur les réseaux informatiques de la DRM, avec le soutien du COMCYBER, un système qualifié visant à analyser les flux en sortie de réseau pour repérer d'éventuelles fuites de données. Son exploitation et le traitement des alertes resteront assurés en interne.	En cours de prise de compte	*****
39	Procéder à un audit régulier des systèmes d'information des services de renseignement et, en tant que de besoin, accompagner ces services dans la démarche d'homologation visant à protéger le secret de la défense nationale.	En cours de prise de compte	Des contrôles sont effectués par les Autorités Qualifiées SSI des différents services du premier cercle. Travaux en cours pour les services du second cercle (homologation du système d'information du SNRP est au centre d'échanges en cours avec le RSSI de la DAP ; la SDAO met actuellement en place son propre réseau classifié avec l'appui de la DCSI).

40	xxx	En cours de prise en compte	xxx
41	Contraindre l'ensemble des agents des services de renseignement à rendre compte à leur officier de sécurité des délits qu'ils ont commis dans un cadre extraprofessionnel, quelle qu'en soit la nature. Lors du renouvellement de leur habilitation, le service enquêteur prendra l'attache des services de police et de gendarmerie afin de recueillir des informations utiles sur les candidats et mettre en lumière toute omission de leur part.	Complètement prise en compte	Les services ont pris en compte cette recommandation, les textes prévoyant que l'administration est tenue informée des modifications affectant la situation personnelle des agents (ce qui sous-entend la communication des délits).
42	Informar la délégation parlementaire au renseignement des manquements déontologiques graves commis par leurs agents ou leurs anciens agents, et des procédures juridiques initiées à leur encontre.	Partiellement prise en compte	Des données chiffrées et des typologies pourraient être transmises à la DPR, mais pas les situations individuelles.
43	Compléter le dispositif de lanceur d'alerte créé par la loi de juillet 2015 et étudier la possibilité de confier une partie de ces missions à la DPR.	Non prise en compte	Le dispositif de lanceur d'alerte (article L.861-3 du CSI) réservé à l'agent d'un service pour les faits pouvant constituer une violation manifeste des dispositions relatives aux TRR est laissé au contrôle de la CNCTR. C'est un dispositif équilibré mis en œuvre pour les cas les plus graves à la seule main d'une autorité administrative indépendante. Le fait qu'il n'ait pas été employé depuis sa création en 2015 ne montre pas forcément une difficulté de mise en œuvre procédurale mais souligne plutôt le professionnalisme des services de renseignement et de leurs agents, respectueux du cadre légal dans l'exercice de leurs missions.
44	Améliorer l'information de la délégation parlementaire au renseignement par la commission nationale de contrôle des techniques de renseignement. Prévoir dans la loi une transmission à la DPR des recommandations adressées par la CNCTR en application de l'article L. 833-6 du code de la sécurité intérieure et, le cas échéant, des signalements adressés au procureur de la République sur le fondement de l'article L. 861-3 du même code.	Non prise en compte	La CNCTR, autorité administrative indépendante, a exercé à deux reprises en 2020 son pouvoir de recommander en application des dispositions de l'article L. 833-6 du CSI. Ses recommandations ont été intégralement mises en œuvre sans qu'elle ait eu besoin de faire usage de la faculté de saisir le CE d'un recours (article L. 833-6 du CSI).

D. SUR LE RENSEIGNEMENT SPATIAL

N°	RECOMMANDATION	ETAT D'AVANCEMENT	COMMENTAIRE
45	Soutenir les modes collaboratifs entre la recherche publique et le secteur privé afin de développer les démonstrateurs nécessaires pour conserver notre avance technologique et stratégique.	Non cotée	*****
46	Afin d'améliorer la compétitivité du lanceur Ariane 6, introduire un « Buy European Act » pour garantir un nombre de commandes institutionnelles nécessaires à la viabilité financière et commerciale du programme.	Non cotée	*****
47	Mettre fin à notre dépendance à l'égard des Etats-Unis en nous dotant de capacités propres -a minima européennes sinon nationales- d'observation et d'analyse de la situation de l'eEspace et lancer un programme français de développement d'un nouveau système plus performant de surveillance de l'espace pour succéder au démonstrateur GRAVES.	Non cotée	*****
48	Développer une capacité autonome d'imagerie radar.	Non cotée	*****
49	Favoriser un accès indépendant aux systèmes et aux données spatiales en développant une filière souveraine de la donnée spatiale, sur l'ensemble de la chaîne, de l'amont (collecte) à l'aval (usages), notamment en ce qui concerne nos capacités de stockage de données.	Non cotée	*****
50	Confirmer la trajectoire budgétaire permettant le renouvellement de nos capacités de renseignement spatial contribuant à la fonction stratégique prioritaire « connaissance et anticipation ».	Complètement prise en compte	*****
51	Clarifier le positionnement du commandement de l'espace en matière de renseignement et constituer en son sein une formation spécialisée « renseignement ». Celle-ci pourrait produire du renseignement d'intérêt spatial au niveau opératif et tactique pour appuyer la planification et la conduite des opérations spatiales militaires.	Complètement prise en compte	*****
52	Restaurer un climat de confiance franco-allemand en élaborant une feuille de route commune au service d'une ambition européenne.	Non cotée	*****
53	Promouvoir au sein de la communauté internationale l'adoption rapide du code de bonne conduite proposé par l'Union européenne pour les activités humaines dans l'espace.	Non cotée	*****

E. SUR LA CYBERDÉFENSE

N°	RECOMMANDATION	ETAT D'AVANCEMENT	COMMENTAIRE
54	La DPR demande que les différents traitements de la menace cyber par les services de renseignement fassent l'objet d'un développement actualisé dans le PNOR et sous forme de plans d'actions comprenant des objectifs à atteindre et des modalités d'évaluation de la réalisation de ces objectifs. Elle demande à pouvoir prendre connaissance de ces documents et, régulièrement, des résultats obtenus au titre de sa mission d'évaluation de la politique publique de renseignement.	Partiellement prise en compte	Cette recommandation, liée à la recommandation n°59, est partiellement prise en compte dans le cadre du Plan National d'Orientation du Renseignement (PNOR) et de la Fiche d'Orientation stratégique (FOS) sur la thématique de la cyberdéfense.
55	Associer la DGSI et la DRSD à la réflexion sur la coordination institutionnelle et la définition d'une stratégie nationale de prévention et de sensibilisation aux risques cyber.	Partiellement prise en compte	Cette recommandation dépasse le périmètre des services. Le risque cyber est pris en compte dans les sensibilisations dispensées sur les risques en général. Le complément relève de l'ANSI.
56	Maintenir un niveau de financement suffisant pour garantir le niveau des investissements des services dans la cyberdéfense et leur permettre de recruter et de fidéliser des personnels de haut niveau.	Complètement prise en compte	Le besoin en financements supplémentaires a bien été identifié et exprimé dans le cadre des travaux de programmation du ministère des Armées. S'agissant des mesures pour assurer l'attractivité, elles doivent concerner en priorité les profils seniors et éviter la situation de concurrence entre les entités étatiques.
57	Poursuivre la mutualisation dans le développement des outils, la formation et les échanges de bonnes pratiques entre les services de renseignement.	Complètement prise en compte	Il s'agit d'un travail de longue haleine et permanent. Il est néanmoins important de garder à l'esprit que la mutualisation n'est pas un objectif en soit mais que cela doit permettre d'apporter un gain en temps, en ressources et en efficacité. Outre les grands programmes mutualisés, le groupe Lagrange reste l'instance générale d'échanges interservices.
58	Associer les services de renseignement au travail prospectif d'élaboration d'une nouvelle stratégie industrielle de souveraineté en cybersécurité et orienter leur action dans sa mise en œuvre.	Complètement prise en compte	De façon générale, l'appui aux stratégies industrielles fait partie des orientations stratégiques en matière de renseignement d'intérêt économique et donc est intégré au PNOR.
59	Mettre en place, sous l'autorité du CNRLT, un outil d'évaluation et de suivi de la contribution des services de renseignement à la politique publique de cyberdéfense. L'inspection des services de renseignement pourrait participer à la conception de cet outil. Une fois ce travail méthodologique réalisé, la DPR souhaite que les résultats de cette évaluation et de ce suivi lui soient communiqués dans le rapport annuel d'activité des services.	En cours de prise en compte	La dimension cyber étant plus précisément décrite dans le nouveau PNOR, les rapports d'activités de la communauté du renseignement permettront de mieux décrire les contributions des SR.

F. RECOMMANDATIONS GENERALES DE LA COMMISSION DE VERIFICATION DES FONDS SPECIAUX

N°	RECOMMANDATION	ETAT D'AVANCEMENT	COMMENTAIRE
1	<p>A l'attention du Premier ministre : Effectuer un "resoclage" de la dotation en fonds spéciaux inscrites au programme 129 pour tenir compte de sbesoins réels et de l'évolution de l'activité opérationnelle des services.</p>	Non cotée	
2	*****	Non cotée	
3	*****	Non cotée	
4	<p>A l'attention du Premier ministre : Désigner par arrêté ou une circulaire non publié au Journal officiel, les entités et services susceptibles de bénéficier de fonds spéciaux. Cet arrêté ou circulaire, et les modifications apportées ultérieurement, seraient communiqués sans délai à la CVFS.</p>	Non cotée	
5	<p>A l'attention du Premier ministre : Réaffirmer la possibilité pour la CVFS d'accéder aux rapports d'inspection et d'audit interne nécessaires à sa pleine information et à l'exercice de son contrôle, par la diffusion d'une instruction aux services.</p>	Non cotée	
6	<p>A l'attention du CNRLT : Mettre en place, au sein de chaque service, des Indicateurs *****</p>	En cours de prise de compte	*****
7	<p>A l'attention du CNRLT : Mettre en place une cellule Interservices *****</p>	Complètement prise en compte	*****

CHAPITRE 2 LES ENJEUX D'ACTUALITÉ LIÉS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

I. ACTIVITES ET RESSOURCES DES SERVICES DE RENSEIGNEMENT

A. LES FAITS MARQUANTS DE L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT EN 2019

Parmi les données figurant au sein du rapport annuel d'activité des services de renseignement et du rapport annuel de synthèse exhaustif des crédits consacrés au renseignement, on peut retenir les éléments suivants :

S'agissant de l'aide à la décision, 15 123 notes ont été produites par les services de renseignement en 2019. C'est supérieur au nombre constaté en 2018 (13 607) mais légèrement inférieur à la production de 2015 (16 722 notes) au plus fort de la menace terroriste. Parmi ces notes, il faut distinguer les notes de renseignement (6 872) des notes d'évaluation (1 894) et d'information (1 851).

La majorité de la production des six services spécialisés du premier cercle porte sur les finalités 1 et 2 de la loi du 24 juillet 2015, à savoir l'indépendance nationale, l'intégrité du territoire et la défense nationale, les intérêts majeurs de la politique étrangère et les engagements internationaux. La production relative à la prévention du terrorisme est en baisse (7 % de moins par rapport à 2018) tandis que celle relative à la protection des intérêts économiques, industriels et scientifiques majeurs poursuit sa progression (3 % de plus qu'en 2018).

On a comptabilisé en 2019, **279 509 transmissions des notes** dont 23 778 à la Présidence de la République, 28 405 au sein des cabinets ministériels et 227 326 au sein de l'administration d'État. Le ministère des Armées est, de loin, celui qui compte le plus grand nombre de destinataires.

S'agissant de la prévention et de la réduction des vulnérabilités, les enquêtes diligentées en matière de renseignement ont principalement concerné la lutte contre le terrorisme. La part des actions relevant des finalités de défense des intérêts majeurs de la politique étrangère a progressé tandis que celle relative à la criminalité et à la délinquance organisées a baissé (de 18 % à 11 %). Les actions relevant de la prévention des atteintes à la forme républicaine des institutions (de 1 % à 4 %) ont également augmenté en raison de l'implication de militants des mouvances radicales dans les manifestations de voie publique.

Le travail interministériel mené dans le cadre de la lutte contre la prolifération des armes de destruction massive s'est traduit par une nette augmentation des actions de prévention et de réduction des vulnérabilités dans ce domaine *****.

L'Académie du renseignement a également conduit de nombreuses actions de sensibilisation qui ont concouru à la diffusion de la culture du renseignement. Ces actions ont concerné 1 909 personnes en 2019 contre 511 en 2018 et 285 en 2017. Si on y ajoute les actions de sensibilisation également effectuées chaque année par la DGSI et la DRSD, on atteint 111 125 personnes sensibilisées en 2019.

Parmi les actions d'entrave et de neutralisation des menaces, il convient de distinguer les mesures s'appliquant aux personnes (inscription dans un fichier, par ex.), de celles relatives aux lieux (fermeture administrative, par ex.), ou encore de celles concernant les biens (saisies administratives, par ex.) et des mesures affectant les fonds et les valeurs (gel d'avoir, par ex.) *****.

(Tableau)

Contrairement aux années précédentes, la majorité des activités d'entrave et de neutralisation ne s'inscrit plus dans la finalité d'indépendance nationale et défense nationale, fortement liée aux OPEX : 39 % contre 70 % en 2018. C'est désormais la finalité de prévention du terrorisme qui prédomine : 45 % en 2019 contre 13 % en 2018.

B. LES RESSOURCES ALLOUÉES AU RENSEIGNEMENT ONT POURSUIVI LEUR PROGRESSION

Qu'elles soient budgétaires ou humaines, les services de renseignement ont bénéficié en 2019 de ressources supérieures à celles des exercices antérieurs.

1. Les ressources budgétaires

Il faut distinguer les fonds normaux des fonds spéciaux.

En ce qui concerne les fonds normaux, 11 programmes budgétaires contribuent au financement de la politique publique du renseignement. L'enveloppe totale des crédits en fonds normaux consacrés au renseignement s'est établie à 2 732 millions d'euros en 2019, soit une hausse de 9,59 % par rapport à 2018. Cette évolution significative s'explique par une augmentation de plus de 13 % des crédits de la mission Défense. *****. L'augmentation des effectifs des services de renseignement a induit une nette progression des dépenses de personnel et de fonctionnement.

S'agissant des fonds spéciaux, les six services spécialisés de renseignement et le GIC en ont bénéficié en 2019 ainsi que, pour la première fois, le SNRP. *****.

2. Les ressources humaines

En 2019 les effectifs des services de renseignement et de leurs structures d'appui se sont établis à **20 168 agents** (dont 14 512 pour les services spécialisés du 1^{er} cercle), en augmentation de 3,1 % sur un an et de 22,1 % depuis 2015.

La répartition des effectifs est restée stable : la DGSE, la DGSi et le SCRT ont concentré 72 % des personnels.

Sur l'ensemble de la communauté du renseignement, le nombre d'agents contractuels est en progression (+14 % par rapport à 2018) pour s'établir à 17,11 % des effectifs (et même 22 % pour les services du 1^{er} cercle).

En termes de catégories, 35,65 % relèvent de la catégorie A, 51,2 % de la catégorie B et 13,07 % de la catégorie C, ce qui est stable par rapport aux années précédentes. La part des femmes a augmenté de 5 % sur une année, pour s'établir à 29,24 %.

S'agissant des flux sortants des services pour motif de sécurité (liés à la perte d'habilitation), on en dénombre 15 en 2019 (contre 22 en 2018, dans le contexte de l'attentat commis à la préfecture de police de Paris).

En 2019, un effort particulier a été mis sur la formation des agents des services de renseignement. En ce qui concerne les formations assurées par l'Académie du renseignement, l'effort de formation a même augmenté de près de 100 % en un an. L'Académie a ouvert ses formations aux agents des services du deuxième cercle qui ont représenté 21 % des participants en 2019 contre 2,4 % en 2018.

Le comité des ressources humaines des services de renseignement (CRHSR) créé en 2018, s'est réuni à quatre reprises en 2019, tenant compte des 21 recommandations issues du rapport de la DPR. Le comité a mis en place un répertoire interministériel des métiers du renseignement visant à favoriser la mobilité interservices. Ce répertoire est structuré autour de 4 filières : renseignement d'origine humaine, renseignement d'origine technique, entrave, appui.

C. LES COOPÉRATIONS

1. Les coopérations opérationnelles thématiques

L'année 2019 a été marquée par un fort dynamisme en matière de coopérations. La lutte contre le terrorisme reste le champ majeur de coopération entre les services, avec un chef de filât exercé par la DGSi.

Ces coopérations sont également tournées vers l'international. Au niveau global, la CNRLT a porté en 2019 le projet de « Collège du renseignement en Europe ».

De multiples cellules ou enceintes de coopération existent en fonction des finalités poursuivies telles que :

- L'indépendance nationale et l'intégrité du territoire et la défense nationale (4 cellules ou structures de coopération).
- La cyberdéfense (4 cellules ou structures de coopération).
- Les intérêts majeurs de la politique étrangère et l'exécution des engagements européens (7 cellules de coopération).
- La prévention de toute forme d'ingérence étrangère (5 cellules ou structures de coopération).
- La défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France (22 cellules ou structures de coopération).
- La prévention du terrorisme (19 cellules ou structures de coopération).
- La prévention de la criminalité ou de la délinquance organisée (9 cellules ou structures de coopération).
- La prévention de la prolifération des armes de destruction massive (17 cellules ou structures de coopération).

2. Les coopérations techniques

Depuis 2017, les coopérations techniques s'organisent autour de trois structures :

- **Le comité de pilotage stratégique (CPS)**, présidé par le CNRLT et dont le secrétariat est assuré par le SGDSN, est l'instance supérieure de gouvernance des capacités techniques mutualisées.
- Des **comités d'orientation et de pilotage** qui réunissent un directeur technique et l'ensemble des services de renseignement qui ont pour objet le pilotage des développements techniques.
- Des comités internes aux programmes (comités utilisateurs).

*****.

II. LA PERSISTANCE D'UNE MENACE TERRORISTE À UN NIVEAU ÉLEVÉ

A. DEPUIS 2015 : UNE MENACE TERRORISTE QUI A CHANGÉ DE NATURE MAIS QUI NE FAIBLIT PAS

39 attentats (21 aboutis et 18 échoués), attribués ou revendiqués par la mouvance islamiste, ont été perpétrés sur le sol français depuis janvier 2015, causant la mort de 263 personnes. 22 de ces attentats ont eu pour cible les forces de sécurité intérieure : policiers, gendarmes, militaires, surveillants pénitentiaires.

1. D'une menace projetée à une menace endogène

Le mode opératoire du terrorisme islamiste a évolué depuis 2015, passant d'une menace projetée (2015) à une menace désormais endogène. Celle-ci fut dans un premier temps soutenue (2016) avant de devenir davantage inspirée sur la période 2017-2019.

34 ressortissants étrangers ont été impliqués dans des projets terroristes aboutis, échoués ou déjoués depuis 2014, ce qui représente environ 20 % du total d'individus impliqués. Parmi eux, si les deux tiers étaient originaires des pays du Maghreb entre 2015 et 2017, cette proportion est retombée à 23 % sur la période 2018-2020. Plus de la moitié (54 %) des auteurs d'attentats sont originaires de Syrie et de Russie.

Lorsqu'il s'agit d'auteurs étrangers, il apparaît que sur la période 2018-2020, environ la moitié d'entre eux avaient le statut de réfugiés ou de demandeurs d'asile. Sur la période antérieure 2015-2017, il y avait parmi les étrangers une majorité de non-résidents ou de titulaires d'un titre de séjour.

