

N° 5128

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale  
le 24 février 2022

N° 547

SÉNAT

SESSION ORDINAIRE DE 2021-2022

Enregistré à la présidence du Sénat  
le 24 février 2022

RAPPORT

FAIT

*au nom de la délégation parlementaire au renseignement*

*relatif à l'activité de la* **délégation parlementaire au renseignement pour l'année 2021-2022**

PAR

M. François-Noël BUFFET, Sénateur

Déposé sur le Bureau de l'Assemblée nationale  
par Mme Yaël BRAUN-PIVET,

*Première vice-présidente de la délégation*

Déposé sur le Bureau du Sénat  
par M. François-Noël BUFFET,

*Président de la délégation*



## SOMMAIRE

	<u>Pages</u>
<b>LISTE DES RECOMMANDATIONS.....</b>	<b>7</b>
<b>INTRODUCTION GÉNÉRALE .....</b>	<b>9</b>
<b>I. LA DÉLÉGATION S'EST FIXÉE DEUX PRINCIPAUX AXES DE TRAVAIL .....</b>	<b>10</b>
<b>II. LA DPR A ASSURÉ UN SUIVI DE L'ACTUALITÉ DU RENSEIGNEMENT, QUI A RÉVÉLÉ LA NÉCESSITÉ D'UNE CLARIFICATION JURIDIQUE DU CHAMP DE SON CONTRÔLE .....</b>	<b>13</b>
<b>A. LA DÉLÉGATION S'EST DOTÉE DE NOUVELLES PRÉROGATIVES .....</b>	<b>13</b>
1. <i>Les missions originelles de la DPR étaient très limitées...</i> .....	13
2. <i>...mais se sont progressivement étendues</i> .....	14
3. <i>Les apports de la loi de juillet 2021</i> .....	14
<b>B. L'ACTUALITÉ DU RENSEIGNEMENT A ÉTÉ MARQUÉE PAR DEUX AFFAIRES MÉDIATISÉES.....</b>	<b>15</b>
1. <i>L'affaire Pegasus</i> .....	15
a) <i>Une investigation qui s'annonce longue et complexe</i> .....	16
b) <i>*****</i> .....	16
c) <i>L'effet de surprise engendré par Pegasus sur les services français alerte la délégation sur la nécessité d'une réponse rapide des solutions souveraines de cybersécurité</i> .....	17
2. <i>L'affaire Sirli</i> .....	17
a) <i>Les faits dénoncés</i> .....	18
b) <i>Les problèmes soulevés</i> .....	18
c) <i>La délégation a souhaité user de la faculté offerte par la loi de juillet 2021 pour s'intéresser à l'affaire Sirli</i> .....	19
<b>C. UNE INTERPRÉTATION JURIDIQUE CONTESTABLE .....</b>	<b>20</b>
<b>CHAPITRE I: LA PRÉVENTION DE LA CRIMINALITÉ ET DE LA DÉLINQUANCE ORGANISÉES .....</b>	<b>23</b>
<b>I. LA LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE CONSTITUE UNE MISSION ESSENTIELLE DE CERTAINS SERVICES DE RENSEIGNEMENT .....</b>	<b>24</b>
<b>A. UN ENJEU ÉCONOMIQUE ET DE SOUVERAINETÉ FACE À LA MUTATION DES FORCES DE LA CRIMINALITÉ ORGANISÉE .....</b>	<b>26</b>
1. <i>Un périmètre en constante évolution qui impose la définition de priorités toujours sujettes à débat</i> .....	26
2. <i>L'implantation de l'écosystème criminel des drogues</i> .....	30
<b>B. LE RÔLE CENTRAL DU RENSEIGNEMENT DANS LA LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE .....</b>	<b>31</b>
1. <i>Une action adaptée au risque aboutissant à l'entrave et à la judiciarisation</i> .....	31
2. <i>L'importance des techniques de renseignement</i> .....	33

---

<b>II. UNE COORDINATION ET UNE STRUCTURATION À RENFORCER ENTRE SERVICES DE RENSEIGNEMENT DU PREMIER ET DU SECOND CERCLES .....</b>	<b>35</b>
<b>A. COORDONNER L’ACTION DE SERVICES AUX COMPÉTENCES COMPLÉMENTAIRES ET PARFOIS CONCURRENTES .....</b>	<b>35</b>
1. <i>Le pilotage de la lutte contre la criminalité organisée est confié à la police judiciaire...</i> .....	35
2. <i>...mais les moyens d’actions sont répartis entre différents offices centraux et services du second cercle...</i> .....	36
3. <i>...et nécessiteraient de mieux structurer le recours aux services de renseignement du premier cercle .....</i>	38
<b>B. ÉLEVER LE NIVEAU DE RÉPONSE FACE À UNE CRIMINALITÉ ORGANISÉE TOUJOURS PLUS TECHNIQUE ET INTERNATIONALE.....</b>	<b>38</b>
1. <i>Des enjeux techniques, dark web et cryptomonnaies .....</i>	39
2. <i>Des enjeux humains.....</i>	39
<b>CHAPITRE II : L’ENCADREMENT DES ÉCHANGES ENTRE LES SERVICES DE RENSEIGNEMENT FRANÇAIS ET LEURS HOMOLOGUES ÉTRANGERS.....</b>	<b>43</b>
<b>I. LES AJUSTEMENTS OPÉRÉS PAR LE ROYAUME-UNI APRÈS L’ARRÊT DE LA CEDH .....</b>	<b>44</b>
<b>II. LE CADRE LÉGISLATIF EN VIGUEUR EN ALLEMAGNE EN MATIÈRE D’ÉCHANGE D’INFORMATIONS .....</b>	<b>47</b>
<b>A. LA CONSTITUTION DE FICHIERS COMMUNS.....</b>	<b>47</b>
<b>B. LA TRANSMISSION D’INFORMATIONS.....</b>	<b>48</b>
<b>CHAPITRE III : L’ACTIVITÉ DES SERVICES DE RENSEIGNEMENT EN 2020 ET EN 2021.....</b>	<b>53</b>
<b>I. LES ENJEUX D’ACTUALITÉ LIÉS A LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT .....</b>	<b>53</b>
<b>A. LES CONSÉQUENCES DE LA CRISE SANITAIRE SUR L’ACTIVITÉ DES SERVICES DE RENSEIGNEMENT .....</b>	<b>53</b>
<b>B. LES MENACES PRÉPONDÉRANTES DEPUIS 2020.....</b>	<b>54</b>
1. <i>La lutte antiterroriste .....</i>	54
2. <i>Les ingérences étrangères.....</i>	54
3. <i>Les menaces hybrides .....</i>	55
4. <i>Les sujets d’intérêt de l’année 2021.....</i>	55
<b>C. LE DÉVELOPPEMENT DE NOMBREUX LEVIERS DE COOPÉRATION AU SEIN DE LA COMMUNAUTÉ DU RENSEIGNEMENT.....</b>	<b>55</b>
<b>D. LA PRISE EN COMPTE DE LA DIMENSION EUROPÉENNE DE L’ACTIVITÉ DE RENSEIGNEMENT, EN AMONT DE LA PRÉSIDENTE FRANÇAISE DE L’UNION EUROPÉENNE.....</b>	<b>56</b>
<b>II. LE BILAN STATISTIQUE DE L’ACTIVITÉ DES SERVICES DE RENSEIGNEMENT AU COURS DE L’ANNEE 2020 .....</b>	<b>57</b>
<b>A. LES DONNÉES RELATIVES À L’AIDE À LA DÉCISION .....</b>	<b>57</b>