Attentats islamistes commis en France depuis 2015

Date	Lieu	Bilan
2015		
7 et 8 janvier 2015	Paris / Charlie Hebdo Montrouge (92)	12 morts, 11 blessés 1 mort
9 janvier 2015	Paris / Hyper Cacher	4 morts, 9 blessés
3 février 2015	Nice	2 blessé
19 avril 2015	Villejuif	1 mort
26 juin 2015	Saint-Quentin-Fallavier	1 mort, 2 blessés
21 août 2015	Oignies (Thalys)	3 blessés
13 novembre 2015	Saint-Denis Paris Bataclan / Terrasses de café	1 mort, 56 blessés 129 morts, 357 blessés
2016		
7 janvier 2016	Paris / Commissariat de la Goutte d'or	Pas de victime
11 janvier 2016	Marseille	1 blessé
13 juin 2016	Magnanville	2 morts
14 juillet 2016	Nice	86 morts, 458 blessés
26 juillet 2016	Saint-Étienne-du-Rouvray	1 mort, 4 blessés
3 septembre 2016	Notre-Dame-de-Paris	Pas de victime
4 septembre 2016	Osny	1 blessé
8 septembre 2016	Boussy-Saint-Antoine	1 blessé
2017		
3 février 2017	Paris / Carrousel du Louvre	2 blessés
18 mars 2017	Aéroport d'Orly	1 blessé
20 avril 2017	Paris / Avenue des Champs-Élysées	1 mort, 2 blessés
6 juin 2017	Paris / Notre-Dame-de-Paris	2 blessés
19 juin 2017	Paris / Avenue des Champs-Élysées	Pas de victime
5 août 2017	Paris / Tour Eiffel	Pas de victime
9 août 2017	Levallois-Perret	6 blessés
12 septembre 2017	Aix en Provence	Pas de victime
15 septembre 2017	Paris	Pas de victime
29 septembre 2017	Paris / Immeuble rue Chanez	Pas de victime
1 ^{er} octobre 2017	Marseille	2 morts
2018		
23 mars 2018	Carcassonne et Trèbes	4 morts, 15 blessés
12 mai 2018	Paris / Quartier de l'Opéra	1 mort, 4 blessés
11 décembre 2018	Strasbourg	5 morts, 11 blessés
2019		
5 mars 2019	Condé-sur-Sarthe	2 blessés
24 mai 2019	Lyon	14 blessés
3 octobre 2019	Préfecture de police de Paris	4 morts, 1 blessé
2020		
3 janvier 2020	Villejuif	1 mort, 2 blessés
4 avril 2020	Roman sur Isère	2 morts, 6 blessés
27 avril 2020	Colombes	2 blessés
25 septembre 2020	Paris / Rue Nicolas Appert	2 blessés
16 octobre 2020	Conflans-Sainte-Honorine	1 mort
29 octobre 2020	Nice	3 morts
2021		
23 avril 2021	Rambouillet	1 mort

2. Les attentats commis depuis 2020 confirment l'évolution de la menace

L'état de la menace terroriste s'est trouvé sensiblement augmenté à l'automne 2020 en raison de tenue du procès des attentats contre Charlie-Hebdo et l'hyper-casher de la porte de Vincennes.

Notre pays a subi à cette période une vague d'attentats avec une fréquence particulièrement soutenue puisque 3 attaques ont été perpétrées en à peine un peu plus d'un mois :

- le 25 septembre 2020 à Paris,
- le 16 octobre 2020 à Conflans-Sainte-Honorine,
- le 29 octobre 2020 à Nice.

Il faut remonter à 2016 pour observer un rythme similaire d'attaques terroristes lorsque trois attentats avaient frappé notre sol en l'espace de seulement six semaines, entre le 13 juin 2016 et le 26 juillet 2016.

La republication des caricatures de Mahomet et le discours du Président de la République sur la lutte contre le séparatisme ont eu un impact sur l'état de la menace. L'agence de presse Thabat, proche d'Al Qaïda, a ainsi appelé le 25 octobre 2020 à mener des actions violentes sur le territoire français, par tous moyens y compris souvent rudimentaires.

La nature des attaques commises et les profils des terroristes soulignent l'évolution de la menace et la difficulté pour les services de renseignement à entraver des auteurs qui sont de plus en plus nombreux à ne pas être connus des services de renseignement.

Les attentats de la période récente soulignent également un processus de radicalisation de plus en plus rapide et une accélération de la décision, prise souvent de façon solitaire, de passage à l'acte, sans aucun contact avec des individus suivis sur le territoire national ou à l'étranger.

Les attentats déjoués depuis 2015

On recense 60 attentats islamistes déjoués sur le territoire français depuis 2015 :

Année	2015	2016	2017	2018	2019	2020	2021 (au 30/06)
Nombre d'attentats déjoués	7	17	20	7	4	2	3

Par ailleurs, 5 projets d'attentats émanant de l'ultra-droite ont été déjoués depuis 2017, révélant le danger pour la sécurité nationale que représente la montée en puissance des mouvances suprémacistes et survivalistes.

B. LES ENSEIGNEMENTS TIRÉS DES ATTENTATS RÉCENTS

1. Renforcer les échanges avec le monde psychiatrique et les préfets dans le cadre de la lutte contre la radicalisation

15,8 % des personnes enregistrées dans le FSPRT présenteraient des troubles psychiatriques¹, à l'instar de l'auteur de l'attaque au couteau perpétrée le 28 mai 2021 contre une policière municipale de La Chapelle-sur-Erdre.

Les actions terroristes commises depuis 2019 ont révélé la nécessité d'améliorer la communication entre le milieu de la santé et l'administration pour mieux prévenir d'éventuels actes terroristes et assurer une prise en charge plus adaptée des profils présentant des troubles du comportement altérant le discernement.

C'est dans ce contexte qu'est intervenu le rapprochement du fichier HOPSYWEB, qui recense et assure le suivi des personnes faisant l'objet de soins psychiatriques sans consentement, avec le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT).

Seul le législateur pouvant autoriser des personnes qui ne sont pas des professionnels de santé à avoir accès à des données protégées par le secret médical, la loi du 30 juillet 2021 relative à la prévention des actes de terrorisme et au renseignement a ajouté dans le code de la santé publique, d'un article L. 3211-12-77 qui permet la communication au préfet et aux services de renseignement du lieu de résidence, et non, comme la loi le prévoyait jusqu'alors, du seul département d'hospitalisation des informations strictement nécessaires à l'accomplissement de leurs missions.

Cette mise en relation des fichiers HOPSYWEB et FSPRT répond à un motif d'intérêt général, comme l'exige le Conseil constitutionnel (CC 22 mars 2012, loi relative à la protection de l'identité, n° 2012-652 DC) et comme l'a reconnu le Conseil d'État (CE 27 mars 2020, cercle de réflexion et de proposition d'actions sur la psychiatrie et *a.*, n° 431350), à savoir « prévenir le passage à l'acte terroriste des personnes radicalisées qui présentent des troubles psychiatriques ».

La finalité qui vise à partager les informations relatives au suivi des ces personnes entre autorités sanitaires et autorités administratives est donc légitime, afin de mieux prévenir les risques de passage à l'acte des personnes faisant l'objet d'un suivi au titre de la radicalisation terroriste. À cet égard, l'autorité de police administrative en charge de ce suivi doit en particulier être à même de savoir si la personne inscrite dans le fichier de signalement pour la prévention de la radicalisation à caractère terroriste fait ou a fait l'objet d'une prise en charge psychiatrique, pour adapter son suivi.

¹ Cf. rapport d'information de l'Assemblée nationale du 27 juin 2019, relatif aux services publics face à la radicalisation.

2. Répondre aux signalements effectués sur les réseaux sociaux

L'attentat commis contre Samuel Paty a souligné l'importance de surveiller les réseaux sociaux et d'analyser les contenus en ligne susceptibles de révéler une menace terroriste.

Le compte twitter (tchetchene270) de l'auteur de cette attaque perpétrée le 16 octobre 2020 avait été signalé une première fois le 12 juillet 2020 à la plateforme Pharos, dédiée au traitement des contenus illicites de l'internet signalés par les particuliers et les professionnels et à l'orientation en temps réel vers les services enquêteurs pour exploitation. Néanmoins, ce premier signalement ne contenait pas de menace explicite contre le territoire national.

Au lendemain de l'attentat contre Samuel Paty, le Premier ministre a annoncé le renforcement des effectifs de cette plateforme, au sein de la sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire.

Une quarantaine de policiers et de gendarmes sont affectés à Pharos qui doit encore poursuivre sa montée en puissance. La cellule de traitement des signalements – qui ne cessent d'augmenter – est composée de 21 enquêteurs, et fonctionne désormais 24h/24 depuis janvier 2021. Au cours de l'année 2020, Pharos a été destinataire de 289 590 signalements correspondant à 130 995 contenus, contre environ 50 000 signalements à la création de la plateforme.

Il y a eu, pour la seule année 2020, 18 626 signalements en matière de terrorisme dont 14 456 ont été effectués en à peine plus de deux mois, après le 16 octobre 2020, date de l'assassinat de Samuel Paty.

Au cours de l'année 2020 :

- 141 procédures judiciaires ont été ouvertes pour apologie du terrorisme,
- 4 214 demandes de retrait de contenus,
- 29 demandes de blocage auprès des fournisseurs d'accès internet (FAI)
- 1 355 demandes de déréférencement de contenus.

Même si la vocation de Pharos est essentiellement judiciaire, il existe des liens avec les services de renseignement. Lors du mouvement des gilets jaunes, entre novembre 2018 et novembre 2019, 332 contenus ont fait l'objet d'une transmission aux services de renseignement compétents.

En matière de lutte anti-terroriste, il est essentiel d'entraver la viralité des contenus, en visant leur retrait dans les plus brefs délais – une quinzaine de minutes – après leur signalement. Pour y parvenir, des mesures administratives peuvent être prises sur la base de l'article 6-1 de la loi sur la confiance dans l'économie numérique, comme l'injonction donnée à un hébergeur de retirer un contenu immédiatement.

En cas de menace terroriste immédiate, le point de contact est la DGSI
*****.

C. DE NOUVEAUX DISPOSITIFS JURIDIQUES DE LUTTE CONTRE L'ISLAM POLITIQUE : LES FERMETURES DES LIEUX DE CULTES ET L'EXTENSION À LEURS DÉPENDANCES

L'action contre le séparatisme islamiste a conduit à la fermeture administrative de plusieurs lieux de culte et à la dissolution d'associations.

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT) a créé l'article L. 227-1 du CSI.

Cet article dispose qu'« *aux seules fins de prévenir la commission d'actes de terrorisme, le représentant de l'État dans le département, ou à Paris, le préfet de police peut prononcer la fermeture des lieux de culte dans lesquels les propos qui sont tenus, les idées ou théories qui sont diffusées ou les activités qui se déroulent provoquent à la violence, à la haine ou à la discrimination, provoquent à la commission d'actes de terrorisme ou font l'apologie de tel actes* ».

En application de ces dispositions, la fermeture administrative d'un lieu de culte est soumise à une double condition :

- elle ne peut être prononcée qu'aux fins de prévenir la commission d'un acte de terrorisme ;
- les propos tenus au sein du lieu de culte concerné, les idées ou théories qui y sont diffusées ou les activités qui s'y déroulent doivent soit provoquer à la violence à la haine ou à la discrimination, soit provoquer à la commission d'actes de terrorisme ou en faire l'apologie.

À la date du 31 mai 2021, et depuis l'entrée en vigueur de la loi SILT du 30 octobre 2017, 8 lieux de culte ont été fermés sur ce fondement : 3 en 2017, 3 en 2018, 1 en 2019 et 1 en 2020, qui concerne la mosquée de Pantin, fermée en novembre 2020 pour six mois, notamment pour avoir relayé une vidéo qui avait mis en cause Samuel Paty avant son assassinat.

Sept des huit décisions de fermeture ont été contestées au fond comme en référé, mais leur bien-fondé a systématiquement été confirmé par le juge administratif.

Sur le plan géographique, ont été concernés les départements du Nord (deux fermetures), des Bouches-du-Rhône (deux fermetures), de l'Hérault, de l'Isère, des Yvelines et de la Seine-Saint-Denis (une fermeture pour chacun de ces départements).

L'ensemble des mesures de fermetures prononcées ont concerné des mosquées en lien avec la mouvance islamiste radicale.

La loi n°2021-998 du 30 juillet 2021 relative à la prévention des actes de terrorisme et au renseignement étend la possibilité de fermeture administrative de locaux dépendants d'un lieu de culte.

En effet, même s'il n'existe pas de définition précise du lieu de culte, qui pourrait être regardé comme tout lieu dans lequel se tient un culte, l'acception commune tend à limiter le lieu de culte au lieu « dédié au culte », rendant de facto sa fermeture relativement aisée à contourner et tend à priver celle-ci d'effet dès lors qu'il existe des espaces adjacents au lieu de culte et en dépendant, au sein du bâtiment en question ou à proximité immédiate, vers lesquels peut être déportée la pratique du culte.

Il doit exister des raisons sérieuses de penser que ces locaux, dont la dépendance organique ou géographique est avérée, sont utilisés pour contourner la mesure de fermeture du lieu de culte. Selon les cas, la mesure de fermeture du lieu dépendant du lieu de culte pourra donc être concomitante à celle prononçant la fermeture dudit lieu de culte, s'il existe des raisons sérieuses de penser que le culte est susceptible de se tenir dans le lieu en dépendant (parce que tel a déjà été le cas par exemple ou parce qu'il existe une imbrication très forte entre les lieux...) ou différée, à raison de manœuvres postérieures de contournement de la mesure.

D. DES MOTIFS DE PRÉOCCUPATION PERSISTANTS

Deux motifs de préoccupation dominant au regard de la menace terroriste : il s'agit d'une part du risque lié aux sortants de prison et d'autre part de la reconstitution possible d'une menace projetée au vu de la dégradation de la situation sécuritaire sur zone.

1. Le suivi en détention et à la sortie de prison

Le nombre de détenus condamnés pour des faits de terrorisme islamiste commence à décliner dans les prisons françaises et le rythme des sorties va sensiblement s'accroître en 2023 et 2024. On recensait au premier trimestre 2021 environ 470 détenus TIS contre 550 à 600 lors du pic atteint sur la période 2018-2019. Il faut y ajouter environ 700 détenus condamnés pour des faits de droit commun radicalisés.

TIS sortants à 3 ans	163
Fin 2020	17
Fin 2021	66
Fin 2022	47
Fin 2023	33

Source : étude d'impact PJJ renseignement

Par ailleurs, de plus en plus de personnes sont suivies en milieu ouvert, par les services pénitentiaires d'insertion et de probation (SPIP). Certains d'entre eux font l'objet de mesures individuelles de contrôle administratif et de surveillance

(MICAS). À titre d'illustration, depuis la promulgation de la loi SILT en octobre 2017, 147 sortants de prison condamnés pour terrorisme se sont vus notifier une MICAS.

Alors qu'une majorité d'actes terroristes a pour cible des forces de sécurité – à l'instar de l'attaque au couteau dans la prison de Condé-sur-Sarthe le 5 mars 2019 – il s'agit pour les services de renseignement de prévenir tant les attentats commis en détention que ceux susceptibles d'être perpétrés par des sortants de prison.

C'est dans ce contexte que le renseignement pénitentiaire a vu ses moyens significativement renforcés ces deux dernières années avec la création du SNRP, l'attribution de fonds spéciaux, et le développement de moyens techniques mutualisés avec la DGSI.

De nouveaux quartiers d'évaluation de la radicalisation (QER) et de prise en charge de la radicalisation (QPR) ont été créés ou le seront prochainement, en particulier dédiés aux femmes. Un QER pour femmes a ainsi été ouvert à la prison de Fresnes qui disposera de 8 places d'ici à la fin de l'année 2021 ; et un QPR pour femmes verra prochainement le jour à la prison de Rennes qui sera, à terme, doté d'une trentaine de places. La Délégation estime nécessaire d'augmenter le nombre de places pour femmes au sein des QER et des QPR dans le cadre du programme immobilier pénitentiaire [*Recommandation n° 2*].

Enfin, la nouvelle loi relative à la prévention d'actes de terrorisme et au renseignement prévoit la création d'une **mesure judiciaire de prévention de la récidive terroriste et de réinsertion**. Cette mesure de sûreté a pour objectif d'assurer le suivi des personnes actuellement détenues pour actes de terrorisme en lien avec la mouvance islamiste dont la peine arrive à échéance dans les prochains mois ou prochaines années.

Cette mesure s'applique aux personnes condamnées à une peine privative de liberté non assortie du sursis d'une durée supérieure ou égale à 5 ans pour des faits de terrorisme, ou 3 ans en cas de récidive, s'il est établi, à l'issue d'un réexamen de leur situation intervenant à la fin de l'exécution de leur peine, qu'ils présentent une particulière dangerosité caractérisée par une probabilité très élevée de récidive et par une adhésion persistante à une idéologie ou à des thèses incitant à la commission d'actes de terrorisme (I de l'article 706-25-16 du code de procédure pénale).

Trois niveaux de prise en charge sont possibles en fonction des besoins repérés dans chacune des dimensions du suivi (psychosociale, psychologique, culturelle, socio-professionnelle...) :

- le niveau 1 dit milieu ouvert renforcé, consistant en une prise en charge de 3 heures par semaine ;

- le niveau 2 dit intermédiaire permettant une prise en charge jusqu'à 10 heures par semaine pour les personnes dont le niveau de radicalité et d'intégration sociale demande un accompagnement important ;
- le niveau 3 dit intensif correspondant à une prise en charge jusqu'à 20 heures par semaine, et visant les personnes ayant un niveau de radicalité élevé et nécessitant par ailleurs un accompagnement intensif en vue de leur réinsertion sociale.

Le niveau de prise en charge proposé par le centre à l'issue du diagnostic est soumis à la validation du SPIP et peut être modifié tout au long du suivi.

La mesure judiciaire de réinsertion sociale antiterroriste a donc pour objectif d'assurer la réinsertion des détenus TIS par un accompagnement resserré et adapté à leur profil, au moyen d'obligations ou d'interdictions à vocation essentiellement sociale.

2. La possible reconstitution d'une menace projetée

Si la menace endogène a pris le pas ces dernières années sur la menace dite projetée depuis l'étranger, il ne faut toutefois pas sous-estimer la reconstitution de réseaux terroristes dans la zone irako-syrienne. Les personnes retenues dans les camps du nord est syrien représentent un vivier stratégique pour Daesh, en particulier les mineurs considérés comme de véritables « lionceaux du califat ».*****

Seul un règlement politique du conflit syrien serait de nature à permettre une sécurisation pérenne de la zone, ce qui n'est pas aujourd'hui le scénario le plus vraisemblable à court ou à moyen terme.

III. L'EXTENSION DES FICHIERS DE POLICE ET DE GENDARMERIE PAR TROIS DÉCRETS DU 2 DÉCEMBRE 2020

Par trois décrets du 2 décembre 2020, le Gouvernement a sensiblement étendu les possibilités de collecte de trois fichiers gérés par la police et la gendarmerie nationales.

Le Gouvernement a justifié ces extensions de possibilités de fichage par les forces de l'ordre en raison de l'évolution des menaces, dans un contexte lié d'une part au mouvement des gilets jaunes et d'autre part à la nécessité de mieux détecter les « signaux faibles » pour lutter plus efficacement contre le terrorisme.

Les trois fichiers concernés sont :

- **Le fichier PASP** (prévention des atteintes à la sécurité publique), créé en 2009 et géré par la direction générale de la police nationale (DGPN). Environ 60 000 personnes y sont inscrites.
- **Le fichier GIPASP** (gestion de l'information et prévention des atteintes à la sécurité publique), créé en 2011 et géré par la direction générale de la gendarmerie nationale (DGGN). Environ 67 000 personnes y sont inscrites.

Ces deux fichiers (PASP et GISASP) ne portent pas sur des personnes condamnées mais seulement « susceptibles d'être impliquées dans des actions de violences collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives ». Entrent dans le cadre de ces fichiers toutes les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique.

- **Le fichier EASP** (enquêtes administratives), créé en 2009 et utilisé en amont du recrutement de fonctionnaires sur des postes sensibles (magistrats, policiers, surveillants pénitentiaires, par ex). Il est géré par la direction centrale de la sécurité publique (DCSP) et la préfecture de police. Destiné à éviter de recruter des personnes potentiellement dangereuses ou radicalisées, ce fichier vise à faciliter la réalisation d'enquêtes administratives au moyen du recueil et de l'exploitation d'informations nécessaires pour répondre aux demandes dévolues au renseignement territorial. 221 771 personnes y étaient inscrites en novembre 2020.

Ces trois fichiers ont été alimentés de façon significative ces dernières années, puisqu'on constate une hausse des inscriptions d'environ 50 %.

A. LES PRINCIPALES MODIFICATIONS APPORTÉES PAR LES DÉCRETS

- Les décrets du 2 décembre 2020 procèdent à l'élargissement des finalités des fichiers PASP et GIPASP, initialement limitées à la prévention des atteintes à la sécurité publiques, aux fins de tenir compte de l'évolution de certaines pratiques dans l'utilisation de ces fichiers. Peuvent désormais être conservées des informations concernant des personnes pouvant porter atteinte non plus seulement à la « sécurité publique » mais, plus largement, à « la sûreté de l'État, à l'intégrité du territoire ou des institutions de la République ». Il est précisé que « les données intéressant la sûreté de l'État sont celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts ».
- Par ailleurs, les décrets du 2 décembre 2020 sont venus élargir les données pouvant faire l'objet d'une collecte et d'un enregistrement dans ces fichiers. Si la collecte de données relatives à « des activités politiques, philosophiques, religieuses ou syndicales » était déjà autorisée, les nouveaux décrets font référence non plus aux « activités » mais aux « opinions » politiques, aux « convictions » philosophiques, religieuses et à l'« appartenance » syndicale.
- Les données relatives à l'état de santé, s'agissant de troubles psychologiques ou psychiatriques, peuvent désormais être collectées.
- Les données de personnes morales et de groupements de fait peuvent également désormais faire l'objet d'un enregistrement dans ces traitements au même titre que celles des personnes physiques. Ceci répond à la volonté du Gouvernement de mieux surveiller les activités associatives, en particulier dans le cadre de la lutte contre la radicalisation et le terrorisme.
- Les types de données pouvant être enregistrées sont sensiblement élargies, en particulier en ce qui concerne les « activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État ». Figurent notamment les « comportements et habitudes de vie », les « déplacements », les « pratiques sportives », « la pratique et le comportement religieux ».
- Les identifiants utilisés sur internet (pseudonymes, sites ou réseaux concernés, autres identifiants techniques) peuvent désormais faire l'objet d'une mention dans ces fichiers, à l'exclusion toutefois des mots de passe. Les informations collectées porteront principalement sur les commentaires postés sur les réseaux sociaux et les photos ou illustrations mises en ligne, ces éléments étant considérés comme pertinents dans le cadre de la prévention des atteintes à la sécurité publique ou à la sûreté de l'État.
- L'accès aux fichiers est élargi, notamment aux procureurs de la République.