B. LES DONNÉES RELATIVES À LA PRÉVENTION ET À LA RÉDUCTION DES VULNÉRABILITÉS .....	59
C. LES DONNÉES RELATIVES À L'ENTRAVE ET LA NEUTRALISATION DES MENACES.....	60
<b>III. LE HAUT NIVEAU DE RESSOURCES ACCORDÉES AUX SERVICES DE RENSEIGNEMENT CONFIRME LA PRIORITÉ DONNÉE A LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT .....</b>	<b>61</b>
A. DES RESSOURCES BUDGÉTAIRES QUI SE STABILISENT À UN NIVEAU ÉLEVÉ ..61	
1. <i>Les crédits en fonds normaux</i> .....	61
2. <i>Les crédits en fonds spéciaux</i> .....	61
B. LA MISE EN ŒUVRE PROGRESSIVE D'UNE POLITIQUE DE RESSOURCES HUMAINES CONSACRÉE À LA FILIÈRE DU RENSEIGNEMENT.....	62
C. UN RECOURS AUX RESSOURCES TECHNIQUES À INTERPRÉTER À LA LUMIÈRE DE LA CRISE SANITAIRE .....	63
<b>CHAPITRE IV : LE RAPPORT GÉNÉRAL DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX SUR L'EXERCICE 2020.....</b>	<b>67</b>
<b>I. PRESENTATION GENERALE DES FONDS SPECIAUX EN 2020.....</b>	<b>68</b>
A. DES RESSOURCES STABLES.....	68
B. UNE REDUCTION DES DEPENSES DANS UN CONTEXTE DE CRISE SANITAIRE ..69	
C. LA NATURE DES DEPENSES.....	70
<b>II. LES OBSERVATIONS COMMUNES A L'ENSEMBLE DES SERVICES.....</b>	<b>70</b>
A. LA PERSISTANCE D'ENTORSES A LA DOCTRINE D'EMPLOI DES FONDS SPECIAUX.....	70
B. DES OBSTACLES A L'EXIGENCE DE DEMARQUAGE ET D'ANONYMISATION ....71	
C. LA NECESSITE D'INVENTORIER LES MATERIELS ACQUIS EN FONDS SPECIAUX.....	72
D. METTRE FIN AUX ANGLES MORTS DU CONTRÔLE DE LA CVFS .....	72
E. POURSUIVRE LE MOUVEMENT DE BASCULEMENT DE FONDS SPÉCIAUX EN FONDS NORMAUX .....	72
F. HARMONISER LES DONNEES COMPTABLES ET BUDGETAIRES TRANSMISES A LA CVFS .....	73
<b>III. LE SUIVI DES RECOMMANDATIONS DE 2019.....</b>	<b>73</b>
<b>ANNEXE : REPRISE DES RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT AU 30 SEPTEMBRE 2022.....</b>	<b>79</b>



## LISTE DES RECOMMANDATIONS

### RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

#### Sur la prévention de la criminalité et de la délinquance organisées :

**Recommandation n° 1 :** Accentuer la lutte contre la fraude à la TVA.

**Recommandation n° 2 :** Augmenter les moyens humains de la DNRED en matière de lutte contre les stupéfiants dans les ports.

**Recommandation n° 3 :** Accompagner la croissance de Tracfin afin de permettre un développement de ses compétences et une diffusion de son expertise en matière de blanchiment.

**Recommandation n° 4 :** \*\*\*\*\*.

**Recommandation n° 5 :** Faire évoluer le régime applicable aux repentis \*\*\*\*\*.

**Recommandation n° 6 :** Renforcer la fluidité du recours des offices, en tant que chefs de file dans leur domaine de compétence respectif, aux services de renseignement spécialisés du premier cercle.

**Recommandation n° 7 :** Améliorer le recrutement et le traitement des sources humaines, en assurant la transmission des connaissances des agents recruteurs.

**Recommandation n° 8 :** Élever le niveau de priorité de la lutte contre la criminalité organisée dans le renseignement fourni par les services du premier cercle, dans le respect de leurs compétences.

**Recommandation n° 9 :** Renforcer les moyens de lutte cyber face au développement des nouveaux modes d'action de la criminalité organisée.

**Recommandation n° 10 :** Développer les mesures de prévention de la corruption des agents et des autorités publiques.

**RECOMMANDATIONS GÉNÉRALES DE LA  
COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX**

**Recommandation générale n° 1 (à l'attention de la CNRLT) :** Au vu de pratiques différentes d'un service à l'autre, s'assurer de la cohérence et du bien-fondé du recours aux fonds spéciaux pour l'acquisition de logiciels.

**Recommandation générale n° 2 :** En lien avec la CNRLT, établir dans chaque service une procédure interne permettant de caractériser l'urgence opérationnelle sur la base d'éléments factuels (date de la demande, délais de procédure, etc.).

**Recommandation générale n° 3 (à l'attention de la CNRLT) :** Constituer un groupe de travail interservices chargé de \*\*\*\*\*.

**Recommandation générale n° 4 :** Mettre en œuvre, dans chaque service, un inventaire des matériels acquis en fonds spéciaux, \*\*\*\*\*.

**Recommandation générale n° 5 :** Accompagner le processus en cours de basculement de fonds spéciaux vers les fonds normaux d'une revalorisation à due proportion des crédits budgétaires alloués aux services et structures concernés.

**Recommandation générale n° 6 (à l'attention de la CNRLT) :** Harmoniser les pratiques et les périmètres comptables afin de pouvoir disposer de données consolidées et comparables d'un exercice à l'autre et fournir à la CVFS les raisons des écarts constatés.



## INTRODUCTION GÉNÉRALE

Depuis sa création en 2007, la délégation parlementaire au renseignement (DPR) a consacré une large partie de ses travaux à la prévention contre le terrorisme, eu égard à l'actualité, qu'il s'agisse des attentats perpétrés sur le territoire national depuis 2015 ou des menaces pesant sur nos intérêts, y compris à l'étranger. Néanmoins, la DPR a toujours eu le souci d'investir d'autres champs du renseignement tels que la défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France, le renseignement territorial, le renseignement pénitentiaire, le renseignement d'intérêt militaire, la cyberdéfense, la surveillance des communications électroniques internationales, etc.

Jusqu'à présent, la délégation ne s'était pas véritablement penchée sur la prévention de la criminalité et de la délinquance organisées alors que, d'une part, cette finalité est l'une des plus invoquées à l'appui des demandes de techniques de renseignement formulées par les services, et d'autre part, certaines organisations criminelles transnationales menacent les intérêts fondamentaux de certains de nos voisins européens, et même leurs institutions.

### LES FINALITÉS FONDANT LES DEMANDES DE TECHNIQUES DE RENSEIGNEMENT

Finalités	Part en 2020	Part en 2019
Prévention du terrorisme ( <i>finalité 4</i> )	46,3 %	38 %
Intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ( <i>finalité 2</i> )	16,5 %	15 %
<b>Prévention de la criminalité et de la délinquance organisées (<i>finalité 6</i>)</b>	<b>14,4 %</b>	<b>19 %</b>
Prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique ( <i>finalité 5</i> )	14,2 %	14 %
Intérêts économiques, industriels et scientifiques majeurs de la France ( <i>finalité 3</i> )	5,0 %	11 %
Indépendance nationale, l'intégrité du territoire et la défense nationale ( <i>finalité 1</i> )	2,3 %	2 %
Prévention de la prolifération des armes de destruction massive ( <i>finalité 7</i> )	1,2 %	1 %

Source : Commission nationale de contrôle des techniques de renseignement (CNCTR).

## I. LA DÉLÉGATION S'EST FIXÉE DEUX PRINCIPAUX AXES DE TRAVAIL

Au cours de l'année 2021-2022, la délégation parlementaire au renseignement (DPR) était ainsi composée :

***pour le Sénat :***

- M. François-Noël Buffet, sénateur Les Républicains, **président de la délégation**, président de la commission des lois,

- M. Christian Cambon, sénateur Les Républicains, président de la commission des affaires étrangères, de la défense et des forces armées,

- Mme Agnès Canayer, sénateur Les Républicains, désignée par le président du Sénat,

- M. Yannick Vaugrenard, sénateur Socialiste, Écologiste et Républicain, **vice-président de la délégation**, désigné par le président du Sénat ;

***pour l'Assemblée nationale :***

- Mme Yaël Braun-Pivet, députée La République en Marche, **première vice-présidente de la délégation**, présidente de la commission des lois,

- Mme Françoise Dumas, députée La République en Marche, présidente de la commission de la défense nationale et des forces armées,

- M. Claude de Ganay, député Les Républicains, désigné par le président de l'Assemblée nationale,

- M. Loïc Kervran, député Agir ensemble, désigné par le président de l'Assemblée nationale.

*La composition est restée inchangée depuis les dernières élections sénatoriales ; seul le bureau de la délégation a été renouvelé en juillet 2021.*

Ce contexte a incité le président de la délégation, le sénateur François-Noël Buffet, président de la commission des lois du Sénat, à proposer la « prévention de la criminalité et de la délinquance organisées » comme axe principal de travail pour l'année en cours.

Par ailleurs, lors de l'examen du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement<sup>1</sup>, la commission des lois du Sénat avait rejeté les amendements tendant à l'encadrement des échanges entre les services de renseignement français et leurs homologues étrangers, au regard notamment des décisions de la Cour européenne des droits de l'homme relatives aux législations britannique et suédoise. Le président Buffet s'était alors engagé à confier à la DPR une étude sur le sujet qui, partant, a constitué le second axe de travail de la délégation.

---

<sup>1</sup> Promulguée en juillet 2021.

Ces travaux ont été conduits au travers d'auditions au Sénat ou au siège des différents services (DGSE, DNRED, Tracfin, SIAT), et de déplacements effectués dans deux villes de France (Le Havre, Marseille). La DPR a ainsi entendu la plupart des directeurs des services du premier cercle de la communauté du renseignement (DGSE, DGSI, DNRED, Tracfin), mais également celles de la Direction du renseignement de la préfecture de police de Paris (DRPP) et du Service national du renseignement pénitentiaire (SNRP), ainsi que le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), à plusieurs reprises, et le directeur central de la police judiciaire (DCPJ).

À cela s'ajoutent naturellement les travaux conduits par la commission de vérification des fonds spéciaux (CVFS), présidée depuis janvier 2021 par M. Loïc Kervran, député, assurés par quatre membres de la délégation (deux sénateurs et deux députés) et dont la synthèse constitue le dernier chapitre du présent rapport. La DPR a entendu le rapport du président de la CVFS le 24 février 2022.

Enfin, comme chaque année, la délégation a accueilli les auditeurs du cycle supérieur de l'académie du renseignement au cours d'une session organisée le 7 octobre 2021 au Sénat.

#### **Calendrier des réunions plénières de la délégation parlementaire au renseignement de juillet 2021 à mai 2022**

##### **Réunion du 27 juillet 2021 :**

audition conjointe de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), et de M. Nicolas Lerner, directeur général de la sécurité intérieure (DGSI).

##### **Réunion du 30 septembre 2021 :**

- audition de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) ;
- audition de Mme Françoise Bilancini, directrice du renseignement de la préfecture de police (DRPP).

##### **Réunion du 4 novembre 2021 :**

- audition de M. Jérôme Bonet, directeur central de la police judiciaire (DCPJ) ;
- table ronde consacrée aux offices :
  - \* Mme Stéphanie Cherbonnier, cheffe de l'Office anti-stupéfiants (Ofast),
  - \* M. Frédéric Malon, sous-directeur de la lutte contre la criminalité organisée, représentant l'Office central pour la répression de la traite des êtres humains (OCRTEH),
  - \* M. Guillaume Maniglier, adjoint au chef de l'Office central de lutte contre le crime organisé (OCLCO),
  - \* Mme Cécile Augeraud, cheffe de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC),
  - \* Général Marc de Tarlé, commandant de l'Office central de lutte contre la délinquance itinérante (OCLDI) ;
- audition de M. Thierry Matta, directeur du renseignement et des opérations, adjoint au directeur général de la sécurité intérieure (DGSI).

**Déplacement au siège de la Direction nationale du renseignement et des enquêtes douanières (DNRED) du 18 novembre 2021 :**

audition de M. Florian Colas, directeur, et de plusieurs cadres de son service.

**Déplacement au siège de la Direction générale de la sécurité extérieure (DGSE) du 2 décembre 2021 :**

audition de M. Bernard Émié, directeur général, et de plusieurs cadres de son service.

**Déplacement au Service interministériel d'assistance technique (SIAT) du 9 décembre 2021 :**

audition de M. Frédéric Veaux, directeur général de la police nationale (DGPN), et de plusieurs cadres de sa direction générale.

**Déplacement au siège de Tracfin du 6 janvier 2022 :**

audition de Mme Manon Perrière, directrice par intérim, et de plusieurs cadres de son service.

**Déplacement au port du Havre du 20 janvier 2022 :**

- audition conjointe de Mme Vanina Nicoli, sous-préfète du Havre, et de M. Stéphane Raison, directeur général de Haropa Port ;
- audition des services douaniers et de police judiciaire.

**Réunion du 10 février 2022 :**

audition de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

**Réunion de travail du 24 février 2022 :**

- présentation du rapport de la commission de vérification des fonds spéciaux (CVFS) sur les comptes de l'exercice 2020 ;
- examen et adoption du rapport annuel.

**Réunion du 30 mars 2022 :**

- audition du Général Vincent Cousin, secrétaire général adjoint de la défense et de la sécurité nationale (SGDSN), de M. Guillaume Poupard, directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI) et de M. Gabriel Ferriol, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

- audition de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

**Réunion du 10 mai 2022 :**

audition conjointe du Général Thierry Burkhard, chef d'état-major des armées, et de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

**Déplacement à Marseille du 20 mai 2022 :**

- audition de Mme Charlotte Hemmerdinger, sous-directrice, cheffe du Service national du renseignement pénitentiaire (SNRP), et de plusieurs cadres de son service ;
- visite du centre pénitentiaire de Marseille « Les Baumettes 2 » ;
- audition de Mme Frédérique Camilleri, préfète de police des Bouches-du-Rhône, et de cadres des services départementaux (renseignement territorial, police judiciaire, douanes, sécurité publique, gendarmerie).

**Réunion du 8 juin 2022 :**

audition de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

## **II. LA DPR A ASSURÉ UN SUIVI DE L'ACTUALITÉ DU RENSEIGNEMENT, QUI A RÉVÉLÉ LA NÉCESSITÉ D'UNE CLARIFICATION JURIDIQUE DU CHAMP DE SON CONTRÔLE**

### **A. LA DÉLÉGATION S'EST DOTÉE DE NOUVELLES PRÉROGATIVES**

#### **1. Les missions originelles de la DPR étaient très limitées...**

Créée par la loi n° 2007-1443 du 9 octobre 2007, la délégation parlementaire au renseignement (DPR) avait, à l'origine, pour seule mission « *de suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget* ».

Aux termes de la loi, la délégation était dépourvue de pouvoir de contrôle, son rôle étant circonscrit au suivi des services de renseignement (activité générale, organisation, budget et moyens). Elle ne pouvait solliciter la communication de documents ou d'éléments d'information qui semblaient utiles à l'exercice de sa mission ; les informations qui lui étaient transmises étaient d'ordre très général, et laissées à la discrétion des ministres dont relevaient lesdits services – en l'espèce, les ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget.

Le rapporteur pour le Sénat du projet de loi précité, M. René Garrec, soulignait à cet égard que « *si une affaire du type du "Rainbow warrior" survenait demain, la délégation parlementaire pour le renseignement ne serait par conséquent pas compétente. Les commissions permanentes ou une commission d'enquête pourraient en connaître mais dans la limite de leurs pouvoirs.* »<sup>1</sup>

Enfin, la liste des personnes pouvant être auditionnées par la délégation était limitativement définie. Ainsi, seuls le Premier ministre, les ministres compétents, le secrétaire général de la défense et de la sécurité nationale (SGDSN) et les directeurs en fonction des services de renseignement, pouvaient être entendus. Dès lors, la DPR ne disposait que d'un nombre très restreint d'interlocuteurs.

---

<sup>1</sup> Rapport n° 337 (2006-2007) de M. René Garrec, fait au nom de la commission des lois du Sénat, sur le projet de loi portant création d'une délégation parlementaire au renseignement.

## 2. ...mais se sont progressivement étendues

La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, a sensiblement étendu les prérogatives de la délégation. La France était jusqu'alors l'une des dernières démocraties occidentales à ne pas être dotée d'un organe parlementaire *ad hoc* dédié au contrôle des services de renseignement.

Cette loi a ainsi mis en place un contrôle parlementaire destiné notamment à évaluer la politique publique de renseignement, permis une meilleure information de la délégation, étendu la liste des personnalités pouvant être entendues et acté l'absorption de la CVFS par la DPR.

En définissant la politique publique de renseignement, la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a, quant à elle, permis de mieux préciser le champ d'évaluation de la délégation parlementaire au renseignement, d'étendre une nouvelle fois la liste des personnes pouvant être auditionnées et d'augmenter son pouvoir d'information.

## 3. Les apports de la loi de juillet 2021

Les deux lois susmentionnées avaient accru les moyens, tant humains que financiers, des services de renseignement ; le renforcement de leur contrôle démocratique apparaissait donc nécessaire pour trouver un juste équilibre.

La loi de juillet 2021 a permis d'accroître les moyens juridiques mis à la disposition des services de renseignement. Ainsi, suivant la même logique, il paraissait naturel de renforcer les pouvoirs de la DPR, au regard des lacunes qu'elle avait mises en lumière dans ses derniers rapports. Ainsi, l'article 21 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a, entre autres, complété les missions de la délégation en prévoyant qu'elle « *assure un suivi des enjeux d'actualité [en matière de renseignement] et des défis à venir qui s'y rapportent* ».