B. LES GARANTIES PRÉVUES PAR LES TEXTES

- Seules les activités « susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État » peuvent donner lieu à l'enregistrement de données sur des activités publiques ou au sein de groupements ou de personnes morales. Cela interdit notamment un enregistrement de personnes dans le traitement fondé sur une simple appartenance syndicale.
- La possibilité d'enregistrer des données relatives aux activités susceptibles de porter atteinte à la sécurité publique sur les réseaux ne peut provenir que de données collectées individuellement et manuellement.
- Les données relatives aux troubles psychologiques ou psychiatriques susceptibles de révéler des facteurs de dangerosité ne peuvent être collectées que si elles sont obtenues conformément aux dispositions législatives et réglementaires en vigueur, ce qui doit garantir le respect du secret médical.
- Il n'est pas autorisé de sélectionner dans le traitement une catégorie particulière de personnes à partir des seules données mentionnées au I de l'article 6 de la loi du 6 janvier 1978, à savoir les opinions politiques, les convictions religieuses et philosophiques ou encore l'appartenance syndicale.
- La possibilité de renseigner dans les fichiers l'indication de renseignement ou non de la personne dans 6 autres fichiers (TAJ, N-SIS II, GIPASP, personnes recherchées, FSPRT, objets et véhicules volés ou signalés) n'autorise pas pour autant l'interconnexion desdits fichiers. En outre, l'accès aux fichiers consultés se fait par des agents expressément et individuellement habilités.

C. UNE EXTENSION QUI FAIT L'OBJET D'UN RECOURS DEVANT LE CONSEIL D'ÉTAT

Plusieurs syndicats, notamment la CGT, FO ou la FSU, mais aussi le syndicat de la magistrature et le syndicat des avocats de France, avaient saisi le Conseil d'État en référé, après la publication des décrets par le ministère de l'Intérieur, le 4 décembre 2020. Ils pointaient la « dangerosité » et le caractère « flou » desdits décrets.

Le 4 janvier 2021, le Conseil d'État a rejeté ces requêtes, considérant que les trois décrets ne portaient pas une atteinte disproportionnée à la liberté d'opinion, de conscience et de religion ou à la liberté syndicale. Il a fait valoir que le recueil de ces données sensibles était déjà, par dérogation, autorisé dans le code de la sécurité intérieure, et que seules les activités « susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État » étaient concernées, ce qui « interdit notamment un enregistrement de personnes sur une simple appartenance syndicale ».

La procédure au fond est néanmoins toujours en cours devant le Conseil d'État appelé à statuer prochainement.

Même si l'extension des possibilités de fichage n'est pas sans rappeler la tentative avortée de création du fichier EDVIGE, en 2008, destinée à collecter des informations personnelles sur des personnes et organismes susceptibles de troubler l'ordre public, la délégation considère que les modifications apportées par les décrets du 2 décembre 2020 visent, en partie, à fixer un cadre légal à des pratiques existantes. Le Gouvernement met en avant la lutte contre la radicalisation et la nécessité de mieux détecter les signaux faibles face à une menace terroriste de plus en plus endogène.

Dans ses avis rendus le 25 juin 2020, préalablement à la publication desdits décrets, la CNIL avait considéré que les finalités de traitement des données avaient été suffisamment précisées pour permettre de distinguer clairement les données ayant vocation à être traitées pour des finalités relevant de la « sûreté de l'État » et faisant l'objet d'un encadrement juridique distinct du règlement général sur la protection des données (RGPD). L'autorité administrative indépendante a estimé qu'il était bien établi que seules les activités « susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État » pouvaient être collectées.

En revanche, la délégation regrette que le Gouvernement n'ait pas soumis à la CNIL la rédaction définitive du décret publié le 2 décembre 2020, qui diffère de celle sur laquelle elle s'était prononcée quelques mois auparavant. L'exécutif a en effet substitué aux « activités politiques, philosophiques, religieuses ou syndicales », les termes « opinions » politiques, « convictions » philosophiques et religieuses et l'« appartenance » syndicale.

Au vu du caractère sensible de cette collecte d'informations, la délégation souhaite que le coordonnateur national du renseignement et de la lutte contre le terrorisme puisse à l'avenir régulièrement lui rendre compte de la mise en œuvre, par les services de renseignement, de ces nouvelles possibilités de collecte [*Recommandation n° 3*].

IV. LA REFORTE DU PLAN NATIONAL D'ORIENTATION DU RENSEIGNEMENT (PNOR)

A. LA VOCATION DU PNOR EN TANT QU'OUTIL DE PILOTAGE

Dans sa forme actuelle, le PNOR trouve son origine dans le Livre blanc sur la défense et la sécurité nationale de juin 2008 qui proposait qu'un « Conseil national du renseignement » – qui n'existait pas encore à cette époque – définisse les grandes orientations assignées aux services de renseignement.

La mission avait alors été confiée au Coordonnateur national du renseignement d'élaborer ce document dans le cadre de son rôle consistant à orienter l'action des services, à définir et à orienter les priorités de recherche du renseignement.

Le PNOR est un document qui traite de la menace et de l'orientation des services. Il vise à orienter les capteurs en fonction d'un état de la menace établi préalablement. À la différence de la « stratégie nationale du renseignement », document public adopté en juillet 2019, le PNOR est un document classifié qui constitue la feuille de route des services.

Depuis 2009, le PNOR a fait l'objet de versions successives adoptées par le Conseil national du renseignement : en 2010, en 2012, en 2014 et en 2018. Ce document a fait l'objet d'une refonte en janvier 2021 que le Coordonnateur national du renseignement et de la lutte contre le terrorisme est venu présenter à la délégation le 17 juin 2021.

Cette refonte du PNOR fait apparaître plusieurs éléments nouveaux par rapport à la version précédente de ce document.

- S'agissant tout d'abord de son élaboration, elle a fait l'objet de consultations très larges, pendant plus d'une année, par le Coordonnateur national du renseignement et de la lutte contre le terrorisme. Ces consultations n'ont pas concerné les seuls services de renseignement, mais l'ensemble des ministères. Tous les directeurs de cabinet ont en effet été sollicités pour identifier les besoins des ministères.
- Ensuite, la classification du PNOR est passée de « secret défense » à « confidentiel défense ». Cet assouplissement vise à partager plus facilement ce document afin que les services et les ministères puissent se l'approprier, notamment aux échelons hiérarchiques intermédiaires. La classification « secret défense » limitait en effet très strictement le nombre de ses destinataires.
- Enfin, à la différence des versions précédentes, le choix a été fait de ne pas donner de durée de vie au PNOR adopté en janvier 2021. Il s'agit d'un document vivant, pluriannuel et adaptable en permanence en fonction des menaces.

Dans le cadre de la refonte de janvier 2021, le PNOR évolue aussi dans sa forme : il est désormais constitué d'un document d'orientation, accompagné de fiches d'orientations stratégiques sur huit thématiques spécifiques qui appellent à une attention accrue de l'ensemble des services de renseignement et à une coordination renforcée. Une comitologie de suivi est mise en place par la CNRTL afin de s'assurer de la mise en œuvre des orientations du plan stratégique.

Depuis 2017, Le PNOR est également complété par des « doctrines » qui définissent une répartition des compétences entre les services de renseignement. Ces doctrines concernent par exemple la lutte antiterroriste, la protection de nos intérêts économiques, le contre-espionnage, la contre-prolifération....

En outre, le PNOR s'articule avec des stratégies nationales de protection et de défense, *****. Ces stratégies nationales de protection et de défense ont un périmètre plus large que la seule communauté du renseignement.

B. LES PRINCIPALES MENACES IDENTIFIÉES PAR LE PNOR

En cohérence avec les grandes lignes de la stratégie nationale du renseignement, les priorités du nouveau PNOR s'articulent autour de quatre volets principaux que sont :

- Les menaces terroristes ;
- L'anticipation des crises et les risques de ruptures majeures ;
- La défense et la promotion de notre économie ;
- Les menaces transversales.

*****.

1. Les menaces terroristes

*****.

2. L'anticipation des crises et risques de ruptures majeures

*****.

3. La défense et la promotion de notre économie :

*****.

4. Les menaces transversales

*****.

5. *****

*****.

C. LES FICHES D'ORIENTATION STRATÉGIQUE

Les grandes orientations du PNOR sont complétées par des fiches d'orientation stratégique au nombre de huit. La volonté du CNRLT, en accord avec le Chef de l'État, a été de ne pas multiplier le nombre de ces fiches afin de ne pas enfermer l'action des services de renseignement dans un périmètre trop contraint pour leur laisser un niveau d'autonomie suffisant.

Les thèmes retenus font l'objet de suivis réguliers par la coordination nationale du renseignement et de la lutte contre le terrorisme et peuvent donner lieu à des échanges et décisions en Conseil de défense.

*****.

Parmi les menaces identifiées, le PNOR met en avant un risque d'ingérence de plus en plus prégnant. À cet égard, les parlementaires sont des objectifs pour des services de renseignements étrangers qui cherchent à recueillir des informations stratégiques. Il est nécessaire de renforcer la sensibilisation des élus de la Nation aux risques d'espionnage dont ils peuvent être la cible, en particulier lors de leurs déplacements à l'étranger, dans le cadre de leur mandat, ou à titre privé. À l'occasion de chaque renouvellement de l'Assemblée nationale et du Sénat, un temps de sensibilisation sur les risques d'espionnage liés à leur mandat devrait ainsi être systématiquement et obligatoirement proposé à tous les parlementaires et un kit d'information sur les bonnes pratiques à respecter devrait être intégré à la mallette du député et du sénateur [*Recommandation n° 4*].

V. L'IMPACT DE LA JURISPRUDENCE EUROPÉENNE SUR L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT ET LE PROJET DE LOI RELATIF À LA PRÉVENTION D'ACTES DE TERRORISME ET AU RENSEIGNEMENT

C'est sous la pression des cours européennes, et malgré la résistance des cours nationales, que le cadre légal encadrant les activités de renseignement a été développé en France. La jurisprudence européenne a ainsi permis un développement du contrôle sur l'activité des services de renseignement. La question de l'équilibre entre les droits issus des traités tels qu'interprétés par les juges et la garantie des intérêts fondamentaux de la nation se pose cependant face aux exigences croissantes des cours. Si elles imposent aux autorités nationales de continuer à renforcer les garanties en matière de recours aux techniques de renseignement, les arrêts rendus par la cour européenne des droits de l'homme et surtout par la cour de justice de l'Union européenne au cours des dernières années semblent atteindre les limites du contrôle possible sans remettre en cause les compétences régaliennes de l'État.

A. UNE JURISPRUDENCE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME FONDÉE SUR LE RESPECT DE LA VIE PRIVÉE

L'article 8 de la Convention européenne des droits de l'homme consacre le « droit au respect de la vie privée et familiale ». Il dispose que :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

« 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

C'est sur ce fondement que la Cour a très tôt exigé qu'un cadre légal soit fixé pour encadrer les ingérences dans la vie privée induites par la mise en œuvre d'activités de surveillance. Pour le juge de Strasbourg, la loi non seulement doit exister (que ce soit sous forme d'un texte ou d'une jurisprudence uniforme et constante), mais il faut encore qu'elle présente une certaine « qualité ». Cette notion de « qualité de la loi » est ancienne et figure déjà dans les arrêts Klass du 6 sept. 1978 et Malone du 2 août 1984. *« Elle signifie que la loi doit remplir certains caractères qui sont l'accessibilité et la prévisibilité. Ce dernier mot veut dire que la loi doit user de termes clairs « pour indiquer à tous, de manière suffisante, en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète et virtuellement dangereuse au droit au respect de la vie privée et de la correspondance » (arrêt Malone), ou employer des termes*

précis, nets « pour fournir à l'individu une protection adéquate contre l'arbitraire » (ibid.) »¹.

Deux arrêts de la Cour européenne des droits de l'homme ont condamné la France pour atteinte au droit au respect de la vie privée *CEDH, arrêté Kruslin et époux Huvig c/ France, 24 avril 1990*. Il s'agissait seulement de la deuxième fois que la France était condamnée pour non-respect de la Convention européenne des droits de l'homme à la demande d'un particulier.

En effet, si le droit français remplissait la condition d'accessibilité de la loi, puisque tout citoyen pouvait connaître les règles juridiques relatives aux écoutes, la condition de prévisibilité n'était en revanche pas remplie aux yeux de la Cour. Même si le gouvernement français avait énuméré une liste de dix-sept garanties pour faire juger le contraire. Tout en reconnaissant leur existence, la Cour a alors souligné deux insuffisances dans le dispositif français : d'une part, le caractère fragmentaire de la jurisprudence ; d'autre part et surtout, l'absence de règles sur des points substantiels : les catégories de personnes ou d'infractions susceptibles de donner lieu à des écoutes, les limites à la durée de la mesure, les conditions d'établissement des procès-verbaux, leur contrôle, leur destruction après non-lieu ou acquittement. En conséquence, la Cour a considéré que, du fait de l'imprécision de son droit pour encadrer l'ingérence dans la vie privée des citoyens, la France ne s'était pas conformée aux exigences de l'article 8 de la Convention.

C'est pour faire face aux conséquences de cet arrêt que la première pierre du dispositif de contrôle de l'activité des services de renseignement fut posée par la loi n° 91-646 du 10 juillet 1991 *relative au secret des correspondances émises par la voie des télécommunications*, qui a soumis les **interceptions de sécurité** à une procédure d'autorisation préalable du Premier ministre et à un contrôle, initialement *a posteriori*, d'une commission indépendante, la commission nationale de contrôle des interceptions de sécurité (CNCIS).

Ainsi que l'a rappelé le précédent rapport de la DPR, c'est notamment le risque d'une nouvelle condamnation de la France par la Cour européenne des droits de l'homme qui a conduit à l'élaboration de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

B. UN CONTRÔLE DE LA CJUE LIÉ AUX OBLIGATIONS REPOSANT SUR LA CONSERVATION DES DONNÉES PERSONNELLES

L'intervention de la CJUE en matière de données conservées aux fins de renseignement se fonde sur la directive dite *ePrivacy* de 2002 ; elle a rendu un arrêt de 2016 dit *Tele2*, qui pose le principe de l'interdiction de la conservation généralisée et indifférenciée des données de trafic et de localisation (i.e. des données

¹ Jean Pradel « Une condamnation des écoutes téléphoniques à la française par la Cour européenne des droits de l'homme », *Recueil Dalloz* 1990 p. 353

de connexion), y compris à des fins de sécurité nationale. C'est pour connaître les implications de cette décision sur la législation française que le Conseil d'État, saisi de recours déposés par plusieurs associations et opérateurs, a posé en 2018 une question préjudicielle à la Cour, qui y a répondu par l'arrêt *La quadrature du Net* du 6 octobre 2020.

1. 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, dite *ePrivacy*

Comme l'a rappelé le Conseil d'État dans la question préjudicielle posée à la CJUE en 2018¹, 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, procède de la volonté de rapprocher les législations des États membres afin de permettre l'établissement et le fonctionnement du marché intérieur.

Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le « traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté ». Mais, ainsi que le rappelle son article 1^{er}, paragraphe 3, elle « ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne [...] et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ». Par ailleurs, son article 15 prévoit que « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ».

¹ *Questions préjudicielles à la CJUE sur la conservation des données de connexion, Arrêt rendu par Conseil d'État 10e et 9e chambres réunies, 26-07-2018, n° 394922 394925 397844 397851, mentionné aux tables.*

Les États membres sont ainsi autorisés, pour des motifs tenant à la sûreté de l'État ou à la lutte contre les infractions pénales, à déroger, notamment, à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, de la directive.

2. Le contrôle exercé par la CJUE sur le respect de cette directive et l'arrêt Tele2

Pendant dans son arrêt *Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres* (C-203/15 et C-698/15), du 21 décembre 2016, la CJUE a estimé qu'il résulte des dispositions de la directive du 12 juillet 2002 qu'elle « doit être regardée comme régissant les activités des fournisseurs [de services de communications électroniques] ». Elle a considéré que les dispositions imposant des obligations à ces fournisseurs, telles que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation de leurs utilisateurs et abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de la directive du 12 juillet 2002, parmi lesquelles figure la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique, relèvent dès lors du champ d'application de cette directive, dans la mesure où elles régissent leur activité. Par ailleurs, le fait que de telles obligations n'interviennent qu'aux seules fins de rendre accessibles aux autorités nationales compétentes les données personnelles qu'elles concernent, implique que la réglementation nationale encadrant l'accès et l'utilisation de ces données relève également du champ d'application de la directive du 12 juillet 2002. En revanche, les dispositions nationales qui portent sur des techniques de recueil de renseignement directement mises en œuvre par l'État sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques ne relèvent pas du champ d'application de cette directive.

Outre la compétence de la CJUE sur les législations nationales en matière de conservation des données, l'arrêt « *Télé2* » affirme que le droit de l'Union s'oppose à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données.

La Cour considère ensuite que, si la directive du 12 juillet 2002 permet aux États membres de limiter la portée de l'obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes, elle ne saurait justifier que la dérogation à cette obligation de principe et, en particulier, à l'interdiction de stocker ces données, prévue par celle-ci, devienne la règle.

En outre, la Cour rappelle sa jurisprudence constante selon laquelle la protection du droit fondamental au respect de la vie privée exige que les dérogations à la protection des données à caractère personnel s'opèrent dans les limites du strict nécessaire. La Cour applique cette jurisprudence aux règles régissant la conservation des données et à celles régissant l'accès aux données conservées.

La Cour constate, s'agissant de la conservation, que les données conservées prises dans leur ensemble sont susceptibles de permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données ont été conservées.

Elle en déduit que l'ingérence résultant d'une réglementation nationale prévoyant la conservation des données relatives au trafic et des données de localisation doit donc être considérée comme particulièrement grave. Le fait que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer, dans l'esprit des personnes concernées, le sentiment que leur vie privée fait l'objet d'une surveillance constante. Par conséquent, seule la lutte contre la criminalité grave est susceptible de justifier une telle ingérence.

La Cour relève qu'une réglementation prévoyant une conservation généralisée et indifférenciée des données ne requiert pas de relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et ne se limite notamment pas à prévoir une conservation des données afférentes à une période temporelle et/ou une zone géographique et/ou un cercle de personnes susceptibles d'être mêlées à une infraction grave. Une telle réglementation nationale excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exige la directive lue à la lumière de la Charte.

En répondant à la question préjudicielle posée par le Conseil d'État en 2018 par l'arrêt *La Quadrature du Net* du 6 octobre 2020, la CJUE procède à plusieurs distinctions fondées sur le niveau d'atteinte à la vie privée. Ces distinctions portent sur les types de données, leurs modalités de traitement, qui comprend les modalités de conservation et d'accès et fixe les finalités légitimes de conservation. Ce panorama très exhaustif tend à délimiter la possibilité pour les États de définir des règles de conservation.

S'agissant des types de données, la Cour distingue données de trafic et données de localisation, dont la conservation est celle qui risque de porter le plus atteinte à la vie privée, ainsi que l'adresse IP qui permet de savoir à partir de quel outil la communication est faite, et l'identité civile de l'utilisateur des services de communication.

La Cour se penche également sur les types de traitement des données en distinguant la conservation généralisée et indifférenciée et la conservation ciblée, plus aisément compatible avec les exigences du droit de l'Union, subdivisée entre le ciblage en fonction de catégories de personnes et le ciblage géographique. Au-delà de la conservation, la Cour s'estime compétente pour juger de l'accès aux données conservées, en distinguant le recueil en temps réel ou différé, ce dernier étant considéré comme moins attentatoire à la vie privée que le premier. La Cour fait référence à la possibilité de conservation dite rapide des données, susceptible d'être utilisée pour la lutte contre la criminalité grave. Enfin, elle mentionne le traitement sous la forme d'une analyse automatisée des différentes données disponibles, soit l'algorithme.