L'objet de l'amendement adopté par la commission des lois de l'Assemblée nationale était d'élargir « *le champ d'action de la DPR en lui reconnaissant explicitement la possibilité de traiter des enjeux d'actualité liés au renseignement. Il s'agit, sans interférer sur les opérations en cours, de souligner l'intérêt pour la DPR de mener des travaux en prise avec l'actualité, en usant de droit d'accès à des informations classifiées, ce qui n'est permis à aucun autre organe parlementaire.* »

Lors de la discussion générale du texte à l'Assemblée nationale, le 1<sup>er</sup> juin 2021, le ministre de l'intérieur, M. Gérard Darmanin, avait déclaré que : « *le renseignement [...], apanage des grandes démocraties, est toujours contrôlé par la délégation parlementaire, quelle que soit sa forme. Le Gouvernement donnera un avis favorable [...] aux demandes d'une transparence accrue sur l'action du Gouvernement et d'un renforcement des pouvoirs de la DPR : assorties d'un respect des pouvoirs constitutionnellement dévolus à chacun, de telles demandes sont bien légitimes en démocratie.* »

## **B. L'ACTUALITÉ DU RENSEIGNEMENT A ÉTÉ MARQUÉE PAR DEUX AFFAIRES MÉDIATISÉES**

Ainsi, outre ses travaux sur les deux thèmes précédemment énumérés, la délégation a assuré un suivi de l'actualité du renseignement. À la lumière des informations parues dans la presse, la délégation a décidé d'élargir ses auditions à deux sujets : l'affaire Pegasus et l'affaire Sirli.

Pour rappel, au lendemain de l'attentat perpétré le 3 octobre 2019 à la préfecture de police de Paris, la DPR avait tenu à entendre, dès le 8 octobre, le ministre de l'intérieur, M. Christophe Castaner, et son secrétaire d'État, M. Laurent Nuñez. Une procédure judiciaire était en cours ; la délégation n'avait alors pas souhaité poursuivre au-delà ses investigations, mais avait orienté une partie de ses travaux sur la maîtrise des risques au sein des services de renseignement (procédure d'habilitation ; sécurité et sûreté des systèmes d'information ; déontologie des agents).

### **1. L'affaire Pegasus**

Un consortium de dix-sept médias, dont *France Info* et *Le Monde*, a révélé, le 18 juillet 2021, qu'une enquête de l'organisation *Forbidden Stories*, avec le soutien technique du laboratoire de cybersécurité d'*Amnesty International*, avait permis d'obtenir une liste de 50 000 numéros de téléphones ciblés entre 2016 et 2021 par le logiciel de surveillance « Pegasus », commercialisé par la société israélienne *NSO Group* à une dizaine d'États (Azerbaïdjan, Bahreïn, Hongrie, Inde, Kazakhstan, Mexique, Maroc, Rwanda, Arabie saoudite et Émirats arabes unis). Dans cette liste, un millier de numéros correspondent à l'indicatif téléphonique de la France.

Compte tenu des possibles conséquences de cette affaire sur le territoire national et sur les ressortissants français, **la délégation parlementaire au renseignement s'est immédiatement saisie de cette question en procédant à l'audition, le 27 juillet 2021, de MM. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme, et Nicolas Lerner, directeur général de la sécurité intérieure.**

Il convient de préciser à cet égard que, interrogé par *France Info* le 21 juillet 2021, le Président du Sénat, M. Gérard Larcher, avait renvoyé ce dossier à la compétence de la délégation chargée de « *contrôler l'action du Gouvernement en matière de renseignement et d'évaluer la politique publique en ce domaine* » dans le respect de « *l'indépendance de cette délégation* », et du « *secret de ses travaux* ».

a) *Une investigation qui s'annonce longue et complexe*

Pegasus est un logiciel d'intrusion « sans clic » et de captation des données de téléphones équipés des systèmes d'exploitation IOS ou Android, qui peut être installé à distance sans manipulation physique des appareils à infecter. Il s'agit d'un dispositif difficilement détectable qui permet notamment de contourner les applications de messagerie chiffrée (*Whatsapp, Signal, Telegram, etc.*) en ce qu'il accède « en clair » aux messages affichés sur les appareils – donc avant cryptage ou après décryptage. Les micros et caméras des postes infectés sont également concernés.

Dans un premier temps, les expertises réalisées par le laboratoire d'*Amnesty International* sur 67 téléphones ont révélé des « traces » de l'utilisation du logiciel Pegasus sur 37 appareils, y compris de personnalités du monde politique et de la presse. Le principal pays à l'origine du ciblage des numéros français serait, toujours selon le consortium, le Maroc. En effet, d'après différents organes de presse (*Le Monde, France Inter, Mediapart, etc.*), plusieurs des personnes qui auraient été visées par ces écoutes ont pour point commun d'être critiques à l'égard du régime de Rabat, en particulier sur le dossier du Sahara occidental. Toutefois, lors des auditions conduites par la DPR sur ce sujet, la communauté du renseignement n'a ni confirmé ni infirmé ces allégations.

\*\*\*\*\*. En conséquence, les premières actions mises en œuvre par les autorités françaises ont été :

– l'action publique a été mise en mouvement par la plainte déposée auprès du parquet de Paris par M. Edwy Plenel, Mme Lénaïg Bredoux et Mediapart, le 19 juillet 2021. Initialement, seule la DCPJ était saisie d'une enquête préliminaire. La DGSI a été co-saisie des investigations à la suite des révélations selon lesquelles des membres de l'exécutif avaient également été les cibles du logiciel à des fins d'espionnage ;

– \*\*\*\*\*

\*\*\*\*\*

b) \*\*\*\*\*

Au-delà du retentissement médiatique d'une telle affaire dans la presse, **il est rappelé que le recours, en France, aux interceptions téléphoniques sans le consentement des intéressés est étroitement encadré** selon qu'il s'agit :



– **en matière administrative**, des interceptions de sécurité autorisées par le Premier ministre, après avis de la CNCTR, en application du code de la sécurité intérieure, et mises en œuvre par le Groupement interministériel de contrôle (GIC) ;

– **en matière judiciaire**, des écoutes mises en œuvre sur demande du procureur de la République ou du juge d'instruction, en application du code de procédure pénale.

Les services français indiquent n'utiliser aucun produit de *NSO Group* (tel que Pegasus), \*\*\*\*\* :

– si la France n'utilise pas Pegasus, il n'en est pas de même pour plusieurs pays de l'Union européenne, dont l'Allemagne pour ses services judiciaires, et la Pologne – celle-ci étant désignée par la presse comme en faisant une utilisation politique. Plus d'une cinquantaine d'États seraient clients de la société *NSO Group* ;

– face au cryptage des données, le principal défi concerne le déchiffrement, lequel nécessite d'importants moyens humains et matériels. \*\*\*\*\*

Selon le CNRLT, « *il n'a jamais été question d'avoir recours à cette société* » (*NSO Group*) compte tenu du lien étroit qu'elle entretient avec l'État israélien et des contentieux impliquant l'entreprise (surveillance d'opposants politiques, piratage de *Whatsapp*, etc.), mais aussi parce que l'utilisation d'un tel outil pourrait nuire à la réputation de la France.

\*\*\*\*\*

*c) L'effet de surprise engendré par Pegasus sur les services français alerte la délégation sur la nécessité d'une réponse rapide des solutions souveraines de cybersécurité*

Les services tendent à relativiser l'effet de surprise engendré par un logiciel déjà connu pour être utilisé par plusieurs États dans la « traque des opposants », \*\*\*\*\*. Le second facteur d'absence de surprise réside dans le fait que ce logiciel est reconnu comme la meilleure solution commerciale du marché, \*\*\*\*\*.

La délégation relève toutefois que **le véritable élément de surprise demeure l'ampleur des cibles françaises** \*\*\*\*\*.

## 2. L'affaire Sirli

Dans un article publié sur Internet le 21 novembre 2021, le média d'investigation *Disclose* indique avoir « *obtenu des centaines de documents "confidentiel-défense" qui dévoilent les dérives d'une opération militaire secrète de la France en Égypte* » ayant permis à l'armée de l'air égyptienne de bombarder des civils depuis 2016.

Le 25 novembre, *France 2*, en partenariat avec *Disclose*, a diffusé un numéro de son magazine d'investigation « Complément d'enquête » intitulé « France-Égypte : révélations sur une opération secrète ».

*a) Les faits dénoncés*

Une source aurait remis des centaines de notes issues des services de l'Élysée, du ministère des armées et de la Direction du renseignement militaire (DRM) :

– sur le **plan opérationnel**, ces documents expliciteraient les conditions de mise en œuvre par la DRM d'un avion léger de surveillance et de reconnaissance (ALSR) dans le but de fournir à l'Égypte des renseignements à but antiterroriste (interceptions de communications et moyens optiques), pour protéger sa frontière ouest d'incursions depuis la Libye ;

– sur le **déroulement de l'opération**, les militaires français auraient signalé à leur hiérarchie que les renseignements fournis aux Égyptiens auraient été utilisés à des fins de lutte contre la contrebande et l'immigration illégale, occasionnant des frappes aériennes sur des civils.

*b) Les problèmes soulevés*

L'opération Sirli aurait été décidée par M. Jean-Yves Le Drian, alors ministre de la défense, en juillet 2015, à la suite d'une demande de son homologue égyptien de sécuriser les 1 200 kilomètres de sa frontière avec la Libye<sup>1</sup> :

– le cadre d'un éventuel accord de coopération technique spécifique n'est pas connu ;

– selon la presse, la DRM opérerait depuis début 2016 au moyen d'une équipe de dix opérateurs (quatre militaires et six agents privés) et d'un ALSR loué à la société luxembourgeoise *CAE Aviation* ;

– toujours selon la presse, un militaire égyptien serait présent dans l'avion pour écouter les communications interceptées ;

– les rapports des opérateurs français auraient informé, à plusieurs reprises depuis 2017, que le renseignement aérien fourni – qui à l'origine n'était pas un outil de ciblage – semblait être immédiatement utilisé par l'armée égyptienne pour éliminer des cibles au sol (véhicules de type pickup) sans aucun moyen de recoupement de l'information quant à l'identité des suspects ni au niveau de la menace ;

– les notes révéleraient enfin que le principal objectif que poursuivent les Égyptiens serait la lutte contre le trafic transfrontalier, suivi

---

<sup>1</sup> *Disclose* rapporte un bilan de la Présidence égyptienne faisant état de « 10 000 voitures remplies de terroristes et de trafiquants » détruites par des frappes aériennes de *Cessna* ou de *F-16* égyptiens.

de l'immigration illégale et, seulement en troisième position, la lutte antiterroriste – soit une liste de priorités inverse à celle qui aurait été communiquée aux forces armées françaises ;

– entre 2016 et 2018, *Disclose* met directement en cause la France dans dix-neuf bombardements conduits par l'armée égyptienne.

Présentées comme des révélations sur la complicité de la France dans des exécutions extrajudiciaires perpétrées par un allié stratégique de notre pays<sup>1</sup>, l'enquête présente l'affaire comme un « scandale d'État » et comme le « soutien à une dictature ».

*c) La délégation a souhaité user de la faculté offerte par la loi de juillet 2021 pour s'intéresser à l'affaire Sirli*

Face à ces révélations, la délégation parlementaire au renseignement a pris l'attache, en décembre 2021, de la ministre des armées et du ministre de l'Europe et des affaires étrangères, pour les auditionner sur cette affaire médiatisée, comme l'y autorise la loi de juillet 2021. En outre, M. Jean-Yves Le Drian était invité à s'exprimer devant la DPR sur l'affaire Pegasus.

Les ministres ont accepté le principe d'une audition, tout en précisant qu'ils ne pourront pas répondre, en l'état actuel du droit, sur les affaires ayant motivé ces demandes.

Cette situation a conduit le président de la DPR à écrire au Premier ministre pour l'informer de la situation et lui demander son appui dans cette démarche, en soulignant que la délégation s'était vue confier, par la loi de juillet 2021, la mission d'assurer « un suivi des enjeux d'actualité et des défis à venir » en matière de politique publique du renseignement. Par conséquent, l'exercice du contrôle parlementaire de l'action du Gouvernement, pour lequel la délégation a été créée il y a bientôt quinze ans, ne peut consister en une simple faculté d'évocation générale des questions relatives au renseignement, faculté qu'a toujours eue la délégation. Il découle donc de la loi du 30 juillet 2021 que tous les sujets relatifs aux services de renseignement ayant fait l'objet d'une couverture médiatique et d'une prise de position officielle du Gouvernement, doivent pouvoir faire l'objet d'auditions tendant à l'information du Parlement, dans le cadre de confidentialité qui est celui de la DPR. Eu égard aux révélations par la presse dont l'affaire Sirli a fait l'objet ces derniers mois, la réserve invoquée ne saurait faire obstacle à un échange, par ailleurs couvert par le secret de la défense nationale, sur des informations déjà révélées par les médias et confirmées par le Gouvernement.

Néanmoins, dans sa réponse au président de la délégation, le Premier ministre a confirmé l'interprétation juridique faite par ses ministres.

---

<sup>1</sup> Client du Rafale mais aussi de navire de combat de conception française.

### C. UNE INTERPRÉTATION JURIDIQUE CONTESTABLE

La notion d'« opération en cours » a été opposée, au cours de l'année écoulée, tant à la DPR (*cf. supra*) qu'à la CVFS (*cf.* chapitre consacré à son rapport général).

Dans sa décision n° 2001-456 DC du 27 décembre 2001, le Conseil constitutionnel avait censuré deux alinéas de l'article 154 de la loi de finances pour 2002 instituant la CVFS : « *Elle reçoit communication de l'état des dépenses se rattachant à des opérations en cours. Elle peut déléguer un de ses membres pour procéder à toutes enquêtes et investigations en vue de contrôler les faits retracés dans les documents comptables soumis à sa vérification.* »

Le Conseil constitutionnel a donc déclaré inconstitutionnelle la faculté des membres de la CVFS de s'intéresser aux opérations en cours et de mener une enquête sur pièces et sur place les concernant. En pratique, une dépense opérationnelle ne pourrait donc être vérifiée de manière détaillée par la commission que si l'opération qu'elle finance est achevée.

Toutefois, le Conseil n'a pas pris la peine de définir la notion d'« opération en cours », laissant pendante une question juridique déjà ancienne. En effet, si le terme d'« opération » est régulièrement utilisé dans des textes législatifs, il n'existe aucune définition unifiée, et surtout, aucun cadre juridique précis.

Consciente que ce terme peut faire l'objet d'interprétations extensives qui auraient pour effet de priver ses contrôles de toute effectivité, la commission a très tôt estimé qu'il convenait de lui donner une définition stricte. Aussi a-t-elle considéré que la notion d'opération recouvrait un ensemble d'actions menées en vue d'obtenir un résultat opérationnel déterminé ; lorsque ce résultat est atteint, elle estime avoir *de jure* accès aux pièces relatives à cet ensemble d'actions.

Dans son rapport pour l'année 2015, la DPR avait formulé une recommandation tendant à régler la question : « *Inciter les directeurs de service à formaliser par une décision signée de leur main ou de la main de leurs (sous-)directeurs le déclenchement et l'achèvement d'une opération.* » D'ailleurs, si la notion d'opération en cours concernait l'ensemble d'un chapitre budgétaire, la CVFS ne pourrait pas exercer son contrôle puisque certains de ces chapitres sont ouverts depuis plusieurs années, et ont vocation à être reconduits – voire pérennisés ; il en va de même pour la DPR.

La DPR avait également proposé d'« *abolir, pour la CVFS et la DPR, la restriction des "opérations en cours" au regard des évolutions constitutionnelles survenues en 2008* », le Parlement étant, depuis, amené à se prononcer sur la reconduction d'une opération extérieure lorsqu'elle excède 4 mois, ce qui n'était pas le cas auparavant. En outre, la loi de programmation militaire pour les années 2014 à 2019 dispose que : « *Les opérations extérieures en cours font, chaque année, l'objet d'un débat au Parlement. Le Gouvernement*

*communiqué, préalablement à ce débat, aux commissions compétentes de l'Assemblée nationale et du Sénat un bilan politique, opérationnel et financier des opérations extérieures en cours. »*

Au regard de ces évolutions législatives, la CVFS ne s'estime pas liée par une interdiction générale de prendre connaissance d'une opération en cours. **Elle retient cependant la nécessité que son contrôle ne puisse en aucun cas entraver le bon déroulement de l'activité opérationnelle des services** – souci évident et légitime du Conseil constitutionnel en 2001.

Le Parlement pourrait donc légitimement s'interroger sur la rédaction de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, qui définit les prérogatives de la DPR, pour tenir compte de cette interprétation.

Par ailleurs, si la Cour européenne des droits de l'homme (CEDH) condamnait la France à encadrer les échanges entre les services de renseignement français et leurs homologues étrangers, l'exclusion portant sur « *les échanges avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement* » pourrait également être remise en cause.