La Cour différencie les atteintes en fonction de la finalité du traitement poursuivi, la légitimité des finalités correspondant à la possibilité de recourir à la conservation et au traitement des données :

- les atteintes à la sécurité nationale ;
- la criminalité grave et les atteintes graves à la sécurité publique ;
- enfin la détection et la poursuite d’infractions pénales.

La possibilité laissée aux États de définir un régime de conservation des données a donc semblé particulièrement faible, et cette décision est parue de nature à remettre en cause l’ensemble du cadre légal français en matière de conservation des données et de techniques de renseignement.

C. UN CADRE NATIONAL CONFORTÉ PAR LA JURISPRUDENCE DU CONSEIL D’ÉTAT ET LES ÉVOLUTIONS APPORTÉES PAR LE PROJET DE LOI RELATIF À LA PRÉVENTION D’ACTES DE TERRORISME ET AU RENSEIGNEMENT, MAIS LA PERMANENCE D’ENJEUX COMPLEXES.

Initialement destiné à tirer les conséquences des échéances prévues par la loi du 24 juillet 2015, la loi du 30 juillet 2021 relative à la prévention d’actes de terrorisme et au renseignement tire les conséquences de la jurisprudence de la CJUE et de la décision du Conseil d’État, 21 avril 2021, French Data Network et autres.

1. Les garanties apportées par le projet de loi relatif à la prévention d’actes de terrorisme et au renseignement

La décision du Conseil d’État du 21 avril 2021 a été largement perçue comme posant un équilibre entre les exigences posées par la CJUE et le cadre institutionnel français. Cet équilibre repose essentiellement sur deux points : la possibilité de conservation de données fondées sur l’état d’une menace grave constatée annuellement par un décret du Premier ministre et le renforcement du contrôle *a priori* des techniques de renseignement exercé par la CNCTR.

En conséquence la loi du 30 juillet 2021 instaure un nouveau régime juridique en matière de conservation des données et, pour les techniques de renseignement soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement (CNCTR), tire les conséquences de l’arrêt de la Cour de justice de l’Union européenne (CJUE) du 6 octobre 2020 et de la décision French data Network et autres du Conseil d’État du 21 avril 2021.

La loi modifie les articles L. 34-1 du code des postes et des communications électroniques (CPCE) et 6 de la loi du 21 juin 2004 pour la confiance dans l’économie numérique (LCEN). Elle prévoit qu’en cas de menace grave, actuelle ou prévisible pour la sécurité nationale, le Premier ministre peut enjoindre aux opérateurs de communications électroniques, par un décret dont la durée d’application ne peut excéder un an, de conserver, pour une durée d’un an, certaines

catégories de données de connexion dont la nature serait précisée par un décret en Conseil d'État.

Il est également inscrit dans la loi la durée de conservation – ainsi que les finalités de cette conservation – des diverses catégories de données et informations.

Enfin, la loi du 30 juillet 2021 prévoit la possibilité, pour les autorités disposant en vertu de la loi d'un accès aux données relatives aux communications électroniques à des fins de prévention de la criminalité grave ou d'autres manquements aux règles dont elles sont chargées d'assurer le respect, de prononcer une injonction de conservation rapide.

Bien qu'il réduise les capacités d'enquête de l'autorité judiciaire en cas d'infractions pénales ordinaires, conformément à la lettre de l'arrêt européen, le nouveau dispositif législatif permet de conserver les capacités opérationnelles des services de renseignement et celles de l'autorité judiciaire en cas de « criminalité grave ».

La loi du 30 juillet 2021 étend également à toute technique de renseignement le mécanisme prévu pour l'introduction dans un lieu privé à usage d'habitation lorsque la CNCTR émet un avis défavorable sur une demande. Dans ce cas, la saisine de la formation spécialisée du Conseil d'État compétente en matière de techniques de renseignement sera obligatoire et celle-ci ne pourra être mise en œuvre, sauf urgence, avant qu'elle n'ait statué. La formation spécialisée devra se prononcer en 24 heures.

2. La nécessité d'anticiper sur les exigences posées par le droit européen

Au regard des exigences anciennes mais toujours importantes de la CEDH et des nouvelles exigences posées par la CJUE, la France doit agir le plus en amont possible des évolutions jurisprudentielles et surtout des condamnations dont elle pourrait faire l'objet

a. Une action sur le droit de l'Union européenne

Dans son arrêt du 21 avril 2021, le Conseil d'État s'est refusé à contrôler la compétence de la CJUE pour intervenir sur les questions relatives au renseignement. Ce débat n'est cependant pas clos et il appartient au Gouvernement, en accord avec les autres États membres, de faire évoluer le droit européen vers une meilleure prise en compte des enjeux liés à la protection des intérêts fondamentaux de la nation. La fin des négociations sur le règlement *ePrivacy* appelé à remplacer la directive de 2002 pourrait être une première occasion en ce sens.

b. La question des échanges d'informations avec les services étrangers.

Par deux arrêts du 25 mai 2021 (n° 58170/13, *Big Brother Watch* et autres) et du 19 juin 2018 (n° 35252/08, *Centrum för rättvisa c. Suède*) la CEDH a condamné le Royaume-Uni et la Suède pour ne pas avoir entouré de suffisamment

de garanties leurs régimes d'obtention de données de communication auprès des fournisseurs de services de communication. Cette condamnation a cependant été largement vue comme offrant aux États des possibilités de conservation des données plus large que celles découlant de la jurisprudence de la CJUE, conformément à l'article 8.2 de la Convention européenne des droits de l'homme.

Cependant la Cour a également été conduite à se prononcer dans ces deux affaires sur la réception de renseignements obtenus auprès de gouvernements et/ou de services de renseignement étrangers. En ce domaine la Cour paraît exiger un niveau de contrôle similaire, sinon identique à celui exercé pour les renseignements recueillis par les services nationaux. La législation française pourrait donc être appelée à évoluer.

Il paraît impossible à la DPR qu'une telle évolution, qui implique les relations internationales de la France et l'existence de liens de confiance avec des services étrangers, se fasse de manière abrupte. Il est cependant nécessaire que le Gouvernement et les services réfléchissent au cadre le plus adapté pour permettre à la France de respecter ses obligations au regard de la Convention européenne des droits de l'homme [*Recommandation n° 5*].

CHAPITRE III LA CONTINUITÉ DES MISSIONS DE RENSEIGNEMENT PENDANT LA CRISE SANITAIRE

I. LE RISQUE PANDÉMIQUE EST CLAIREMENT IDENTIFIÉ, MAIS INSUFFISAMMENT SUIVI PAR LES SERVICES DE RENSEIGNEMENT

A. UN RISQUE PRIS EN COMPTE PAR LA REVUE STRATÉGIQUE DE DÉFENSE ET DE SÉCURITÉ NATIONALE DE 2017

Dans la revue stratégique de défense et de sécurité nationale de 2017, les risques sanitaires sont présentés comme des « fragilités », des « facteurs d'aggravation des crises ».

Revue stratégique de défense et de sécurité nationale de 2017 (*extraits*)

3. Des fragilités multiples, facteurs d'aggravation des crises

[...]

3.3. Risques sanitaires

69. L'accroissement de la mobilité de la population favorise l'extension des aires de diffusion de certaines maladies, ainsi que la propagation rapide et à grande échelle de virus à l'origine d'épidémies diverses (syndrome respiratoire aigu sévère – SRAS). Le service de santé des armées et ses capacités de recherche sont ainsi régulièrement mobilisés pour faire face à ce type de situation. La dernière épidémie d'Ébola survenue en 2014-2016 dans des pays fragiles d'Afrique de l'Ouest a démontré combien la densification des flux pouvait compliquer le confinement des grandes crises sanitaires, au point de devoir faire appel à la communauté internationale.

70. Le risque d'émergence d'un nouveau virus franchissant la barrière des espèces ou échappant à un laboratoire de confinement est réel. De même, l'interconnexion des filières alimentaires génère des risques sur la santé humaine et offre un terrain propice à d'éventuelles actions « agro-terroristes ». Plus grave encore, la diffusion des biotechnologies pourrait permettre à des groupes terroristes de conduire des attaques biologiques sophistiquées.

Ainsi, l'émergence d'un nouveau virus est bel et bien prise en compte parmi les risques sanitaires susceptibles d'avoir des conséquences sur nos intérêts. *****.

B. POURTANT, LES SERVICES DE RENSEIGNEMENT N'AVAIENT, JUSQU'ALORS, DÉVELOPPÉ AUCUNE CAPACITÉ D'ANTICIPATION

Force est de constater que la pandémie de coronavirus a engendré des bouleversements sur le plan géopolitique, et fait peser des risques quant à notre souveraineté économique, technologique et scientifique avec, notamment, des tentatives de prédation sur des entreprises et des savoir-faire français. *****.

Dans la mesure où les crises sanitaires naissent principalement hors de nos frontières, il semblerait utile que les services de renseignement français présents à l'étranger puissent être associés à une telle démarche, afin de tenir compte, comme en matière de contre-terrorisme, du continuum entre sécurité extérieure et intérieure. À cet effet, plusieurs capteurs pourraient utilement être utilisés et orientés sur ce sujet : recherche sur les réseaux sociaux (renseignement d'ambiance), recrutement de sources étrangères spécialisées dans le domaine épidémiologique (renseignement humain et « d'alerte »), analyse de l'imagerie satellitaire pour détecter des comportements anormaux (construction soudaine d'infrastructures médicales, hausse sensible de la fréquentation des cimetières, etc.). À ce titre, la Délégation estime nécessaire de mettre en œuvre une capacité interservices d'anticipation et d'appréciation des menaces sanitaires [*Recommandation n° 6*].

II. MALGRÉ LE CONFINEMENT, LES SERVICES ONT ASSURÉ LA CONTINUITÉ DE LEURS MISSIONS ESSENTIELLES

Naturellement, le confinement n'a pas été sans conséquence sur l'organisation interne des services de renseignement, sans pour autant interrompre leurs activités identifiées comme prioritaires.

A. LORSQUE LA CRISE SANITAIRE S'EST DÉCLARÉE, TOUS LES SERVICES DE RENSEIGNEMENT NE DISPOSAIENT PAS D'UN PLAN DE CONTINUITÉ D'ACTIVITÉ ADAPTE

1. Un document indispensable pour surmonter une crise nouvelle et soudaine

En mars 2020, alors que le premier confinement venait d'être annoncé, tous les services de renseignement, *****, disposaient d'un plan de continuité d'activité (PCA) ou d'un document équivalent. *****.

En cas de pandémie, le PCA doit prendre en compte les risques sanitaires afin, notamment, de protéger les agents, de limiter la contagion au sein du service et de conserver sa capacité à mener ses missions essentielles, quel que soit le degré ou la phase de la crise sanitaire. À ce titre, le PCA doit préciser, entre autres, les missions prioritaires du service, son organisation interne pour assurer la continuité desdites missions et le nombre maximal d'agents pouvant être présents dans les locaux du service en prévoyant, si nécessaire, un redéploiement des effectifs vers un ou plusieurs autres sites. Le profil des agents doit d'ailleurs faire l'objet d'un examen approfondi : situation personnelle (état de santé connu, enfants à charge, distance entre le domicile et le lieu de travail, capacité de déplacement autonome), polyvalence au regard des missions à exercer, capacité d'accueil dans les locaux du service au regard des règles de distanciation sociale et des contraintes immobilières (bureau individuel ou collectif), etc.

2. Les plans de continuité d'activité des services ont rapidement évolué pour prendre en compte la situation sanitaire

*****.

Afin d'éviter, à l'avenir, toute impréparation à la survenance d'un risque déjà anticipé, les services sont invités à consolider leur plan de continuité d'activité.

Aussi, il convient d'accompagner les services de renseignement des premier et second cercles dans la rédaction d'un plan de continuité d'activité (PCA) prenant en compte l'ensemble des risques décrits par la revue stratégique de défense et de sécurité nationale de 2017. Ce PCA devra, entre autres, identifier les moyens informatiques et de communication nécessaires à la poursuite des missions jugées essentielles ou prioritaires, y compris à distance [*Recommandation n° 7*].

B. UNE ACTIVITÉ RÉDUITE ET RECENTRÉE SUR LES MISSIONS PRIORITAIRES

1. L'organisation interne des services

Après que le premier confinement a été annoncé par le Président de la République, les services ont décidé, sur la base de leurs PCA, de réduire la présence de leurs agents sur site. L'ensemble des services a choisi le travail par roulement pour éviter que les agents ne se croisent et réduire ainsi les risques de contagion du virus en leur sein.

Tous les services ont adapté leurs conditions de travail à la situation : respect strict des gestes barrières, organisation de « bordées », mise en place d'horaires de travail décalés, aménagement des locaux de restauration, etc.

*****.

2. Une activité concentrée sur les missions jugées essentielles

Compte tenu de cette réduction d'effectifs, les services de renseignement ont dû définir des priorités afin d'assurer, sur celles-ci, la continuité de leurs missions.

*****.

L'ensemble des services ont pu garantir les missions prioritaires qu'ils ont identifiées.

TABLEAU

Missions investies prioritairement par les services de renseignement lors du premier confinement

3. La coopération internationale a été sensiblement ralentie par la crise, au contraire de la coopération interservices

Les échanges avec les partenaires étrangers ont fortement diminué en raison des conséquences du confinement (tarissement des flux migratoires, ralentissement de l'activité économique, etc.). *****.

Compte tenu des mesures de restriction de déplacements, certains services ont entretenu leurs relations partenariales par visioconférence, quand cela était compatible avec la nécessaire confidentialité des échanges, ou par l'entremise des détachements et des postes à l'étranger.

S'agissant des outils de visioconférence, les services relevant du ministère des armées ont parfois privilégié l'emploi de moyens de communication classifiés interalliés. *****.

En revanche, la coopération entre les services au niveau national s'est maintenue pendant la crise sanitaire grâce aux bordées organisées dans chaque service et aux moyens dématérialisés de communication. Cependant, les services se sont heurtés aux limites de certains outils de visioconférence et à la multiplicité des plateformes techniques utilisées.

Afin d'assurer la permanence de la coopération interservices lorsque les réunions ne peuvent se tenir en présentiel, tout en garantissant la préservation du secret de la défense nationale, il est important que les services puissent bénéficier d'outils de téléphonie et de visioconférence souverains et classifiés, ***** , qui permettent d'organiser des audioconférences réunissant plusieurs participants. À cet égard, au-delà de ces deux solutions difficiles à déployer à grande échelle, les services pourraient s'appuyer sur l'interconnexion existante pour développer de telles solutions, comme ils le font déjà grâce à leurs réseaux internes respectifs

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) pourrait se voir confier la mise en œuvre d'un outil de visioconférence souverain et sécurisé permettant aux services de l'État, dont les services de renseignement, d'échanger des informations classifiées [*Recommandation n° 8*].

4. Un recours au télétravail très restreint

Les agents des services n'ont pu recourir que très marginalement au télétravail, pour des raisons de sécurité d'une part, aucune donnée classifiée ne pouvant être traitée sur un ordinateur personnel ou au domicile des agents, et pour des raisons juridiques d'autre part, le cadre réglementaire n'ayant pas ouvert cette possibilité pour les agents de certains services.

Ainsi, seuls les agents ayant des missions compatibles avec le télétravail – c'est-à-dire pouvant s'exercer sans accès aux applications classifiées (fonctions supports, principalement) – ont pu travailler à distance pendant le confinement. *****.

Néanmoins, certains services du second cercle, ***** , se sont heurtés à leur manque de moyens informatiques pour autoriser un accès élargi au télétravail. En effet, en centrale, moins de dix personnes étaient équipées du matériel nécessaire au début de la crise sanitaire, et ces agents ont rencontré des problèmes de connexion car le réseau n'était pas configuré pour supporter une telle charge liée au travail à distance. Le télétravail a donc nécessité l'utilisation de moyens personnels (matériels informatiques) ou professionnels (téléphones de service) qui présentent des limites en termes de sécurité et de traces laissées sur les sites internet visités.

*****.

C. DES CONSÉQUENCES SUR LE RECRUTEMENT LIMITÉES

La crise sanitaire n'a pas véritablement perturbé les plans de recrutement des services. En effet, les procédures de recrutement lancées avant le confinement ont simplement été ajournées et les concours ont pu se tenir. Si certains événements comme la participation aux salons étudiants ont dû être annulés, ils ont été compensés par une présence croissante sur les réseaux sociaux.

Certains recrutements de personnels contractuels, dont le contrat de travail avait été signé avant le début du premier confinement, n'ont pas pu être différés. Leur prise de fonctions s'est donc déroulée dans un contexte où les effectifs étaient essentiellement placés en télétravail ou en autorisation spéciale d'absence, ce qui n'a pas permis de les accueillir et de les former convenablement pendant plusieurs semaines. Ce retard a néanmoins été résorbé à la faveur du déconfinement et de la reprise progressive de l'activité des services.

Eu égard aux conséquences de la crise sanitaire sur le marché de l'emploi, certains services ont noté un accroissement important du nombre de candidatures reçues, y compris pour le recrutement de certains profils techniques dans les filières sous tension.

Enfin, il convient de souligner que cette crise n'a conduit aucun service à revoir le profil des personnes recrutées ; les métiers et les profils recherchés sont demeurés identiques. Ainsi, il n'est pas envisagé de recruter des médecins ou des chercheurs pour travailler à la prévention de ce type de risques.

III. PENDANT LA CRISE SANITAIRE, LES MENACES PESANT SUR LA FRANCE ET SES INTÉRÊTS N'ONT PAS FLÉCHI

A. LA CRISE N'A PAS EU DE CONSÉQUENCE SUR L'ÉVOLUTION DE LA MENACE TERRORISTE, TOUJOURS AUSSI PRÉGNANTE

La situation sanitaire n'a pas eu d'incidence notable sur la menace terroriste djihadiste qui est demeurée à un niveau très élevé.

En revanche, les mouvances violentes d'ultra-gauche et d'ultra-droite ont vu en la crise sanitaire un contexte propice à l'action, chacune voyant dans les origines supposées de la pandémie une validation de ses propres thèses :

- lors du premier confinement, l'ultra-gauche a diffusé un appel à un « *mois de mai dangereux* », et continue depuis de prospérer dans un contexte social tendu ;
- pour la mouvance d'ultra-droite, la crise sanitaire a été perçue comme un évènement validant ses thèses survivalistes, complotistes et racistes : repli communautaire sur des bases à défendre, critique des valeurs républicaines comme prétexte à l'instauration d'une dictature, rejet de l'immigration, etc.

Les restrictions imposées par la crise sanitaire ont exacerbé les mécontentements sociaux et idéologiques qui ont donné lieu à des contestations ainsi qu'à des occupations de la voie publique. Les manifestations du premier trimestre 2021 ont pu avoir un effet exutoire pour certains individus, signe d'un comportement plus hostile vis-à-vis des institutions et de la force publique. Enfin, la pandémie a fait naître d'autres motifs et formes de contestation : contestation virtuelle, mouvements anti-masque et anti-vaccin, contestation des mesures de restriction de liberté, etc.

B. LES TENTATIVES D'INGÉRENCE N'ONT PAS CONNU DE RÉELLE ÉVOLUTION, MAIS LES RISQUES SE SONT ACCENTUÉS

Après une période d'adaptation, la DGSI a observé une certaine constance des activités d'espionnage et des tentatives d'ingérence ou d'influence menées sur le territoire national par les principaux services offensifs *****.

C. LES TRAFICS ET LES FRAUDES N'ONT PAS BAISSÉ NON PLUS

Durant la pandémie, la DNRED a constaté une forte résilience des trafiquants qui se sont rapidement adaptés aux contraintes logistiques en recourant davantage au fret et au transport par poids lourds, moins concernés par les restrictions de déplacements. Par ailleurs, le service relève un accroissement des menaces d'arnaques et de fraudes sur des produits sanitaires.

Le trafic de cocaïne n'a pas faibli pendant la crise sanitaire ; au contraire, le maintien des flux maritimes l'a renforcé. En revanche, la fermeture des frontières décidée lors du premier confinement a porté un coup d'arrêt aux échanges commerciaux et a suspendu certains schémas de fraude, par exemple la contrebande d'alcool. Cependant, un effet de rattrapage temporaire a pu être observé lorsque les frontières ont rouvert.

Tracfin s'est intéressé aux fraudes au chômage partiel et au prêt garanti par l'État, ainsi qu'à la prédation économique *****.

D. DES DIFFICULTÉS SE SONT FAIT JOUR AU SEIN DE CERTAINS ÉTABLISSEMENTS PÉNITENTIAIRES

La pandémie a mis en exergue des vulnérabilités au sein de certains établissements pénitentiaires (arrêt des activités et des visites, absence de nombreux personnels de surveillance) et un potentiel d'aggravation des difficultés de gestion de la population pénale (mutineries, agressions, destructions de biens et d'équipements).