\*

\* \*

Enfin, la délégation a pris connaissance avec satisfaction du taux de mise en œuvre des recommandations de ses trois derniers rapports – pour les années 2018, 2019-2020 et 2020-2021 –, qui s'élèvent à 52 sur 126, auxquelles s'ajoutent 18 recommandations partiellement prises en compte et 21 en cours d'examen.

Nonobstant leur 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.

*Réunie le jeudi 24 février 2022 sous la présidence de M. François-Noël Buffet, président, la délégation parlementaire au renseignement a adopté le présent rapport relatif à son activité pour l'année 2021-2022 et l'ensemble des recommandations formulées.*

## CHAPITRE I : LA PRÉVENTION DE LA CRIMINALITÉ ET DE LA DÉLINQUANCE ORGANISÉES

Théorisée par la sociologie américaine du début du XX<sup>e</sup> siècle, la notion de « criminalité organisée » n'est entrée que relativement récemment dans le droit positif français, le code pénal ayant recours à la notion de « bande organisée »<sup>1</sup>, circonstance aggravante de plusieurs infractions mais aussi à une infraction spécifique, l'« association de malfaiteurs »<sup>2</sup>, pour appréhender les ensembles structurés de personnes se livrant à des infractions. La convention des Nations unies contre la criminalité transnationale organisée, dite convention de Palerme, signée en 2000, ratifiée par la France en 2002 et approuvée par l'Union européenne en 2004, a marqué une évolution importante dans l'ordre juridique international, en apportant une définition commune du terme.

C'est dans le prolongement de la convention de Palerme que la loi portant adaptation de la justice aux évolutions de la criminalité, adoptée en 2004<sup>3</sup>, a opéré l'intégration de la notion de criminalité organisée dans la procédure pénale française.

Il découle en droit positif de la combinaison des qualifications figurant dans le code pénal, et des spécificités procédurales prévues dans le code de procédure pénale, que la criminalité organisée est le fait de bandes organisées ou d'associations de malfaiteurs.

Pour répondre à la criminalité organisée, le code de procédure pénale permet la mise en œuvre de plusieurs moyens d'investigation spécifiques définis aux articles 706-73 et suivants du code de procédure pénale : un régime de garantie des droits moins favorable, en particulier en matière de durée de la garde à vue, qui peut durer jusqu'à 96 heures (art. 706-88), l'infiltration (art. 706-81 à 706-87), le recours à des techniques spéciales d'enquête, comme l'enquête sous pseudonyme (art. 230-46), les perquisitions en dehors des heures légales (art. 706-91), les interceptions judiciaires (art. 706-95) et la captation de données informatiques (art. 706-102-1), notamment.

---

<sup>1</sup> Article 132-71 du code pénal : « Constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions. »

<sup>2</sup> Article 450-1 du code pénal réprime « tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement ».

<sup>3</sup> Loi n° 2004-204 du 9 mars 2004.

La loi de 2004 a également prévu la création de juridictions interrégionales spécialisées en matière de criminalité et de délinquance organisées, bénéficiant d'une compétence concurrente de celle des juridictions de droit commun (articles 706-75 à 706-79 nouveaux du code de procédure pénale).

Si la lutte contre la criminalité organisée relève à titre principal de la police judiciaire et des juridictions pénales, la police administrative y a toute sa place. L'article 27 de la convention de Palerme prévoit ainsi la coopération entre les services de détection des États parties afin notamment « *de renforcer ou, si nécessaire, établir des voies de communication entre [leurs] autorités, organismes et services compétents pour faciliter l'échange sûr et rapide d'informations concernant tous les aspects des infractions visées par la présente convention (...).* »

L'article L. 811-3 du code de la sécurité intérieure permet aux services l'usage des techniques de renseignement pour « *la prévention de la criminalité et de la délinquance organisées* », qui constitue la sixième des finalités prévues.

\*\*\*\*\*

Après s'être penchée en 2017 sur les défis du renseignement économique et financier, puis à plusieurs reprises sur le renseignement en matière de radicalisation et de terrorisme, et en 2021 sur le renseignement territorial, la délégation parlementaire au renseignement a souhaité cette année consacrer la partie thématique de son rapport annuel au renseignement criminel. Bien qu'un temps moins visible du fait de la priorité légitimement accordée à la lutte contre le terrorisme, la lutte contre la criminalité organisée est une mission ancienne et centrale de plusieurs des services de renseignement du premier cercle. Restructuré à l'initiative de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) pour permettre un fonctionnement transversal des services, le renseignement criminel fait face aujourd'hui à la nécessité d'adapter ses moyens à la réalité mouvante d'une menace en pleine expansion.

## **I. LA LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE CONSTITUE UNE MISSION ESSENTIELLE DE CERTAINS SERVICES DE RENSEIGNEMENT**

La police judiciaire dispose de services destinés à fournir des analyses d'ensemble, des renseignements et à mener des actions dans les phases pré-judiciaire et judiciaire des enquêtes concernant la criminalité organisée.

Le début des années 2000 a vu un accroissement des moyens légaux à sa disposition dans cette lutte. L'attention portée à la criminalité organisée a cependant pu paraître un temps moins soutenue, les pouvoirs publics



s'étant après 2015 tournés prioritairement vers la lutte contre le terrorisme. Néanmoins, le renseignement criminel n'a pas été laissé de côté : parallèlement au renforcement de la structuration de la lutte contre le terrorisme, les instances en charge de la coordination des services de renseignement ont, dans les deux stratégies nationales du renseignement de 2014 et 2019, et dans leur déclinaison sous la forme du plan national d'orientation du renseignement, défini les enjeux liés à la criminalité et à l'action des services.

Ces évolutions s'inscrivent dans le prolongement de compétences déjà anciennes des services en la matière. Les services de renseignement relevant du ministère de l'économie, des finances et de la relance ont une compétence historique en matière de lutte contre la criminalité organisée. La Direction nationale du renseignement et des enquêtes douanières (DNRED), en charge du renseignement, du contrôle et de la lutte contre la fraude en matière douanière, se trouve naturellement en première ligne pour l'entrave et la préparation de la judiciarisation des trafics internationaux. Parallèlement aux dispositions du code de procédure pénale, le code des douanes permet à la DNRED de mettre en œuvre des pouvoirs d'investigation particulièrement efficaces pour lutter contre la criminalité organisée, notamment des techniques spéciales d'enquêtes prévues à l'article 67 *bis* et suivants du code des douanes, telles que le « coup d'achat », la livraison surveillée, la géolocalisation en temps réel, les enquêtes sous pseudonyme. Plus récent, le service de Traitement du renseignement et action contre les circuits financiers clandestins (Tracfin) a déployé des moyens de lutte contre la criminalité financière.

Par ailleurs, dans le cadre de leur mission de lutte contre les troubles à l'ordre public, le renseignement territorial (Service central du renseignement territorial - SCRT - et Direction du renseignement de la préfecture de police de Paris - DRPP) recueille du renseignement sur des individus et des groupes liés à la criminalité organisée.

Créé en 2017, le Service national du renseignement pénitentiaire (SNRP) a également parmi ses attributions la lutte contre la criminalité organisée.

La DGSE, dont la compétence s'exerce en dehors du territoire national, est elle aussi appelée à participer à la lutte contre la criminalité organisée \*\*\*\*\* :

- d'une part, \*\*\*\*\* ;
- d'autre part, \*\*\*\*\*.

Enfin, la DGSI se voit confier par l'article 2 de son décret de création du 30 avril 2014, la responsabilité de concourir à la prévention et à la répression de la criminalité liée aux technologies de l'information et de la communication. À ce titre, elle travaille sur la criminalité informatique, *a fortiori* lorsqu'elle est liée à des États adverses, en vue d'identifier ses

principaux acteurs, d'en attribuer les actions et d'analyser les principaux modes opératoires.

En matière de cybercriminalité, le service judiciaire de la DGSI est systématiquement saisi par le parquet de Paris pour traiter des infractions portant atteinte aux intérêts fondamentaux de la Nation. Celles-ci ont trait aux attaques commises au préjudice de personnes morales de droit public (réseau de l'État, des administrations déconcentrées, des établissements publics, etc.), d'opérateurs d'importance vitale, d'établissements disposant de zones à régime restrictif, ou d'entreprises particulièrement innovantes, à but d'espionnage, de sabotage, ou encore de déstabilisation. En revanche, les attaques purement crapuleuses (escroquerie, rançongiciel) ne sont pas traitées par la DGSI, sauf exception.

\*\*\*\*\*

L'évolution de la criminalité organisée suppose donc une implication croissante des services de renseignement. \*\*\*\*\*

#### **A. UN ENJEU ÉCONOMIQUE ET DE SOUVERAINETÉ FACE À LA MUTATION DES FORCES DE LA CRIMINALITÉ ORGANISÉE**

Le caractère protéiforme de la criminalité organisée, qui investit potentiellement tout le champ des infractions mais tend aussi à contaminer l'économie légale et les institutions, oblige les services de renseignement à une adaptation constante et fait appel à des champs de compétences qui dépassent de plus en plus souvent les attributions d'un seul service.

##### **1. Un périmètre en constante évolution qui impose la définition de priorités toujours sujettes à débat**

La convention de Palerme tend à la répression de la « *participation à un groupe criminel organisé* » et du blanchiment tant du produit du crime que d'argent. Si les activités visées sont limitées aux « *infractions graves* », le champ couvert est particulièrement vaste. Les protocoles se rapportant à la convention apparaissent ainsi comme autant de priorités – traite des personnes, trafic illicite de migrants, trafic illicite d'armes à feu et de munitions – qui s'ajoutent à la lutte contre le trafic de stupéfiants, déjà visé par des conventions internationales<sup>1</sup>, ou encore contre le trafic de tabac.

Les enjeux internationaux en matière de lutte contre la criminalité organisée doivent s'articuler avec les priorités définies au niveau européen<sup>2</sup>

---

<sup>1</sup> Singulièrement la convention des Nations unies contre le trafic illicite de stupéfiants et de substances psychotropes, signée à Vienne en 1988.

<sup>2</sup> Ainsi, la stratégie pour cinq ans présentée par la Commission européenne le 21 avril 2021 pour lutter contre la criminalité organisée qui prévoit de « cibler des formes de criminalité spécifiques et hautement prioritaires » en intensifiant « la coopération au niveau de l'UE

mais aussi au niveau national. S'agissant spécifiquement des missions confiées aux services de renseignement la stratégie nationale de juillet 2019 comporte les éléments suivants :

### **La stratégie nationale du renseignement de juillet 2019**

#### **La criminalité organisée**

Suivant une logique de prédation et de pouvoir, la criminalité organisée tend à substituer son ordre crapuleux à la souveraineté des Etats par l'intimidation, la violence et la corruption, au mépris de la vie et de la dignité humaines ainsi que des droits et des libertés fondamentales.

Elle cause des dommages parfois irréversibles – et souvent peu visibles – à la cohésion nationale, à la santé publique, à l'environnement et à la biodiversité, à l'éducation, à la sécurité économique et sociale, à la maîtrise des flux migratoires ainsi qu'aux finances publiques.

Si la criminalité organisée répond d'abord à des intérêts privés, elle peut peser sur les relations internationales, exercer une influence sur des gouvernements, des parlements ou des autorités judiciaires, policières ou militaires, et dans certains cas prendre le contrôle d'États ou parties d'État. Enfin, certaines organisations criminelles sont devenues de vraies puissances en capacité de concurrencer les États.

Cette criminalité facilite le terrorisme, y compris en Europe, en affaiblissant le niveau de contrôle sécuritaire de certaines zones géographiques et en fournissant des moyens de financement ou d'approvisionnement en armes, faux documents et matériels.

Les profits dégagés conduisent à la mise en place de circuits de blanchiment transnationaux et potentiellement sophistiqués, qui participent de la dérégulation financière et de la fraude fiscale et sociale, contribuent au détournement des richesses et à l'affaiblissement des finances publiques ainsi que des mécanismes de solidarité nationale.

Les services de renseignement contribuent à l'identification des entités, des acteurs et des flux alimentant cette criminalité organisée.

---

pour démanteler les structures de la criminalité organisée. Afin d'apporter une réponse efficace à certaines formes de criminalité, la Commission proposera de réviser les règles de l'UE en matière de lutte contre la criminalité environnementale et mettra en place une boîte à outils européenne de lutte contre la contrefaçon, notamment des produits médicaux. Elle présentera des mesures destinées à combattre le commerce illicite de biens culturels. La Commission [a] présent[é] également (...) une stratégie visant à lutter contre la traite des êtres humains. »

[https://ec.europa.eu/commission/presscorner/detail/fr/ip\\_21\\_1662](https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1662)

Plusieurs priorités ressortent de la stratégie nationale :

- le trafic de stupéfiants ;
- la criminalité environnementale ;
- le trafic de personnes ;
- la cybercriminalité ;
- le trafic de personnes migrantes ;
- la fraude à la TVA, aux prélèvements sociaux et aux prestations sociales.

Le pouvoir de corruption de la criminalité organisée sur les personnes et sur les pouvoirs publics est souligné, de même que les interactions entre criminalité et terrorisme.

Parallèlement aux trafics de stupéfiants, de personnes et d'armes identifiés de longue date, plusieurs trafics ont pris au cours des années 2000 un essor lié à la criminalité organisée : en particulier la criminalité environnementale, s'agissant notamment du trafic d'espèces rares ou de recyclage des déchets, et la cybercriminalité. L'ampleur des menaces fait l'objet de plusieurs synthèses annuelles ou pluriannuelles conduites par la Direction centrale de la police judiciaire (DCPJ) et par les différents services<sup>1</sup>. Ces documents, comportant des éléments de synthèse objectifs sur l'état et l'évolution de la criminalité organisée, sont de nature à nourrir utilement le débat public et devraient être plus largement diffusés, d'abord auprès des parlementaires habilités.

Au-delà de ces enjeux identifiés, la question de l'« hybridation » des risques, et singulièrement de la conjonction de la criminalité organisée et des groupes terroristes, a été présentée comme un phénomène émergent au cours des années 2000. Les éléments à la disposition de la délégation tendent plutôt au constat de l'absence d'unité des mouvements terroristes et criminels et au maintien d'une typologie reposant sur des moyens d'opération propres au service d'objectifs distincts. Intéressante à cet égard est la notion de « narco-djihadisme » parfois utilisée pour décrire la collusion entre trafiquants internationaux (latino-américains) ou locaux, et djihadistes en Afrique de l'Ouest<sup>2</sup>. L'expression s'avère trompeuse si elle est entendue comme décrivant une unité ou une alliance ; il apparaît en fait que groupes criminels et trafiquants entretiennent des relations complexes fondées sur l'intérêt pragmatique qu'ont ces acteurs à la coexistence plutôt qu'à la concurrence sur un même territoire<sup>3</sup>. La lutte contre la criminalité organisée

---

<sup>1</sup> \*\*\*\*\*.

<sup>2</sup> Nouveau Conflits : « Afrique de l'Ouest. Le péril narco-djihadiste », *revue Conflits*, 2 juillet 2021.

<sup>3</sup> Guillaume Soto-Mayor. Trafics et trafiquants : éléments structurants des sociétés sahéliennes. *Recherches Internationales, Association Paul Langevin, 2020, janvier-mars (n° 117), pp. 117-135.*

reste donc distincte de la lutte contre le terrorisme et doit disposer de moyens propres.

Face aux multiples aspects de la criminalité organisée, la délégation constate que malgré l'expertise et la mobilisation des services de renseignement ceux-ci ne peuvent affecter des ressources équivalentes sur l'ensemble des thématiques ; ils sont donc affectés en fonction des priorités définies par les pouvoirs publics. Le choix des thématiques moins prioritaires est nécessairement sujet à débat. La délégation a ainsi pu entendre que l'ampleur de la fraude à la TVA par l'intermédiaire du commerce électronique, fraude organisée depuis la Chine, reste sans réponse adéquate faute de moyens suffisants et ce malgré son impact sur les finances publiques françaises et européennes. La stratégie de submersion des services douaniers empêche l'organisation d'une entrave et de poursuites efficaces en l'absence d'une volonté déterminée de contrôle au niveau européen. Malgré l'action d'Europol, l'Union paraît en effet privilégier la fluidité de circulation des biens et l'allègement des procédures, au détriment du respect des règles fiscales. Même si cette question ne relève pas uniquement de la criminalité organisée, l'ampleur et le caractère systématique des activités frauduleuses incite la délégation à demander le renforcement des moyens matériels, juridiques et humains accordés à la DNRED pour démanteler les réseaux de fraude à la TVA et l'engagement du Gouvernement pour une meilleure prise en compte de ce phénomène au niveau européen.