Ces éléments ont été pris en compte, dès le premier confinement, par le SNRP qui a renforcé la veille et la collecte de renseignements au profit de la sécurité des établissements et des personnels pénitentiaires. Grâce à une veille sur les réseaux sociaux, une équipe d'analystes-veilleurs a permis d'identifier des menaces ayant pour origine des personnes détenues ou leurs proches. Ces informations ont alimenté la cellule de crise mise en place au sein de la direction de l'administration pénitentiaire.

L'ordonnance n° 2020-303 du 25 mars 2020 portant adaptation de règles de procédure pénale sur le fondement de la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, a permis de réduire les difficultés causées par la surpopulation carcérale dans certains établissements. Les mesures prises ont entraîné une baisse des menaces d'atteinte à la sécurité des établissements et des personnels pénitentiaires.

Le service a également fait part des adaptations et priorisations rendues nécessaires afin d'assurer le maintien de son activité opérationnelle habituelle¹, en même temps que la gestion des effets de la crise sanitaire sur les tentatives ou les actions de déstabilisation des établissements pénitentiaires.

¹ Rédaction de notes de renseignement, de mesures de police administrative et de réponses à réquisitions judiciaires ; actualisation des tableaux de suivi des sortants de prison ; etc.

CHAPITRE IV LE RENSEIGNEMENT TERRITORIAL, MAILLON CLÉ DE LA SÉCURITÉ INTÉRIEURE

I. LE RENSEIGNEMENT DE PROXIMITÉ EN PREMIÈRE LIGNE FACE AUX NOUVEAUX RISQUES D'ATTEINTE À L'ORDRE PUBLIC ET À LA PRÉVENTION DU TERRORISME

Tant la stratégie nationale du renseignement adoptée en juillet 2019 que le Livre blanc sur la sécurité intérieure de septembre 2020 alertent sur l'évolution des menaces et affirment le rôle confié aux services de renseignement en matière d'anticipation des crises et des risques de ruptures majeures.

Le renseignement de proximité, dont l'organisation actuelle est encore récente, est en première ligne face à la multiplication des phénomènes contestataires, aux tentations séparatistes liées à certaines dérives religieuses et à la persistance d'une menace terroriste devenue endogène.

A. LA MULTIPLICATION DES PHÉNOMÈNES CONTESTATAIRES

Plus nombreux et souvent plus violents, les phénomènes contestataires touchent l'ensemble du territoire national, tant en milieu urbain que dans le monde rural. L'évolution des modes opératoires rend l'expression de ces contestations souvent moins prévisibles et plus difficiles à appréhender.

1. Des contestations plus nombreuses et plus radicales...

La décennie qui vient de s'écouler a été marquée par des mouvements sociaux et sociétaux d'ampleur qui se sont traduits par des mobilisations importantes, qu'il s'agisse par exemple des manifestations contre le mariage pour tous (2013), contre la loi travail El Khomri (2016), contre la réforme de la SNCF (2018) ou encore contre le projet de système de retraites à points (2019). Ces contestations ont pris des formes classiques à travers les traditionnelles manifestations de voie publique à l'initiative de syndicats ou de grandes associations.

À ces mouvements, importants par leur ampleur mais habituels dans la façon dont ils se sont exprimés, se sont ajoutées d'autres formes de contestations, plus spontanées et rapides en termes de mobilisation, témoignant de nouveaux modes opératoires, avec des regroupements qui ne sont pas toujours déclarés et s'affranchissent souvent des principes de la réglementation des manifestations sur de voie publique.

Le **mouvement des Gilets Jaunes**, commencé le 17 novembre 2018 et qui s'est installé dans la durée, en est l'exemple le plus emblématique. L'absence d'organisation structurée et d'interlocuteurs identifiés a représenté un défi pour les services de renseignement en termes d'anticipation et de suivi de la contestation.

La période récente est également marquée par plusieurs phénomènes concomitants :

- La résurgence de mouvements contestataires, qu'ils soient de l'**ultra gauche** ou de l'**ultra droite**. L'ultra droite conteste la légitimité d'un État en déficit d'autorité tandis que l'ultra gauche cherche à déstabiliser le système avec un discours justifiant la violence et une dialectique insurrectionnelle.
- L'apparition de **mouvements radicaux**, tels « Extinction Rébellion », qui appellent à la désobéissance civile non violente en réponse à un État jugé oppresseur ou *a minima* le complice de dérives sociétales.
- Le développement, à la faveur de la crise sanitaire, de **mouvements subversifs**. Même marginaux, ces mouvements environnementalistes, anti-nucléaires, animalistes, féministes, ou liés aux phénomènes émergents du masculinisme, du survivalisme, du complotisme peuvent ainsi accueillir des individus radicaux susceptibles de basculer dans l'action violente.

Des contestations qui procèdent de l'importation de **mouvements liés à des problématiques extérieures au territoire national**, à l'instar du mouvement *#metoo* ou de celui des « *Black Lives Matter* » avec la spontanéité des manifestations françaises dénonçant les circonstances du décès de George Floyd survenu aux États-Unis. Cette importation de causes étrangères, capables de mobiliser des publics parfois novices en matière de manifestations sur la voie publique, représente un défi pour le renseignement territorial à la fois dans la détection du fait générateur et dans l'évaluation des volumes de mobilisation. L'interdiction par la préfecture de police de Paris d'une manifestation de soutien à Gaza prévue le 15 mai 2021 a été ainsi justifiée par « *un risque sérieux que les affrontements entre Palestiniens et forces de l'ordre israéliennes ne se transportent sur le territoire national* », occasionnant « *des troubles graves à l'ordre public* ».

2. ... qui concernent l'ensemble du territoire...

Caractérisé par son utilisation des réseaux sociaux, son horizontalité et sa déconcentration, le mouvement des Gilets Jaunes a montré sa capacité de mobilisation simultanée sur l'ensemble du territoire, tant en milieu urbain que dans le monde rural qui se révèle être un théâtre à part entière de contestations.

Ainsi les ZAD – zones d'aménagement différé devenues « zones à défendre » – expriment une nouvelle forme de contestation politique de la part de ceux qui les occupent et qui revendiquent une quête de sens et pour certains un mode

ultime d'action. Ce sont de véritables villages en lutte qui se sont ainsi constitués un temps à Notre-Dame-des-Landes, mais aussi à Bures (66) contre le centre de stockage de déchets nucléaires, à Roybon (38) contre la construction d'un *Center Parcs* ou à Strasbourg (67) contre le contournement ouest de la ville.

Entre mars 2020 et mars 2021, la zone gendarmerie, qui couvre 95 % du territoire national, mais seulement 52 % de la population, a été le théâtre d'environ 150 faits judiciairisés. Il s'agit souvent d'actions violentes commises contre des agriculteurs ou de démontage d'antennes relais 5G qui sont généralement le fait de mouvements contestataires de l'ultra-gauche.

Les phénomènes contestataires touchent également l'outre-mer, notamment aux Antilles. Mayotte fait également l'objet d'une attention particulière du fait d'une situation sociale particulièrement fragile dans un département où 90 % de la population est de confession musulmane. En Nouvelle-Calédonie, la préparation du troisième référendum sur l'indépendance appelle également à une vigilance particulière quant à de possibles regains de violence.

3. ...amplifiées par les réseaux sociaux ...

Le développement des réseaux sociaux et des usages numériques n'est plus un phénomène nouveau, mais il rend sensiblement plus difficile la tâche des services de renseignement.

Les réseaux sociaux sont des amplificateurs, tant des sujets que des mobilisations. Internet met chacun au même niveau et favorise la constitution de groupe qui permet à leurs membres d'échanger librement et gratuitement parfois sur des sujets illégaux. Le recours accru aux messageries cryptées (*Telegram*, *WhatsApp*) représente un défi supplémentaire pour les services de renseignement. En juin 2020, dans le contexte du premier déconfinement, environ 2000 personnes ont participé à une fête improvisée à Paris, sur l'esplanade des Invalides. L'invitation à cette fête baptisée « *Projet X* », en référence au film américain sorti en 2012, avait été lancée à peine quelques heures auparavant et n'a pu être entravée. S'en sont suivis des affrontements avec les forces de l'ordre. Le même phénomène s'est reproduit au même endroit le 12 juin 2021.

*****.

4. ...et qui s'accompagnent d'une recrudescence des violences

« La montée en puissance des mouvements et réseaux à caractère subversif constitue un facteur de crise d'autant plus préoccupant qu'ils visent directement à affaiblir voire à ruiner les fondements de notre démocratie et les institutions républicaines par la violence insurrectionnelle. Cela se traduit par des actions violentes contre les personnes ou contre les biens (black bloc, pénétration dans les enceintes protégées, sabotages...), mais aussi par la captation des revendications traditionnelles que ces mouvements s'emploient à infiltrer afin de les radicaliser »

Stratégie nationale du renseignement – juillet 2019

La contestation de l'autorité a laissé la place à des atteintes à l'autorité (forces de l'ordre, élus locaux et nationaux), témoignant d'une désinhibition des colères.

De manière générale, indépendamment de l'idéologie défendue, le recours à la violence est décomplexé et son degré élevé. L'ultra-droite se singularise par une appétence pour les armes létales.

Dans ce contexte, le nouveau **schéma national du maintien de l'ordre**, présenté le 16 septembre 2020 par le ministre de l'Intérieur, confie aux services de renseignement la charge *« d'assurer un suivi dans la durée des mouvements contestataires les plus radicaux, à l'origine d'actions violentes. Ce travail doit permettre de déjouer des projets d'actions violentes au sein ou en marge des manifestations, voire d'envisager la dissolution de certains groupes constitués lorsque les conditions de droit sont réunies »*.

Les mouvements de subversion violente constituent en effet une menace réelle caractérisée par un recours décomplexé à la violence et parfois par une remise en cause des principes fondamentaux de la République et des institutions. Au-delà de l'idéologie violente qu'ils promeuvent, ces groupes constituent également un risque au titre des oppositions qu'ils suscitent. Loin d'être tournés exclusivement vers la remise en cause d'un système qu'ils dénoncent unanimement, ces groupuscules violents restent également focalisés sur la lutte contre l'idéologie adverse qu'ils n'hésitent pas à combattre physiquement par le recours à la violence. Ces mouvances continuent à faire des émules au sein de populations jeunes et volontaires, malgré les coups d'arrêt portés à une frange « historique » grâce aux mesures de dissolution administrative qui ont pu être mises en œuvre.

La remise en cause de l'État tous azimuts entraîne la délégitimation de l'État, le faisant apparaître comme un acteur bloquant qu'il convient de contourner voire de combattre. Privé de son statut d'arbitre et donc de vecteur d'apaisement, l'État laisse le champ libre à des individus désireux d'exprimer leurs idées et leurs visions en dehors du cadre démocratique y compris en ayant recours à la violence. Cette situation crée des lignes de fractures entre idéologies et pratiques incompatibles pouvant aller jusqu'à l'affrontement physique : agriculteurs contre défenseurs de l'environnement ou de la cause animale, identitaires contre tenants d'une pratique rigoriste de l'Islam, mouvance anarcho-autonome contre les projets d'aménagements ou de déploiement technologiques, affrontements entre communautés étrangères... On a ainsi assisté, en juin 2020, à une véritable expédition punitive menée dans un quartier de Dijon par environ 200 Tchétchènes en représailles de l'agression de l'un des leurs.

B. LES MOUVEMENTS SÉPARATISTES LIÉS AUX DÉRIVES RELIGIEUSES

Le service central du renseignement territorial est chargé du suivi de l’Islam de France. Cela concerne les grandes fédérations et représentations de l’Islam de France, les mouvements religieux musulmans, les projets de mosquées, le recensement des lieux de culte ainsi que des problématiques liées à l’islam (hallal, pèlerinage, financement des lieux de culte, formation des imams, enseignement). Le SCRT assure également la détection et le suivi des déstabilisations de mosquées, des mouvements radicaux et dérives communautaires.

Selon Lucile Rolland, directrice du SCRT, « *l’immense majorité des lieux de culte ne pose aucun problème. Mais une petite minorité propage un discours fondamentaliste, comme il en existe dans les deux autres religions du Livre. Une fraction encore plus faible répond à un discours pouvant être qualifié de séparatiste. Il peut être qualifié ainsi, car il fait prévaloir la loi de Dieu sur la loi des hommes, et particulièrement sur celles de la République* »¹. Sur environ 2 400 lieux de culte musulmans en France, moins d’une centaine tiendrait un discours séparatiste ne respectant pas les principes fondamentaux de la République que sont la liberté, l’égalité, la fraternité et la laïcité.

Dans le cadre de ses missions, le renseignement territorial peut proposer des mesures de police administrative, principalement aux préfets et au ministre de l’Intérieur. C’est ainsi que depuis l’entrée en vigueur de la loi SILT (2017), 7 lieux de culte ont été fermés à l’initiative du SCRT. Le service peut également proposer la dissolution d’une association, *****. Les mesures d’entrave peuvent aussi prendre la forme de mesures d’expulsion, d’interdiction administrative du territoire, de déchéance de la nationalité pour des binationaux², de gel d’avoirs financiers ou encore l’interdiction administrative d’acquisition et de détention d’armes.

Ces mesures peuvent se combiner les unes avec les autres. *****

L’action du renseignement territorial s’intègre dans le cadre plus large des **Cellules départementales de lutte contre l’islamisme et le repli communautaire** (CLIR) créées par la circulaire du 27 novembre 2019 et constituées dans tous les départements. Le renseignement territorial est ainsi amené à proposer des objectifs susceptibles de faire l’objet de mesures d’entrave diligentées par d’autres services de l’État et motivées par la violation de normes particulières (droit régissant les établissements recevant du public, les établissements scolaires hors contrat, droits fiscal ou social, ...).

Ces CLIR mobilisent ainsi l’ensemble des services départementaux, sous la présidence du préfet et en lien avec le procureur de la République ; les services de sécurité y participent (police, gendarmerie, renseignement territorial) et elles

¹ Audition le 15 janvier 2021 de Mme Lucille Rolland, cheffe du Service central du renseignement territorial, par la Commission spéciale chargée d’examiner le projet de loi confortant le respect des principes de la République.

² Sous certaines conditions strictement énoncées par les articles 25 et 25-1 du code civil.

associent également, selon les thématiques identifiées, des partenaires extérieurs (élus, bailleurs sociaux, opérateurs de transports, etc.), se coordonnent avec les Groupes d'Évaluation Départementaux (GED) et les Cellules de Prévention de la Radicalisation et pour l'Accompagnement des Familles (CPRAF). Les CLIR sont chargées d'établir un diagnostic de l'état de l'islamisme et du repli communautaire dans le département. Elles sont également le lieu de centralisation et de partage des informations confidentielles sur les phénomènes d'islamisme et de repli communautaire.

De janvier 2020 à mars 2021, 8 395 contrôles ont été réalisés dans le cadre des CLIR, 559 établissements accueillant du public ont été fermés et plus de 43 millions d'euros ont été redressés par les services fiscaux.

C. LA MENACE TERRORISTE ENDOGÈNE

Dans le contexte de l'affaire Merah (2012), qui avait mis en évidence la nécessité de renforcer les liens entre le renseignement territorial et le renseignement intérieur, le SCRT a acquis une compétence en matière de prévention du terrorisme sur la base du décret n° 2015-923 du 27 juillet 2015 modifiant le décret n° 2013-728 du 12 août 2013 portant organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer.

Au sein du SCRT, il existe ainsi une division exclusivement consacrée au traitement de la radicalisation et de la prévention du terrorisme. Elle est constituée de deux sections :

- La section « mesures de police administrative » qui propose, en concertation avec les SDRT, des mesures de police administrative (Fiches S, MICAS, IST, expulsions, IAT/TE, gels des avoirs, criblages régaliens, prêcheurs radicaux, fermeture des salles de prière) et en assure le suivi.
- La section « suivi des objectifs et des individus signalés », qui assure le suivi renforcé des cas individuels, notamment des individus inscrits au FSPRT, les dossiers d'objectifs (prévention du terrorisme), par département, par type de profils et comportements (notamment profession sensible, sorties de détention...).

Alors que la Direction générale de la sécurité intérieure (DGSI), service chef de file de la lutte antiterroriste, travaille sur « le haut du spectre » en suivant les « objectifs » nécessitant un niveau élevé de surveillance, ceux jugés moins dangereux, dits du « bas du spectre » sont suivis par le service central du renseignement territorial (SCRT) et, pour Paris et sa petite couronne (départements 92, 93 et 94), par la Direction du renseignement de la préfecture de Paris (DRPP). Ceci, dans le droit fil de la mission qu'exerçaient auparavant les RG qui suivaient les mouvements radicaux lorsque la DST travaillait sur les objectifs de contre-terrorisme d'État d'une part et l'ensemble des organisations terroristes d'inspiration étrangère d'autre part.

Bénéficiant du maillage tant des services territoriaux de sécurité publique que des unités de gendarmerie, le renseignement territorial, grâce à son réseau de proximité, doit jouer un rôle déterminant, notamment dans la détection des « signaux faibles » et contribue à ce titre à la mission de prévention du terrorisme. Au sein du SCRT, la détection de la radicalisation et la prévention du terrorisme font l'objet d'un dispositif complémentaire particulier : des antennes du renseignement territorial situées en zone gendarmerie sont ainsi composées de gendarmes, mais placées pour emploi sous l'autorité du chef du SDRT.

La détection de ces signaux faibles permettant de contrecarrer le passage à l'acte d'un individu isolé est un défi majeur pour le renseignement territorial dans le cadre de son concours à la lutte anti-terroriste. À ce titre, et compte tenu des profils des objectifs du renseignement territorial, le dialogue avec la médecine psychiatrique et la lutte contre les vecteurs de propagande constituent aujourd'hui des enjeux prioritaires. En effet, alors que les récents attentats commis en France ont pour la plupart du temps été le fait de personnes non connues des services de renseignement, la problématique est de plus en plus celle d'un suivi de masse d'individus plus ou moins imprégnés d'islam radical ou de propagande terroriste et présentant des troubles psychiatriques les rendant instables et particulièrement influençables.

La prévention de la menace terroriste et le suivi des phénomènes de radicalisation appellent également une coordination indispensable et qui s'est renforcée ces dernières années. Elle se déploie dans diverses enceintes, notamment les groupes d'évaluation départementale (GED), les CEPRAF et au niveau national, l'état-major permanent (EMaP) hébergé par la DGSI au titre de son rôle de chef de file de la lutte anti-terroriste.

II. LONGTEMPS CONSIDÉRÉ COMME LE PARENT PAUVRE DU RENSEIGNEMENT INTÉRIEUR, LE RENSEIGNEMENT TERRITORIAL RESTE EN CONSTRUCTION

Le renseignement intérieur a fait l'objet d'importantes réformes d'abord en 2008 puis en 2014. La disparition des renseignements généraux s'est accompagnée d'une crise de confiance et d'identité d'un renseignement de proximité qu'il a fallu réinventer.

Dans le contexte d'une menace terroriste persistante et diffuse, ces réformes ont profondément réinterrogé les modalités d'organisation des services de renseignement du ministère de l'Intérieur.

A. LES RÉFORMES DE 2008 ET 2014 ET L’AFFIRMATION PROGRESSIVE DU RENSEIGNEMENT TERRITORIAL

Le renseignement intérieur a fait l'objet d'un important mouvement de réforme, intervenu en deux temps : d'abord en 2008 avec la constitution de la DCRI – qui deviendra la DGSI – puis en 2014 avec la création du service central du renseignement territorial (SCRT).

Jusqu'en 2008, le renseignement intérieur était organisé en France autour de deux grandes directions :

- La direction de la surveillance du territoire (DST) chargée du contre-espionnage, de la lutte contre le terrorisme et de la défense du patrimoine industriel, économique et scientifique du pays.
- La direction centrale des renseignements généraux (DCRG), en charge du suivi des phénomènes sociaux et des mouvances extrémistes et reposant sur un maillage territorial fin.

Cette organisation a montré ses limites, conduisant la DST et les RG à se livrer une concurrence qui pouvait parfois conduire à une véritable guerre des polices. L'évolution de la menace terroriste a aussi progressivement rendu obsolète la pertinence de la répartition des rôles entre ces deux directions.

Dans un contexte politique marqué par la Révision Générale des Politiques Publiques (RGPP), le renseignement a ainsi été marqué par une première réforme en 2008 avec la création de la Direction centrale du renseignement intérieur (DCRI) qui a consisté à regrouper au sein d'une même direction les personnels de la DST et une partie substantielle de la direction centrale des renseignements généraux. Au terme de cette réforme, la nouvelle DCRI est devenue seule compétente en matière de lutte contre le terrorisme, dans le cadre de sa mission plus large consistant à « *lutter contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la Nation* ».

Cette même réforme de 2008 a confié à la Direction centrale de la sécurité publique (DCSP) une mission d'information générale avec la création en son sein d'une sous-direction de l'information générale (SDIG) qui reprend l'essentiel des missions des renseignements généraux. À la DCRI le renseignement principalement en milieu fermé ; à la SDIG le renseignement principalement en milieu ouvert.

À sa création, le SDIG compte 1 544 agents répartis sur l'ensemble du territoire national, dans le cadre d'un renseignement de proximité. La participation directe de la gendarmerie à cette mission d'information générale était prévue *via* le détachement par la gendarmerie d'un militaire au sein de chaque service départemental d'information générale.

Cette réforme de 2008, initialement présentée comme une fusion entre la DST et les renseignements généraux, s'est toutefois révélée être davantage une absorption – brutale – des RG, mal vécue par les agents concernés. Sans que cela ne soit jamais assumé, il s'agissait en quelque sorte d'effacer la culture RG. La SDIG disposait de peu de moyens.

Il s'en est suivi une crise d'identité et de reconnaissance du renseignement territorial qui a conduit à une nouvelle réforme, en 2014, avec la transformation du SDIG en un service central à part entière dédié au renseignement territorial. Cet échelon central a été distingué des autres sous-directions de la DCSP en devenant le Service central du renseignement territorial (SCRT) ; composé très majoritairement de policiers mais aussi de gendarmes. Pour le diriger, un second poste de directeur central adjoint de la sécurité publique, spécialement chargé du renseignement territorial, a été créé. La participation active de la gendarmerie à la mission de renseignement s'est traduite par la création, en décembre 2013, de la sous-direction de l'anticipation opérationnelle (SDAO) au sein de la direction générale de la gendarmerie nationale (DGGN). La SDAO, comme le SCRT, appartient au second cercle de la communauté du renseignement ; elle centralise, analyse en temps réel et anime toute la chaîne fonctionnelle chargée du recueil du renseignement dans la gendarmerie, en liaison étroite avec le SCRT qui relève pour sa part de la DGPN.

La DCRI fut pour sa part transformée en Direction générale de la sécurité intérieure (DGSI), service actif de la police nationale, mais directement rattaché au ministre et non plus dépendant de la DGPN, lui conférant une autonomie de recrutement et de fonctionnement. Ses missions sont fondées sur la défense de la souveraineté nationale, des intérêts fondamentaux de la Nation et de l'intégrité des institutions républicaines.

Le maillage territorial du SCRT

Le service central du renseignement territorial (SCRT) et ses services déconcentrés bénéficient du maillage territorial des directions départementales de la sécurité publique (DDSP) et des commissariats, au plus près des réalités du terrain. Des militaires de la gendarmerie nationale lui étant rattachés organiquement et fonctionnellement et des antennes du renseignement territorial ayant été mises en place dans des compagnies ou brigades territoriales, le « RT » bénéficie aussi de l'apport de la gendarmerie et de ses échelons territoriaux. Grâce à cet ancrage dans les territoires et au professionnalisme de ses agents, le renseignement territorial joue ainsi un rôle déterminant de surveillance, d'évaluation et de suivi des individus présentant des risques de radicalisation ou déjà radicalisés. Il contribue à ce titre à la mission de prévention du terrorisme.

Le SCRT dispose de 255 implantations territoriales réparties sur le territoire métropolitain et les départements et territoires d'outre-mer comme suit :

- 97 services « départementaux » (échelons zonal, régional ou départemental)
- 87 services du renseignement territorial (SRT – échelon infra-départemental)
- 63 antennes locales (ART) en zone gendarmerie
- 8 antennes aéroportuaires : *****

De cette réforme de 2014 est résultée une séparation plus stricte entre renseignement intérieur et renseignement de proximité, tout en établissant un *continuum* indispensable en matière de lutte contre le terrorisme.

B. LE SCRT, UN SERVICE « BAROQUE »

La réforme de 2014 a incontestablement corrigé les déséquilibres de celle de 2008, **sans pour autant parvenir à rationaliser totalement l'organisation administrative du renseignement de proximité.**

À ce titre, le service central du renseignement territorial demeure un service « baroque » selon le terme utilisé par sa directrice lors de son audition devant la délégation parlementaire au renseignement.

Sa compétence géographique reste en effet amputée de Paris et des départements de la petite couronne (92, 93 et 94) qui relèvent de la **Direction du renseignement de la préfecture de police de Paris (DRPP)**. La DRPP, ***** , exerce une pleine compétence dans le domaine du renseignement territorial à l'exception du suivi des dérives urbaines qui sont du seul ressort du SCRT. La DRPP concourt par ailleurs à l'activité de la DGSI pour la surveillance des individus, groupes, organisations et phénomènes de société susceptibles, par leur

caractère radical, leur inspiration ou leurs modes d'action, de porter atteinte à la sécurité nationale.

S'agissant de **l'articulation avec la SDAO**, la circulaire ministérielle du 21 mars 2014, créant le SCRT, insiste sur la nécessité de fournir aux autorités gouvernementales et à leurs représentants, **un renseignement unifié**. Cette mission incombe au SCRT tant au plan territorial que national. Intégrant des militaires de la gendarmerie, le SCRT exerce ses missions en lien direct avec la gendarmerie nationale et à son profit. Il agrège et consolide, dans ses notes, un renseignement unifié remontant des services de police et des unités de gendarmerie. Les notes portent le double timbre « Police nationale » et « Gendarmerie nationale ». Pour ce faire, il développe au niveau central une relation privilégiée avec la SDAO et, sur le terrain, par le truchement de ses services territoriaux, avec les échelons territoriaux de la chaîne renseignement de la gendarmerie (Bureau Renseignement, Cellule Renseignement). Concrètement, un bureau de liaison SDRT-GGD se réunit hebdomadairement pour échanger des informations, évoquer les priorités et besoins, les notes en cours de rédaction, répartir le travail et préparer certaines réunions. La complémentarité se fonde également sur le partage des productions entre le groupement de gendarmerie et le SDRT : la gendarmerie partage ses fiches de renseignement opérationnel avec le SDRT et le SDRT adresse au groupement de gendarmerie ses notes de renseignement. Les responsables départementaux des deux forces peuvent l'un comme l'autre exprimer des besoins et priorités. En revanche, seul le SDRT adresse ses notes de renseignement au préfet.

Se pose également la question de la **répartition de compétences avec les Directions départementales de la sécurité intérieure (DDSI)**. Celle-ci est thématique : les intérêts fondamentaux de la nation dont le terrorisme relève des DDSI. La prévention des troubles graves à l'ordre public relève du SCRT qui concourt également, sous pilotage DGSI, à la prévention du terrorisme. En matière de radicalisation religieuse ou de subversions violentes, si une dérive vers le terrorisme est détectée ou suspectée, la compétence DGSI s'impose.

C. UNE MONTÉE EN PUISSANCE RAPIDE DEPUIS 2014, ET QUI N'EST PAS ENCORE ACHEVÉE

Les augmentations d'effectifs réguliers et les créations de nouvelles antennes dans les territoires ont permis au SCRT de retrouver progressivement les moyens et le maillage dont disposaient les RG à l'aube de leur disparition.

1. Le renforcement des effectifs

À sa création en 2014, le Service Central du Renseignement Territorial (SCRT) comptait 1967 agents, soit davantage qu'en 2008 lors de constitution de la sous-direction de l'information générale, mais seulement 60 % des effectifs des anciens renseignements généraux.

Au cours de ses premières années d'existence, le SCRT et la DRPP ont bénéficié du renforcement de leurs effectifs dans le cadre du Plan de lutte contre le terrorisme. Le SCRT a ainsi pu compter sur 500 agents supplémentaires (350 policiers et 150 gendarmes), auxquels se sont ajoutés 130 policiers dans le cadre du Pacte de Sécurité du 16 novembre 2015.

Ces hausses d'effectifs ont permis de renforcer, aux différents échelons locaux du renseignement territorial, les capacités de surveillance, d'évaluation et de suivi des individus présentant des risques de radicalisation ou déjà radicalisés.

Elles se sont poursuivies avec un nouveau plan de renfort quinquennal 2017-2022 de 410 agents supplémentaires (policiers et gendarmes) mais dont la mise en œuvre a réellement débuté en 2019.

À l'issue de ce plan en cours de déploiement, les effectifs du SCRT devraient atteindre 3200 agents, dont 90 % affectés sur le terrain dans chacun des départements de l'hexagone, et en outre-mer. Avec 126 agents, c'est le département du Nord qui concentre le plus grand nombre d'agents, suivi de près par les Bouches-du-Rhône (117 agents). À l'opposé, c'est le département ***** qui compte l'effectif le plus réduit (9 agents).

*****.

Parmi les 3 103 agents du SCRT, 326 relèvent de la gendarmerie nationale, soit environ 10 %. Cette proportion est appelée à croître dans les années à venir pour se situer autour de 15 %, avec 420 gendarmes. En effet, le plan de recrutement 2018-2022 qui prévoit le renforcement des forces de sécurité intérieure à hauteur de 10 000 emplois sur la période, a induit la création de 27 équivalents temps plein (ETP) en gendarmerie nationale en 2020 afin d'accompagner la montée en puissance des activités de renseignement au sein de la gendarmerie nationale.

Le profil des agents du SCRT révèle une faible part de hauts gradés – à l'inverse de la DGSI – puisqu'on ne dénombre que 51 commissaires et 17 officiers de gendarmerie. Cette typologie des fonctions n'est pas sans conséquence sur le niveau de mobilité des agents.

Les actions de formation des agents du renseignement territorial

Depuis les réformes de 2008 et de 2014, des progrès significatifs ont été accomplis dans le domaine de la formation des agents du service central du renseignement territorial.

Il existe à ce jour trois grands domaines de formations pour les personnels affectés dans un service de renseignement territorial, qui ont bénéficié à 1 020 agents en 2019 et 730 en 2020, année perturbée en raison de la crise sanitaire.

Les formations proposées concernent :

Des stages d'intégration au RT, sorte de formation initiale pour les personnels qui viennent d'être affectés dans un service RT et qui regroupe 3 modules (acquisition des fondamentaux, conférences thématiques et sécurisation des déplacements officiels) – 563 personnels formés en 2019 et 409 en 2020.

*****.

Des stages thématiques, vus comme un approfondissement du métier d'agent de renseignement territorial et à destination soit des personnels actifs, soit des personnels administratifs. Il s'agit des stages « Appréhender le monde de l'entreprise sous l'angle RT », « RT et lutte contre la radicalisation : contexte, objectifs et méthodes » et du stage « Professionnalisation des personnels administratifs affectés en RT » – 90 personnels formés en 2019 et 40 en 2020.

Au-delà des modules de formation obligatoire existant, l'idée d'un « parcours de formation » pour les personnels du renseignement territorial est en cours de définition.

Ce parcours de formation pourrait s'articuler autour de trois axes :

Une formation « initiale » pour tout personnel affecté en SCRT revue et davantage axée sur les besoins pragmatiques liés à une prise immédiate de poste (connaissance de la matière du renseignement, connaissance des modalités de prise de contact, de rédaction et de structuration d'une note de renseignement...).

La révision des modules « thématiques » (autour des 3 grands thèmes du SCRT : Dérives urbaines, radicalisation et repli identitaire ; Économique et social et intelligence économique, et enfin, Mouvements contestataires subversifs et contestation sociétale) qui permettront pour un personnel du RT d'approfondir ses connaissances en fonction de la section thématique dans laquelle il est affecté, ou de préparer une mutation ou un changement de section.

L'objectif est de mieux cibler, par rapport aux choix évoqués supra, une adéquation entre le stagiaire et ses missions, d'une part en anticipant le développement de nouvelles compétences en lien avec une nouvelle mission de type changement de groupe ou de service, et d'autre part, en raccourcissant les délais entre affectation en RT et le départ en stage d'intégration.

Les formations extérieures au périmètre DCRFPN, qui sont amenées à se développer en raison de la technicité requise pour certaines missions du SCRT ***** , sur des thématiques soit très spécifiques, soit très pointues, et qui nécessitent d'une part de dégager un budget et d'autre part de cibler les stagiaires. Sur ce type de stage, la création de clause de fidélisation et/ou de rôle de référent national sont des pistes à réfléchir.

2. Le renforcement des moyens budgétaires

Les plans successifs de lutte contre le terrorisme et de renforcement des services de renseignement ont eu comme corollaire des besoins en matériels spécifiques ainsi qu'une augmentation continue des missions opérationnelles.

La montée en puissance du SCRT, *****, a conduit la direction centrale de la sécurité publique (DCSP) à financer les moyens nécessaires à ses activités dans le cadre du programme budgétaire 176 (Police nationale).

En crédits de paiement, les dépenses de fonctionnement du SCRT sont en augmentation constante. Sur la période 2018-2020, elles ont augmenté de 22 % passant de 966 576 euros en 2018, à 1 176 596 euros en 2019 et 1 179 691 euros en 2020 malgré une activité perturbée par la crise sanitaire et le premier confinement.

Les dépenses du SCRT concernent principalement les déplacements et l'équipement. Pour 2020, la répartition a été la suivante :

- Frais de transport et déplacements : 633 124 euros.
- Dépenses de carburant : 179 171 euros.
- Dépenses de péage : 59 745 euros.
- Achat divers mobiliers et matériels : 216 623 euros.

3. Le renforcement de la filière « recherche et appui »

Si environ 80 % de l'activité du renseignement territorial s'effectue en milieu ouvert, le SCRT a également recours aux techniques de renseignement et à des investigations en milieu fermé, qui mobilisent « recherche et appui ».

*****.

D. DES FRAGILITÉS PERSISTANTES

1. La difficulté à prioriser les missions

Le SCRT dépend de la Direction centrale de la sécurité publique (DCSP), une direction qui se caractérise par le périmètre très large de ses missions, le renseignement n'en étant qu'un volet parmi d'autres. Ainsi, le SCRT et ses services départementaux sont sollicités sur beaucoup d'autres sujets que le renseignement, liés au maintien de l'ordre public. Avec des effectifs parfois très réduits et l'existence de priorités spécifiques pour chaque territoire, il existe un risque de dispersion de l'action du SCRT.

À sa création en 2014, le SCRT est un service de renseignement d'ordre public. Mais dès 2015, lui sont rajoutées de nouvelles missions en matière de lutte anti-terroriste, de suivi de l'Islam de France et des phénomènes de radicalisation. La proportion des notes produites par le SCRT relatives à des questions d'ordre public reste d'environ 80 %.

Le SCRT remplit également deux missions annexes mais néanmoins particulièrement chronophages : les enquêtes administratives d'une part, et la participation à la sécurisation des déplacements officiels des membres du Gouvernement d'autre part.

À plusieurs reprises, le renseignement territorial a été pointé du doigt pour son manque d'anticipation. Sans pour autant que cette mise en cause ne soit forcément toujours étayée de façon objective.

Il est en ainsi des scènes de guérilla urbaine liées à la communauté tchéchène qui se sont déroulées dans un quartier de Dijon les 13 et 14 juin 2020, avec des tirs à l'arme lourde et de nombreux véhicules incendiés. Pourtant, dès les 12 juin 2020, le service du renseignement territorial du département de l'Aube produisait une note intitulée : « *Tchéchènes : appel à expédition punitive à Dijon* » après l'interception la veille, sur le réseau *Snapchat*, d'un message rédigé par un membre de la communauté tchéchène résidant dans la banlieue de Troyes et lançant un appel au rassemblement « pour les frères de Dijon et des alentours ». La préparation d'une action violente était détectée, et sa dangerosité correctement évaluée. En revanche, le renseignement territorial envisageait une action de la communauté tchéchène plus tardive alors qu'à l'évidence, les choses se sont précipitées. L'ensemble de la chaîne police a bien rendu compte au préfet concerné qui a décidé du dispositif de maintien de l'ordre à déployer. Pour le renseignement territorial, il apparaît toutefois qu'au-delà de la détection, il s'agit aussi de travailler sur l'exploitation des informations recueillies.

Quelques mois plus tard, lors de l'attentat commis contre Samuel Paty le 16 octobre 2020, le renseignement territorial est à nouveau mis en cause au vu du faisceau d'indices qui, a posteriori, aurait dû alerter les services de renseignement. Mais là encore, la situation est plus complexe. Le maire de Conflans-Saint-Honorine avait été alerté dès le 9 octobre par la Principale du collège des tensions observées dans l'établissement et de la menace qui pesait sur l'enseignant. L'édile a alors fait remonter cette crainte auprès du renseignement territorial qui, à son tour, a fait remonter aux autorités préfectorales le 12 octobre par une note évoquant « un incident en lien avec les principes de laïcité » et concluant, en dépit de la diffusion des vidéos qui ont animé les réseaux sociaux, sur « *aucune tension palpable majeure* » et sur le fait que « *la communication entre la direction et les familles avait permis d'apaiser les tensions* ». On sait a posteriori qu'il en a été différemment.

Comment expliquer cette erreur d'appréciation sur la réalité de la situation ? Auditionné par la Délégation, le directeur départemental du renseignement territorial a mis en avant le fait qu'en l'absence de compétence judiciaire du renseignement territorial (à la différence de la DGSI), son service n'a pas eu à connaître des informations liées aux plaintes déposées le 8 octobre par Brahim Chnina, le père d'une élève de la classe de M. Paty, pour « diffusion d'images pornographiques » et, ce même jour, par le professeur d'histoire-géographie, pour diffamation. En l'espèce, la judiciarisation a eu pour effet de préempter la capacité d'analyse du renseignement territorial, dès lors qu'il n'est pas possible de se prévaloir dans des notes d'analyse, d'informations contenues dans des procédures en cours. Or une même personne ne tiendra pas forcément les mêmes propos en renseignement et en judiciaire.

La note de renseignement du 12 octobre 2020 révèle une lecture très partielle de la situation qui n'est en réalité abordée que sous le seul prisme de l'ordre public, et en aucun cas de la menace terroriste. La semaine de l'attentat, le service départemental de renseignement territorial a produit 39 notes d'analyse et autant de notes Flash ; il a par ailleurs dû gérer quatre déplacements officiels et ses effectifs ont été mobilisés sur deux sujets d'importance : d'une part, la mobilisation d'agriculteurs qui voulaient bloquer l'accès à Paris et d'autre part, la fête des Loges dans le contexte de la crise sanitaire. En d'autres termes, l'arbitrage entre l'urgent et l'important est une difficulté majeure. L'affaire Paty aura montré à quel point il est nécessaire de pouvoir se détacher du flux quotidien pour consacrer des moyens humains à la mission spécialisée, en l'espèce la prévention d'un terrorisme endogène. Ceci nécessite de renforcer la mission de pilotage et de coordination des services départementaux afin de prioriser les missions.

Soumis à des contraintes multiples et devant s'adapter à un contexte extrêmement mouvant, le SCRT travaille davantage à partir d'indicateurs d'activité que de réels objectifs : volumétrie des notes produites, nombre de techniques de renseignement mises en œuvre, sources humaines traitées. Sur la base de ces indicateurs d'activité, l'appréciation qualitative du renseignement fourni par le service repose essentiellement sur l'évaluation qu'en font les « donneurs d'ordre ».

2. L'absence d'autonomie

À la différence de la DGSI, service de renseignement du premier cercle rattaché directement au ministre de l'Intérieur, le SCRT, comme la DRPP et la SDAO ne disposent pas d'une autonomie propre.

Le service central du renseignement territorial présente cette particularité d'être placé au sein de la Direction centrale de la sécurité publique (DCSP), sous la tutelle de la direction générale de la police nationale (DGPN), alors même qu'il compte dans ses effectifs un nombre significatif et croissant de gendarmes. Cette singularité présente à la fois des avantages et des inconvénients.

Il existe en effet une réelle plus-value pour le renseignement territorial à faire partie de la maison « sécurité publique » de la police et de la gendarmerie. Cela permet une proximité qui favorise la fluidité dans l'échange d'informations et facilite la mise en œuvre d'actions d'entrave, notamment judiciaire. Cette proximité avec les services de police n'est pas exclusive d'une relation riche avec la gendarmerie nationale qui joue pleinement son rôle de captation du renseignement. Ce renseignement issu de la gendarmerie est partagé avec le SCRT qui le fusionne et l'analyse à l'échelle nationale.

Néanmoins, le fait de ne pas disposer d'un statut autonome n'est pas sans poser de difficultés. Dans la gestion quotidienne du SCRT, ces difficultés sont de deux ordres :

- D'une part, l'absence de budget dédié, soclé et protégé. Les crédits alloués au SCRT émanent d'une direction centrale, la DCSP, qui ne dispose elle-même pas d'un budget propre. Ceci complique considérablement la planification du développement du service, crée un aléa au niveau de la ressource financière disponible et entraîne la mise en concurrence de projets du SCRT avec d'autres projets de la Police Nationale. Cette situation empêche également la définition d'une stratégie budgétaire pluriannuelle, tant en fonctionnement qu'en investissement.
- D'autre part, la complexité à déployer une politique de ressources humaines, en l'absence de pouvoir de nomination de la directrice du service.

Ces difficultés sous-tendent la réflexion sur l'organisation administrative du renseignement territorial et les effets induits par la coexistence de trois structures distinctes que sont le SCRT, la SDAO et la DRPP. Dans un rapport d'observation sur l'organisation du renseignement territorial, la Cour des comptes pose la question d'un service de renseignement territorial unifié entre les structures du second cercle. Une telle option peut sembler séduisante à première vue, car elle ferait œuvre de rationalisation. Pour autant, elle mérite d'être questionnée au vu de la spécificité du renseignement territorial qui se nourrit avant tout du terrain et d'une dimension humaine.

En créant un service unifié du renseignement territorial, il ne faudrait pas perdre cette capacité de capteurs sur l'ensemble du territoire national, en ne disposant plus de tous les moyens d'un maillage territorial dense. L'enjeu est de ne pas mettre à mal l'origine du renseignement.

3. Des freins techniques

Si le renseignement d'origine humaine reste largement prépondérant, tant la montée en puissance des contestations violentes que la mission confiée au SCRT en matière de lutte contre la menace terroriste endogène conduisent à recourir plus fréquemment aux techniques de renseignement et investigations en milieu fermé.

Le SCRT a accès aux techniques de renseignement suivantes :

- Balisage (BAL)
- Captation de données informatiques (CDI)
- Captation de données par dispositif de proximité (DDP)
- Données en temps réel (DTR)
- Interception par dispositif de proximité (IDP)
- Introduction dans un lieu privé (ILP)
- Interception de sécurité (ISO)
- Recueil de données informatiques (RDI)
- Sonorisation (SON)
- Vidéo surveillance (VDO)
- Données de connexions
- Géolocalisation en temps réel (GTR).

On constate une augmentation significative du recours aux TR au cours de la période récente *****.

Toutefois, le SCRT n'est aujourd'hui pas en mesure de mettre en œuvre la totalité des techniques de renseignement que la loi met à sa disposition. *****.

La filière « recherche et appui » ne dispose pas encore des outils et moyens techniques lui permettant de remplir pleinement ses missions. Elle n'a pas encore recruté tous les fonctionnaires qui devaient l'être. La DNRA cherche à maintenir son niveau d'effectif actuel sans parvenir à atteindre son effectif total. Quant aux GRA de création plus récente, l'effectif de 8 GRA n'est pas atteint avec d'importantes différences selon la date de création du GRA ; *****.

Plus globalement, le renseignement territorial souffre d'un niveau de dotation technique qui n'est pas ou plus en phase avec les exigences de ses missions. Ses agents disposent d'outils basiques pour réaliser leurs recherches numériques et certains n'ont même pas d'accès à l'internet grand public !

Le matériel technique est souvent obsolète et aucun plan pluriannuel d'investissement ne prévoit à ce jour son renouvellement complet.

Enfin, le SCRT ne dispose d'aucun système sécurisé de communication interne, ce qui constitue une entrave importante à la circulation d'une information protégée. *****. Il conviendrait aussi de renforcer la sécurité bâtementaire de ses

implantations territoriales du SCRT. En d'autres termes, dans bien des domaines, le renseignement territorial exerce ses missions du 21^e siècle avec des outils techniques du 20^e siècle.

4. Des prérogatives juridiques encore limitées

Les freins juridiques à l'action du renseignement territorial concernent tout à la fois l'accès à certaines techniques de renseignement, l'accès à certains fichiers et enfin l'accès à des informations de nature judiciaire.

a. Un accès aux techniques de renseignement limité à certaines finalités

S'il dispose d'un accès à un large éventail de techniques de renseignement, le SCRT n'a toutefois pas accès à l'ensemble d'entre elles, comme c'est le cas pour les services du premier cercle.

Le SCRT souhaiterait une modification de l'article R853-3 du CSI qui lui interdit de s'introduire dans un domicile au titre de la finalité 5c¹ de l'article L. 811-3 du CSI ; cette possibilité lui est en effet seulement possible au titre de la finalité 4, à savoir la prévention du terrorisme.

b. Un accès restreint aux fichiers de souveraineté

S'agissant de **l'accès aux fichiers de souveraineté**, le décret modificatif des fichiers du renseignement territorial, en date du 2 décembre 2020, a permis de clarifier les catégories de données à caractère personnel que le service est en droit de collecter au regard de la RGPD. De plus, en classant une partie de ces données comme relevant de la sûreté de l'État, le décret permet de restreindre en partie le droit d'accès des particuliers qui pouvait, dans certains cas, nuire au suivi effectué sur des personnes identifiées comme dangereuses.

Des freins existent toutefois quant à l'accès des agents à certains fichiers de renseignement. *****. Or si le partage de l'information est devenu la règle en matière de lutte antiterroriste, la coordination entre le renseignement territorial et la DGSJ est moins aboutie s'agissant du suivi des subversions violentes.

Au sein du SCRT, les capacités d'accès aux fichiers ne sont d'ailleurs pas les mêmes selon que l'agent de renseignement est issu de la police ou de la gendarmerie. Les militaires affectés dans les SDRT disposent en effet d'un accès au fichier de renseignement de la gendarmerie. Mais l'inverse n'étant pas vrai, il s'institue alors un droit tacite de préemption de l'information brute intégrée dans ce fichier par les gendarmes des unités territoriales. La production réalisée est alors absorbée et exploitée avec les services du renseignement territorial. L'action de la gendarmerie peut se trouver à la fois diluée et reléguée à celle de la simple captation au profit de partenaires extérieurs.

¹ La finalité 5c correspond aux violences collectives de nature à porter gravement atteinte à la paix publique

c. Le cloisonnement avec les informations de nature judiciaire

L'attentat commis contre Samuel Paty a révélé la difficulté que pouvait poser, pour un service de renseignement, le fait de **ne pas avoir accès à des informations de nature judiciaire**.

Le cumul au sein d'un même service d'une compétence en renseignement et d'une compétence judiciaire (sur le modèle de la DGSI) est une exception dans le monde du renseignement. Le renseignement est une activité éminemment régaliennne rattachée au pouvoir exécutif et ne peut s'accorder avec un contrôle de l'autorité qu'avec des règles de cloisonnement strictes telles celles mises en œuvre par la DGSI. Au demeurant, la compétence judiciaire de la DGSI est fondée sur des contentieux spécifiques donnant lieu à des échanges avec des juridictions spécialisées (lutte antiterroriste, compromission de secret).

Les infractions qui peuvent être mises en lumière par le SCRT sont essentiellement des infractions de droit commun, donnant lieu à des saisines des juridictions territorialement compétentes. À ce titre l'alternative consistant pour le SCRT à judiciariser son renseignement *via* des services judiciaires de police ou de gendarmerie reste la solution la plus pertinente.

Pour autant, il serait utile d'autoriser les services du second cercle à pouvoir demander la transmission d'informations judiciaires.

Des réflexions sont également menées sur certaines modifications réglementaires qui permettraient au SCRT d'accéder à différents systèmes de traitement de données pouvant intéresser ses investigations.

III. PLUTÔT QU'UNE NOUVELLE REFORME, LE RENSEIGNEMENT TERRITORIAL A SURTOUT BESOIN DE MOYENS OPÉRATIONNELS PLUS ADAPTÉS À L'EXERCICE DE SES MISSIONS

Plutôt qu'une nouvelle réforme de son organisation administrative, le renseignement territorial a surtout besoin de disposer des moyens de ses ambitions, dans une période où l'évolution des menaces lui confère un rôle stratégique.

Si la question d'un service unifié du renseignement territorial peut légitimement se poser, elle pourrait en l'état susciter davantage de difficultés que de solutions.

Il apparaît en revanche possible, sans remettre en cause les structures actuelles, de promouvoir une véritable filière du renseignement territorial autour de coopérations renforcées entre les services du second cercle.

Pour en finir avec une forme de nostalgie des renseignements généraux d'un côté, et le sentiment que le renseignement territorial serait pour toujours le parent pauvre du renseignement intérieur, la Délégation propose un plan d'action pour le renseignement territorial, autour de douze mesures concrètes.

1. Créer au sein du ministère de l'intérieur une direction générale réunissant le SCRT, la SDAO et la DRPP.

Trois entités distinctes concourent aujourd'hui au renseignement territorial : le SCRT, rattaché à la DGPN, la SDAO, rattachée à la DGGN et la DRPP qui exerce une compétence géographique sur le périmètre de Paris et sa petite couronne.

Sans remettre en question les spécificités de chacune de ces structures, il conviendrait néanmoins de les réunir au sein d'une seule et même direction générale du ministère de l'intérieur qui s'accompagnerait de la mutualisation des fonctions support de ces trois entités.

Les services du second cercle partagent en effet des problématiques similaires mais sans aucun pilotage commun, qu'il s'agisse des questions relatives aux ressources humaines, aux enjeux budgétaires, aux moyens techniques, etc.

La création de cette direction générale dédiée au renseignement territorial deviendrait le cadre d'un pilotage unifié et autonome du renseignement de proximité et le gage d'une reconnaissance de la fonction renseignement au sein du ministère de l'intérieur [*Recommandation n° 9*].

2. Doter le renseignement territorial de budgets opérationnels de programme « BOP » dédiés.

Trois services du second cercle concourent au renseignement territorial : le SCRT et la DRPP qui dépendent de la police nationale, et la SDAO qui dépend de la gendarmerie nationale. En cohérence avec la création d'une direction générale dédiée, il est proposé d'adosser le renseignement territorial à un BOP spécifique.

L'existence de deux programmes budgétaires distincts « Police nationale » (176) et « Gendarmerie nationale » (152) rend nécessaire la création de deux BOP distincts ; mais ceux-ci devraient faire l'objet d'un pilotage commun.

L'absence d'autonomie budgétaire est en effet un handicap majeur pour la fonction renseignement territorial dont les moyens budgétaires sont dépendants de deux programmes budgétaires séparés.

La création de BOP dédiés au renseignement territorial permettra au SCRT, à la DRPP et à la SDAO de disposer d'une sécurité budgétaire ainsi que d'indicateurs de pilotage et de performance [*Recommandation n° 10*].

3. Confier au renseignement territorial le chef de filât sur la prévention et le suivi des subversions violentes.

À l'instar de la DGSI dont le rôle de chef de file a été consacré en matière de lutte contre le terrorisme, le renseignement territorial devrait devenir chef de file s'agissant des subversions violentes.

Le renseignement territorial serait ainsi chargé du pilotage de l'analyse et de la synthèse afin de fournir un renseignement unifié sur les activités de ces mouvements [*Recommandation n° 11*].

4. Promouvoir la mobilité des agents.

Depuis fin 2019, le SCRT s'est doté d'une clé de répartition des effectifs employables pour les adapter à la charge d'activité des services territoriaux. Cette clé de répartition tient notamment compte d'un critère de population mais s'appuie également sur des données spécifiques au renseignement territorial (fréquence des visites officielles, évaluations, productions, manifestations, nombre de fiches créées, travail en milieu fermé, etc.). En mêlant ces données, il s'agit d'obtenir la vision la plus juste possible de la charge de travail de chaque service de renseignement territorial pour répartir de la façon la plus pertinente les effectifs. En effet, chaque territoire a ses spécificités et un traitement uniformisé de l'ensemble ne saurait les refléter, ce qui conduirait alors à une mauvaise répartition des effectifs, premiers acteurs du renseignement.

Alors que le SCRT indique ne pas disposer d'informations sur la durée moyenne d'affectation de ses personnels non soumis à une obligation de mobilité, cet outil devrait être utilisé pour mettre en place un plan incitatif de mobilité des agents. Pour la qualité du renseignement produit, la durée d'affectation dans un service ou sur un territoire ne doit en effet être ni trop courte (effet négatif d'un *turn over* trop fréquent) ni trop longue (effet routinier). La mobilité des agents devrait également être favorisée entre services de renseignement du second cercle [*Recommandation n° 12*].

5. Renforcer les compétences du renseignement territorial par un recrutement plus diversifié et des formations adaptées aux besoins des missions de renseignement.

Depuis la création du SCRT, des progrès ont été accomplis dans le domaine de la formation des personnels du renseignement territorial. Environ un millier d'agents bénéficient chaque année d'une action de formation (stage d'intégration, modules thématiques, formations techniques).

Il convient d'adapter en permanence cette offre de formation à l'évolution des menaces et des modes opératoires. À ce titre, un plan de formation linguistique (arabe, anglais, turc...) devrait être déployé à destination des agents du renseignement territorial qui sont en charge des sujets liés à la radicalisation et à la lutte contre le terrorisme. De même, des formations aux outils et aux usages numériques devraient être développées.

Un partenariat renforcé entre l'Académie du renseignement et les services du second cercle est également souhaitable afin de pourvoir à la formation d'analystes au sein de la filière « renseignement territorial » [*Recommandation n° 13*].

6. Faire du dialogue avec les élus des territoires un critère d'évaluation des cadres du renseignement territorial.

Par leurs contacts directs et permanents avec la population et les corps intermédiaires, les élus des territoires, en particulier les maires, sont des capteurs d'information qu'il serait dommage de négliger. Or force est de constater que, depuis la disparition des renseignements généraux, les liens se sont distendus entre le renseignement territorial et les élus.

Les maires ne sont ainsi jamais sollicités dans le cadre des GED et ne sont pas plus en retour informés de situations individuelles qui concernent leur territoire.

Il semble important de sensibiliser les élus des territoires aux enjeux du renseignement territorial pour en faire des capteurs actifs et utiles. Un kit d'information des maires pourrait utilement être élaboré et, sur le modèle des cellules de veille qui existent en matière de sécurité et de prévention de la délinquance, des réunions périodiques pourraient être organisées, dans le respect de la confidentialité des situations individuelles, sur les sujets qui intéressent le renseignement de proximité.

La réalité du dialogue avec les élus devrait faire partie des critères d'évaluation des cadres du renseignement territorial [*Recommandation n° 14*].

7. Doter le SCRT d'un réseau classifié sécurisé

Le partage de l'information est essentiel à la fonction renseignement. Or, à l'heure actuelle, le SCRT ne dispose d'aucun réseau sécurisé. Au-delà d'une seule messagerie, il s'agit de pouvoir transmettre et partager des informations en toute sécurité avec les 255 implantations territoriales du service, en métropole comme en outre-mer.

L'absence de réseau classifié sécurisé est aujourd'hui un vrai frein à la fluidité de l'information et la réactivité. La délégation recommande, comme l'envisagerait la DGSJ *****, que soit créé un réseau classifié commun à l'ensemble des services de renseignement, dont ceux concourant au renseignement intérieur [*Recommandation n° 15*].

8. Prévoir un plan pluriannuel de modernisation des matériels

Accès limité à internet, matériel informatique obsolète : les agents du renseignement territorial disposent souvent d'outils très basiques pour effectuer leurs investigations. Les services zonaux de recherche et d'appui (SZRA) possèdent seulement des équipements basiques ***** mais qui doivent être renouvelés au vu de leur obsolescence.

Un diagnostic du parc informatique existant, des matériels disponibles et des besoins du service devrait être réalisé dans le cadre d'un plan de renouvellement des matériels, adossé à un plan pluriannuel d'investissement.

Au vu de l'évolution des modes opératoires et de l'intensification des usages numériques, il apparaît également nécessaire de généraliser l'accès à l'internet grand public pour les agents du renseignement territorial. Un effort de dotation en matière d'internet grand public pour accéder à certaines applications et un accès à des applications de collecte automatisée serait le gage d'une plus grande efficacité [*Recommandation n° 16*].

9. Donner à la filière « recherche et appui » du SCRT les moyens humains et matériels de sa montée en puissance

La montée en puissance de la filière « recherche et appui » a pris du retard, le niveau d'effectifs annoncé n'ayant pas été atteint. Il est impératif de mener à son terme le plan de renforcement de la DNRA et des SZRA en procédant aux créations de postes prévues.

S'agissant des moyens en matériel, il convient de doter la direction nationale de recherche et d'appui des équipements techniques lui permettant de mettre en œuvre les techniques de renseignement que la loi met à disposition du SCRT.

Quant aux groupes de recherche et d'appui (GRA), il s'agit de les doter des matériels nécessaires pour couvrir leurs besoins, en particulier en termes de véhicules automobiles [*Recommandation n° 17*].

10. Autoriser l'accès du renseignement territorial aux techniques de renseignement pour la finalité 5c « subversions violentes »

La stratégie nationale du renseignement fait de la prévention des subversions violentes une mission du renseignement qui doit anticiper et prévenir. Or paradoxalement, le renseignement territorial est limité, pour cette finalité, dans son accès aux techniques de renseignement. En effet, la mise en place, l'utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1) et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu d'habitation lui sont possibles pour la seule finalité de prévention du terrorisme.

De même, la mise en place, l'utilisation ou le retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) ne sont également autorisées que pour la seule finalité de prévention du terrorisme.

Le recours à ces techniques devrait être élargi à la finalité 5c.

Plus globalement, la question de l'accès à certaines techniques de renseignement que la loi réserve au premier cercle doit être expertisée, à la fois sur la réalité du besoin, sur l'appréciation juridique et politique qui peut être portée sur ce vœu et sur la pertinence d'une évolution [*Recommandation n° 18*].

11. Autoriser l'accès du renseignement territorial aux informations judiciairisées

Parmi les enseignements tirés de l'attentat commis contre Samuel Paty on peut retenir que le cloisonnement de l'information entre les volets administratifs (renseignement) et judiciaire peut provoquer des angles morts en termes d'analyse des informations recueillies. Sans donner de compétence judiciaire au renseignement territorial, il faudrait néanmoins l'autoriser à accéder à des informations judiciairisées en lui permettant de les solliciter auprès des procureurs de la République [*Recommandation n° 19*].

12. Envisager la création d'un fichier commun dédié renseignement territorial (SCRT, SDAO et DRPP)

Les gendarmes affectés au sein des services départementaux du renseignement territorial disposent d'un accès au fichier de renseignement de la gendarmerie. Or, l'inverse n'étant pas vrai, s'institue alors un droit tacite de préemption de l'information brute intégrée dans ce fichier par les gendarmes des unités territoriales. La production réalisée est alors absorbée et exploitée avec les services du renseignement territorial. L'action de la gendarmerie s'en trouve à la fois diluée et reléguée à celle de la simple captation au profit de partenaires extérieurs.

Aussi, il conviendrait d'étudier la possibilité de créer un fichier commun dédié à l'ensemble des services de renseignement territorial (SCRT, SDAO et DRPP) avec des modalités d'accès et d'usage harmonisées. Ceci serait cohérent avec l'objectif fixé par le livre blanc sur la sécurité intérieure de septembre 2020 qui appelle à la production de synthèses analytiques consolidées et endossées par l'ensemble des services impliqués [*Recommandation n° 20*].

CHAPITRE V RAPPORT GÉNÉRAL DE LA CVFS

Conditions d'emploi des fonds spéciaux au cours de l'exercice 2019

Le contrôle de l'utilisation des fonds spéciaux a été confié par le législateur (loi de finances pour 2002) à la commission de vérification des fonds spéciaux (CVFS) dont la composition a été modifiée par la loi de programmation militaire du 18 décembre 2013 qui en fait une formation spécialisée de la délégation parlementaire au renseignement (DPR).

La CVFS, composée de deux députés et deux sénateurs membres de la DPR est chargée de « *s'assurer que les crédits [en fonds spéciaux] sont utilisés conformément à la destination qui leur a été assignée par la loi de finances* ».

Au mois de janvier 2020, sa composition était la suivante :

- M. Michel Boutant, sénateur (SER) de la Charente, président ;
- M. François-Noël Buffet, sénateur (LR) du Rhône ;
- M. Loïc Kervran, député (LREM) du Cher ;
- M. Patrice Verchère, député (LR) du Rhône.

À la suite des élections municipales de mars et juin 2020, puis des élections sénatoriales de septembre 2019, la CVFS a été profondément renouvelée. À compter du mois de novembre, la commission était composée comme suit :

- M. François-Noël Buffet, sénateur (LR) du Rhône, président ;
- M. Claude de Ganay, député (LR) du Loiret ;
- M. Loïc Kervran, député (LREM) du Cher ;
- M. Yannick Vaugrenard, sénateur (SER) de la Loire-Atlantique.

Pour mener sa mission et réaliser son rapport, la CVFS s'est déplacée au siège de chacune des structures bénéficiaires de fonds spéciaux pour y réaliser des contrôles sur place et sur pièces.

Elle s'est ainsi rendue :

- à la direction générale de la sécurité extérieure (DGSE), les 9 juillet, 12, 16, 26 et 30 octobre, 2 et 6 novembre, et 3 décembre 2020 ;

- à la direction générale de la sécurité intérieure (DGSI), les 25 et 26 juin, et 30 novembre 2020 ;
- à la direction du renseignement militaire (DRM), les 2 juillet, 9 et 16 octobre 2020 ;
- à la direction du renseignement et de la sécurité de la défense (DRSD), le 18 juin 2020 ;
- à la direction nationale du renseignement et des enquêtes douanières (DNRED), le 7 juillet 2020 ;
- à Tracfin, le 17 septembre 2020 ;
- au service national du renseignement pénitentiaire (SNRP), le 17 septembre 2020 ;
- au groupement interministériel de contrôle (GIC), les 17 septembre et 20 novembre 2020.

Au cours de ces visites, la commission a auditionné les principaux responsables des services et a systématiquement procédé à un contrôle par échantillon des pièces comptables.

En raison du contexte sanitaire, elle n'a pu, contrairement aux années précédentes, se déplacer auprès de postes à l'étranger pour y effectuer des contrôles.

I. PRÉSENTATION GÉNÉRALE DES FONDS SPÉCIAUX EN 2019

A. *****

Les services spécialisés de renseignement et le GIC ont disposé en 2019 d'un montant moins important de ressources en fonds spéciaux, en comparaison avec l'exercice précédent. **Le total s'élève à ***** , soit une baisse de près de 5,5 % par rapport à 2018.**

RESSOURCES EN FONDS SPÉCIAUX – ÉVOLUTION 2018/2019 (EN M€)

Tableau *****

Cette baisse globale de l'enveloppe de fonds spéciaux masque toutefois des **évolutions contrastées selon les services.**

Dans ses précédents rapports, la CVFS a souligné le **recours très important à des décrets pour dépenses accidentelles et imprévisibles (DDAI) et à des décrets de transfert** pour abonder en cours d'année les moyens alloués aux services.

Considérant que cette pratique pouvait s'apparenter à une atteinte à la sincérité de la prévision budgétaire, dès lors que lesdites dépenses étaient en réalité largement prévisibles, **elle recommandait d'effectuer un resoclage de la dotation initiale en fonds spéciaux** inscrite au programme 129 pour tenir compte des besoins réels et de l'évolution de l'activité opérationnelle des services (recommandation générale n° 18.01).

Cette pratique s'est toutefois sensiblement réduite au cours des deux derniers exercices. *****

Recommandation générale n°1 : Mettre un terme à la pratique de redéploiement entre services des dotations non consommées dans l'année, à titre d'avance sur l'exercice suivant.

B. *****

En 2019, le montant des fonds spéciaux dépensés dans l'année a connu une **baisse sensible** *****

Tableau *****

Là encore, cette évolution générale ne reflète qu'imparfaitement la situation des différents services. *****

De nombreux services ont en revanche vu leur trajectoire de dépenses continuer leur progression rapide, avec des hausses très marquées pour certains services, en proportion de leurs dépenses totales *****

Comme pour l'exercice précédent, **les dépenses en fonds spéciaux n'ont pas été intégralement couvertes par le montant de la dotation annuelle.** *****

Tableau *****

Compte tenu de ces évolutions, le niveau global de la trésorerie a diminué, *****

Une interrogation sur les modalités de présentation des informations budgétaires et comptables transmises à la CVFS

La CVFS n'a pas été en mesure, cette année, de procéder à une évaluation plus fine des dépenses réalisées en fonds spéciaux, en particulier s'agissant de la nature des dépenses.

Elle a en effet constaté des écarts importants entre les données consolidées qui lui ont été transmises par la CNRLT et celles qui lui ont été communiquées directement par les services bénéficiaires.

La commission a, en conséquence, fondé ses analyses sur les données communiquées par les services, consolidant elle-même les informations lorsque cela était possible. Elle regrette toutefois de n'avoir pu disposer d'une information fiable sur l'ensemble des données dont elle assure habituellement l'analyse, ce qui nuit à l'exercice de son contrôle.

Outre une différence de périmètre dans la comptabilisation des dépenses de la DGSE, la commission s'interroge sur le fait que certaines dépenses puissent être prises en compte deux fois dès lors que deux services interviennent dans le processus de règlement.

Elle invite en conséquence la CNRLT à examiner avec les services bénéficiaires les raisons des écarts constatés et à fiabiliser les informations qu'elle transmet chaque année à la CVFS concernant le montant des ressources en fonds spéciaux, le montant des dépenses annuelles ainsi que l'état de la trésorerie en fin d'année (**recommandation générale n° 2**).

II. OBSERVATIONS COMMUNES À L'ENSEMBLE DES SERVICES

L'examen des comptes en fonds spéciaux des services bénéficiaires permet à la CVFS de disposer d'une vision globale et transversale de la gestion des fonds spéciaux.

S'il existe des spécificités propres à chaque structure, il n'en demeure pas moins que des réflexions et des problématiques communes interpellent la commission.

A. LE PÉRIMÈTRE D'EMPLOI DES FONDS SPÉCIAUX

1. Des marges de manœuvre qui persistent pour la normalisation de certaines dépenses

a. La bascule progressive de certaines dépenses en fonds normaux

Conformément aux recommandations de la CVFS, la plupart des services bénéficiaires de fonds spéciaux se sont engagés dans un effort d'identification des dépenses susceptibles d'être basculées en fonds normaux, aux fins d'assurer un respect plus strict de la doctrine d'emploi des fonds spéciaux.

De nouvelles avancées ont pu être réalisées au cours de l'année 2019, tant par les services les plus consommateurs de fonds spéciaux ***** que par les services les plus petits*****.

Comme elle a déjà eu l'occasion de le rappeler, la CVFS admet que ce mouvement de bascule ne puisse être que progressif, compte tenu soit de la complexité des opérations que cela nécessite, soit du caractère historique de certaines dépenses dont la bascule implique d'attendre le renouvellement d'un contrat. *****

En dépit des avancées réalisées, **la CVFS observe qu'à défaut de définition d'une doctrine commune, des pratiques hétérogènes persistent entre les services, y compris pour des dépenses de même nature**. Il n'est bien entendu pas question, pour la commission, de demander un alignement complet des pratiques, chaque service conservant des besoins propres liés à la spécificité de ses missions et de ses modalités d'action.

Ceci étant, elle estime qu'un effort, si ce n'est d'harmonisation, du moins de rapprochement doit être conduit **par la diffusion, à l'ensemble de la communauté du renseignement, de bonnes pratiques mises en place par certains services**.

Recommandation générale n°3 : *****

b. *****

La CVFS a formulé des recommandations spécifiques invitant les services concernés à corriger leur pratique.

De manière plus générale, elle rappelle à destination de l'ensemble des services que l'usage des fonds spéciaux a vocation à demeurer résiduel et limité aux seules situations dans lesquelles aucune possibilité de prise en charge de fonds normaux n'existe. **Elle observe, à cet égard, que les entorses observées résultent parfois d'une méconnaissance du droit de la commande publique**, et notamment des possibilités de discrétion et/ou d'urgence qu'il offre pour certaines catégories de marchés de défense et de sécurité.

Elle **invite en conséquence la CNRLT à mettre en place un groupe de travail** en vue d'aider les services à étudier les possibilités de prise en charge en fonds normaux des achats de matériels ou d'équipements qui ne seraient pas justifiés par un besoin absolu de démarquage ou d'urgence (**recommandation générale n°4**).

c. Étudier les possibilités d'anonymisation dans l'application Chorus

Dans certains cas, l'usage des fonds spéciaux paraît justifié par un besoin de confidentialité non pas tant vis-à-vis de l'extérieur, mais plutôt à l'égard du reste de l'administration interne de l'État. Plusieurs services ont en effet indiqué à la commission recourir aux fonds spéciaux lorsque l'usage de fonds normaux impliquerait *****

2. *****

B. LE NECESSAIRE RENFORCEMENT DU CONTRÔLE INTERNE

Les fonds spéciaux bénéficient d'un régime juridique dérogatoire au regard du droit budgétaire commun (absence d'annualité budgétaire, pas de spécialisation des crédits).

En contrepartie, la CVFS estime indispensable que leur usage soit soumis à des règles strictes et précises ainsi qu'à un contrôle interne et externe approfondi.

Si les pratiques divergent d'un service à l'autre, **elle se félicite des progrès accomplis en la matière au cours des derniers exercices**, tant par les services historiquement les mieux dotés en fonds spéciaux que par les services qui n'en font qu'un usage restreint et récent.

Assez logiquement, **la structuration de l'environnement de contrôle interne ne saurait être identique d'un service à l'autre**. À cet égard, la commission estime nécessaire de distinguer les services les plus consommateurs en fonds spéciaux, ou ceux dont la dotation tend fortement à augmenter, des services pour lesquels les dépenses en fonds spéciaux ne représentent que quelques dizaines, voire quelques centaines de milliers d'euros.

Dans le premier cas, il importe qu'un dispositif de contrôle interne consolidé soit mis en place, comprenant, dans la mesure du possible, deux niveaux de contrôle. L'année 2019 a été marquée, à cet égard, par des évolutions importantes. *****

Dans les services ayant un usage des fonds spéciaux plus restreint, le renforcement de l'environnement de contrôle interne se traduit principalement par la mise en place d'une doctrine stricte d'usage des fonds spéciaux et d'un contrôle de régularité comptable *a posteriori*. Là aussi, la commission a pu constater des **progrès notables au cours de son contrôle**. *****

Ici ou là, la CVFS a néanmoins pu observer des fragilités qui confirment la nécessité de parfaire les réformes engagées. *****

La commission a formulé des recommandations spécifiques aux services concernés.

À moyen terme, **la CVFS suggère qu'un nouvel audit des dispositifs de contrôle interne soit confié à l'ISR, de manière à évaluer la pertinence des réformes conduites**.

C. L'ACCÈS DE LA CVFS À UNE INFORMATION FIABLE ET EXHAUSTIVE

La qualité du contrôle exercé par la CVFS dépend, très largement, de sa capacité à accéder à une information fiable et exhaustive.

À cet égard, la commission se félicite du souci croissant de transparence dont les services font preuve à son encontre à l'occasion de ses contrôles.

D. LE SUIVI DES RECOMMANDATIONS

Au début de l'exercice 2019, **16 recommandations générales émises en 2016, 2017 et 2018 restaient à mettre en œuvre** ou ne l'avaient été que partiellement.

Au terme de son contrôle, la CVFS n'a pu clôturer que trois de ces recommandations :

- la **recommandation générale n° 16.16** relative au renforcement des moyens de contrôle de la CVFS : la commission est progressivement

montée en puissance dans l'exercice de ses missions, augmentant le temps consacré à ses contrôles et élargissant le champ de ses actions (déplacements à l'étranger et en province). Elle a pu, ce faisant, accompagner les services dans le renforcement de leur dispositif de contrôle interne, ainsi que la sécurisation de certaines de leurs opérations, par exemple en matière de démarquage ;

- la **recommandation générale n° 16.13** qui visait à renforcer et formaliser les environnements de contrôle interne et à établir à l'attention de la CVFS une synthèse documentée sur les contrôles mis en œuvre et leurs résultats. La CVFS a été destinataire des notes établies par les services bénéficiaires de fonds spéciaux sur leur dispositif de contrôle interne. L'extinction de cette recommandation générale ne fait toutefois pas obstacle à ce qu'elle formule des préconisations spécifiques à l'égard de tel ou tel service ;
- la **recommandation générale n° 18.03 *******

Les autres recommandations demeurent en revanche ouvertes, soit parce qu'elles sont restées sans effet à ce jour, soit parce qu'elles étaient encore en cours de mise en œuvre en 2019 ou que la CVFS n'a pu constater par elle-même leur réalisation.

RECOMMANDATIONS GÉNÉRALES 2016, 2017 ET 2018 RESTANT OUVERTES

N°	Objet	Observations de la CVFS
16.02	Exclusion des fonds spéciaux de l'assiette de calcul de la réserve de précaution du programme 129.	La CVFS se félicite que la réserve de précaution du programme 129 ait systématiquement été levée s'agissant de l'enveloppe de fonds spéciaux. Pour autant, elle n'est pas explicitement exclue de l'assiette de calcul de la réserve. La CVFS maintient donc la recommandation, et restera attentive à l'évolution de la situation, particulièrement en période budgétaire contrainte.
16.05	*****	*****
16.07	Constituer un groupe de travail sur les possibilités de démarquage existantes dans le logiciel Chorus.	La CVFS maintient cette recommandation, aucun groupe de travail n'ayant été lancé sur le sujet. *****
16.09	Augmenter la dotation en fonds normaux à due proportion des montants transférés en fonds spéciaux.	***** La CVFS sera très attentive à la mise en œuvre de cette recommandation qui constitue une condition <i>sine qua non</i> au mouvement de déport vers les crédits ministériels.

N°	Objet	Observations de la CVFS
17.03	Définir des principes et des outils communs à l'ensemble des services spécialisés de renseignement s'agissant du contrôle interne de la gestion des sources : <i>turn over</i> régulier des agents, élaboration d'indicateurs au niveau central, séparation des fonctions de gestion et de contrôle, etc.	Les notes portant sur le contrôle interne transmises à la CVFS ne font pas toutes état des règles de gestion et de contrôle des sources humaines. ***** Elle maintient en conséquence sa recommandation.
17.04	*****	*****
17.05	*****	*****
18.01	Effectuer un « resoclage » de la dotation en fonds spéciaux inscrite au programme 129 pour tenir compte des besoins réels et de l'évolution de l'activité opérationnelle des services.	La CVFS salue l'effort de resoclage entrepris par les services du Premier ministre, *****
18.02	*****	*****
18.04	Désigner par arrêté ou une circulaire, non publié au <i>Journal officiel</i> , les entités et services susceptibles de bénéficier de fonds spéciaux. Cet arrêté ou circulaire, et les modifications apportées ultérieurement, serait communiqués sans délai à la CVFS.	La CVFS n'a été informée de la publication d'aucun arrêté ou circulaire en ce sens.
18.05	Réaffirmer la possibilité pour la CVFS d'accéder aux rapports d'inspection et d'audit interne nécessaires à sa pleine information et à l'exercice de son contrôle, par la diffusion d'une instruction aux services.	Plusieurs services ont infléchi leur position sur le sujet, ce qui devrait permettre à la commission d'avoir accès aux documents sollicités lors de son prochain contrôle annuel. La recommandation est néanmoins maintenue pour s'assurer de sa mise en œuvre.
18.06	Mettre en place, au sein de chaque service, des indicateurs *****	Aucune information n'a été communiquée à la CVFS en ce sens.
18.07	Mettre en place une cellule interservices *****	Aucune information n'a été communiquée à la CVFS en ce sens. *****

III. RECOMMANDATIONS GENERALES 2019 EMISES PAR LA CVFS

Recommandation générale n° 1 (à l'attention de la CNRLT) : Mettre un terme à la pratique de redéploiement entre services des dotations non consommées dans l'année, à titre d'avance sur l'exercice suivant.

Recommandation générale n° 2 (à l'attention de la CNRLT) : Remettre à plat, en collaboration avec les services bénéficiaires, les modalités de consolidation des données comptables et budgétaires relatives aux fonds spéciaux et fiabiliser les informations transmises à la CVFS concernant le montant des ressources et des dépenses annuelles, ainsi que le niveau global de la trésorerie en fin d'année.

Recommandation générale n° 3 : *****

Recommandation générale n° 4 (à l'attention de la CNRLT) : Mettre en place un groupe de travail transversal à l'ensemble des services bénéficiaires de fonds spéciaux sur les possibilités de discrétion et/ou d'urgence offertes par le droit de la commande publique.

RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU TITRE DE SON RAPPORT ANNUEL D'ACTIVITÉ 2020-2021

ÉVALUATION ET CONTRÔLE PARLEMENTAIRE DE LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

Recommandation n° 1 : Intégrer au rapport annuel d'activité des services spécialisés de renseignement et des services mentionnés à l'article L. 811-4 du code de la sécurité intérieure un chapitre consacré au suivi des recommandations formulées par la Délégation parlementaire au renseignement dans ses rapports annuels d'activité.

LUTTE CONTRE LE TERRORISME ET RENSEIGNEMENT PÉNITENTIAIRE

Recommandation n° 2 : Augmenter le nombre de places pour femmes en quartiers d'évaluation de la radicalisation (QER) et quartiers de prise en charge de la radicalisation (QPR) dans le cadre du programme immobilier pénitentiaire.

FICHIERS DE RENSEIGNEMENT

Recommandation n° 3 : Réaliser une évaluation du recours aux nouvelles possibilités de collectes dans les fichiers PASP, GIPASP et EASP permises par les décrets du 2 décembre 2020 et rendre la Délégation parlementaire au renseignement destinataire de cette évaluation.

SENSIBILISATION DE LA REPRÉSENTATION NATIONALE AUX RISQUES D'ESPIONNAGE

Recommandation n° 4 : À l'occasion de chaque renouvellement de l'Assemblée nationale et du Sénat, proposer systématiquement et obligatoirement à tous les parlementaires un temps de sensibilisation sur les risques d'espionnage liés à leur mandat ainsi qu'un kit d'information, intégré à la mallette du député et du sénateur, sur les bonnes pratiques à respecter.

ÉCHANGE D'INFORMATIONS AVEC LES SERVICES DE RENSEIGNEMENT ÉTRANGERS

Recommandation n° 5 : Au regard de la jurisprudence récente de la Cour européenne des droits de l'homme (Arrêt *Big Brother Watch et autres* du 25 mai 2021) sur l'échange d'informations avec des services de renseignements étrangers, engager avec la Délégation parlementaire au renseignement une réflexion sur la définition d'un mécanisme approprié d'encadrement de ces échanges.

CONTINUITÉ DES MISSIONS DE RENSEIGNEMENT PENDANT LA CRISE SANITAIRE

Recommandation n° 6 : Mettre en œuvre d'une capacité interservices d'anticipation et d'appréciation des menaces sanitaires, comme le préconise la revue stratégique de défense et de sécurité nationale de 2017.

Recommandation n° 7 : Établir un plan de continuité d'activité (PCA) prenant en compte l'ensemble des risques décrits par la revue stratégique de défense et de sécurité nationale de 2017. Ce PCA devra, entre autres, identifier les moyens informatiques et de communication nécessaires à la poursuite des missions jugées essentielles ou prioritaires, y compris à distance.

Recommandation n° 8 : Mettre en place un outil de visioconférence souverain et sécurisé, avec le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), permettant aux services de l'État, dont les services de renseignement, d'échanger des informations classifiées.

RENSEIGNEMENT TERRITORIAL

Recommandation n° 9 : Créer au sein du ministère de l'intérieur une direction générale réunissant le SCRT, la SDAO et la DRPP et permettant de mutualiser les fonctions supports de ces trois entités.

Recommandation n° 10 : Doter le renseignement territorial de budgets opérationnels de programme « BOP » dédiés

Recommandation n° 11 : Confier au renseignement territorial le chef de filât sur la prévention et le suivi des subversions violentes.

Recommandation n° 12 : Établir un indicateur permettant de connaître la durée d'affectation dans leur poste des agents du renseignement territorial et développer les incitations à la mobilité géographique et fonctionnelle des agents non soumis à une obligation statutaire de mobilité.

Recommandation n° 13 : Renforcer les compétences du renseignement territorial par un recrutement plus diversifié et des formations adaptées aux besoins des missions de renseignement, en particulier dans le domaine linguistique et en matière de connaissance et de suivi des usages numériques.

Recommandation n° 14 : Faire du dialogue avec les élus des territoires un critère d'évaluation des cadres du renseignement territorial.

Recommandation n° 15 : Doter le SCRT d'un réseau classifié sécurisé, permettant d'échanger des informations avec les 255 implantations territoriales du service.

Recommandation n° 16 : Prévoir un plan pluriannuel de modernisation des matériels.

Recommandation n° 17 : Donner à la filière « recherche et appui » du SCRT les moyens humains et matériels de sa montée en puissance.

Recommandation n° 18 : Autoriser l'accès du renseignement territorial aux techniques de renseignement pour la finalité 5c « subversions violentes ».

Recommandation n° 19 : Autoriser l'accès du renseignement territorial aux informations judiciairisées.

Recommandation n° 20 : Envisager la création d'un fichier commun dédié au renseignement territorial (SCRT, SDAO et DRPP).

EXAMEN PAR LA DÉLÉGATION

Réunis le jeudi 1^{er} juillet 2021 sous la présidence de Mme Françoise Dumas, la Délégation a procédé à l'examen de son rapport annuel.

Après un exposé de sa présidente, la Délégation a adopté son rapport pour 2020-2021 (chapitres I à IV), en application du VI de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958.

Par ailleurs, elle avait entendu le jeudi 28 janvier 2021 la présentation du rapport de la Commission de vérification des fonds spéciaux en application du VI de l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002 (chapitre V).