<p><b>Recommandation n° 1 : Accentuer la lutte contre la fraude à la TVA.</b></p>
---

La délégation note enfin l'intérêt particulièrement marqué de la presse d'investigation envers le sujet de la criminalité organisée : les actions menées par les services, dès lors qu'elles aboutissent à des actions publiques, sont particulièrement suivies, ce qui impose non seulement une discrétion renforcée, mais aussi une stratégie de communication. Des enquêtes journalistiques souvent très fouillées s'effectuent en parallèle de l'analyse des services et reposent parfois sur des sources similaires. La délégation a ainsi pu retrouver dans certaines présentations qui lui ont été faites, et dans des articles de presse, des éléments très proches.

La délégation parlementaire au renseignement a elle-même dû choisir les thématiques sur lesquelles elle s'est penchée dans le cadre de son rapport. Pour illustrer les enjeux du renseignement criminel, elle s'est intéressée à titre principal à la question du trafic de drogue en métropole, en provenance des pays d'Amérique latine et transitant par le port du Havre. En effet, outre qu'il mobilise les services de renseignement, le trafic de drogue, du fait de l'impact sur la santé publique et des revenus qu'il génère pour les trafiquants, est un facteur majeur d'atteinte au vivre ensemble et de corruption de la société.

## 2. L'implantation de l'écosystème criminel des drogues

Le risque de déstabilisation lié au trafic de stupéfiants est connu de longue date, non seulement en Amérique latine, mais aussi en Afrique où l'influence des réseaux de trafics de stupéfiants sur certains États comme la Guinée-Bissau est documentée par les organismes internationaux. En Europe même, l'emprise des réseaux sur les Pays-Bas, qui ont conduit récemment au meurtre d'un journaliste et à la nécessité de placer sous protection le Premier ministre, est depuis plusieurs années un sujet d'inquiétude pour les autorités de police locale, et nécessairement pour la France<sup>1</sup>, pour laquelle la proximité avec les réseaux implantés aux Pays-Bas a un impact direct.

En France, la lutte contre les stupéfiants fait depuis mai 2021 l'objet d'un comité interministériel installé par le Premier ministre qui, dans le prolongement du plan national de lutte contre le trafic de stupéfiants du 17 septembre 2019, entend « agir sur l'ensemble des dimensions liées à ce phénomène. Des trafics internationaux aux deals dans les cages d'escalier ». Le chef de file chargé de la coordination des services est l'Office anti-stupéfiants (Ofast). Les moyens d'entrée des stupéfiants en provenance d'Amérique latine sur le territoire national sont multiples et certains ont fait l'objet de rapports parlementaires<sup>2</sup> spécifiques.

La délégation parlementaire au renseignement s'est particulièrement intéressée à l'impact du report des trafics de stupéfiants en provenance d'Amérique latine des ports d'Anvers et de Rotterdam sur le port du Havre, qui fait l'objet d'une attention particulière des autorités, et plus particulièrement de la DNRED. La croissance du port du Havre, déjà premier port français en termes de fret et appelé à se développer au cours des prochaines années, en fait un enjeu stratégique. \*\*\*\*\*.

\*\*\*\*\*

L'État a par ailleurs déployé d'importants outils de détection sur le port du Havre, dont un scanner à camion opéré par les services des douanes : la délégation a pu constater son rythme soutenu d'utilisation et son efficacité lors de son déplacement sur place.

Des enjeux de coopération entre les dockers, les entreprises de manutention portuaires, les autorités portuaires, les douanes et la police judiciaire demeurent pourtant. Ainsi, les communications d'informations sur les activités illégales et la sécurisation des sites restent perfectibles même si des programmes d'investissement ont été engagés par les autorités

---

<sup>1</sup> [https://www.lemonde.fr/m-actu/article/2018/03/05/pour-les-policiers-neerlandais-les-pays-bas-sont-devenus-un-etat-narco\\_5265700\\_4497186.html](https://www.lemonde.fr/m-actu/article/2018/03/05/pour-les-policiers-neerlandais-les-pays-bas-sont-devenus-un-etat-narco_5265700_4497186.html)

<sup>2</sup> Notamment le trafic de drogues entre la Guyane et la métropole, qui a fait l'objet du rapport d'information n° 707 (2019-2020) « Mettre fin au trafic de cocaïne en Guyane : l'urgence d'une réponse plus ambitieuse » de M. Antoine Karam, fait au nom de la mission d'information sénatoriale sur le trafic de stupéfiants en provenance de Guyane.

portuaires et les entreprises. La pression exercée par les réseaux dans un contexte de production massive de stupéfiants en Amérique latine ne fait en effet qu'augmenter. La presse<sup>1</sup> a largement repris les données les plus récentes concernant le trafic de cocaïne : 2,2 tonnes saisies au cours du seul mois de janvier 2022 – soit plus qu'au cours de l'année 2019 –, et 10,086 tonnes saisies en 2021. Ces chiffres doivent être mis au regard de l'estimation communément admise selon laquelle les saisies ne représenteraient que 10 % du volume de drogues transitant par le port.

\*\*\*\*\*

**Recommandation n° 2 : Augmenter les moyens humains de la DNRED en matière de lutte contre les stupéfiants dans les ports.**

## ***B. LE RÔLE CENTRAL DU RENSEIGNEMENT DANS LA LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE***

La lutte contre le trafic de stupéfiants sur le port du Havre, et spécialement les saisies, reposent pour une large part sur l'action des services douaniers. \*\*\*\*\*.

### **1. Une action adaptée au risque aboutissant à l'entrave et à la judiciarisation**

Le renseignement criminel dispose de moyens légaux importants, reposant sur les dispositions du code de la sécurité intérieure mais aussi des autres codes qui peuvent lui donner des prérogatives. Pour conduire leurs opérations, les services douaniers peuvent ainsi s'appuyer sur des dispositions contenues dans le code des douanes et dans le code monétaire et financier. La nécessité de choisir la base légale la plus adéquate constitue un enjeu important pour l'action des services, mais la multiplicité de ces bases est facteur de souplesse.

Cette souplesse permet aux services d'intervenir en matière de renseignement, de remontée des filières et d'entrave jusqu'à la judiciarisation.

L'action des services en matière de renseignement découle d'abord de la nécessité de surveillance d'activités qui ne sont pas en soi illégales ou pour lesquelles les moyens judiciaires seraient difficiles à mobiliser dans un temps adéquat. Comme le soulignait l'étude d'impact du projet de loi relatif au renseignement en 2015 : « *Dans le domaine de la haute criminalité organisée, les mêmes dispositifs [de renseignement] permettront d'acquérir des informations précieuses à l'occasion de réunions de représentants de groupes criminels*

---

<sup>1</sup> [https://www.lemonde.fr/societe/article/2022/02/07/le-port-du-havre-sous-l-emprise-croissante-du-traffic-de-cocaine\\_6112600\\_3224.html](https://www.lemonde.fr/societe/article/2022/02/07/le-port-du-havre-sous-l-emprise-croissante-du-traffic-de-cocaine_6112600_3224.html)

*transnationaux qui peuvent se tenir en France, compte tenu de son attrait. De telles réunions, qui ne constituent pas en soi une infraction susceptible de mobiliser des moyens judiciaires, nécessitent une forte réactivité dès lors que les déplacements de ces personnes sont signalés dans le cadre de coopération avec les services partenaires. »*

La caractérisation des réseaux criminels, l'établissement des liens entre des acteurs et leur identification alors même que certains, notamment pour les activités passant par le « *dark web* », ne connaissent par les identités réelles de leurs complices, nécessitent des compétences d'investigation et des compétences techniques de pointe à la mesure de la complexité des moyens de communication utilisés par les réseaux.

Ces recherches sont aussi nécessaires à l'étude des évolutions des moyens d'actions de la criminalité, et à la détection des risques émergents. Un exemple récent, ayant fait l'objet d'une communication de la DNRED à la presse, est l'apparition de nouveaux profils d'acheteurs d'armes issues du trafic, désireux d'assurer par ces moyens illégaux leur « protection » ou celle de leur famille.

Le service à compétence nationale Tracfin apparaît comme l'un des centres du renseignement criminel, susceptible d'irriguer l'action de l'ensemble des autres services par le suivi des flux financiers nationaux et internationaux finançant les activités criminelles ou destinés au blanchiment. La mise en lumière des réseaux liés au financement du crime organisé offre une capacité d'entrave et de démantèlement particulièrement efficace. Elle offre également la possibilité de détecter la pénétration de l'économie légale par les flux financiers issus du crime organisé, sujet de vigilance nécessaire des pouvoirs publics. L'extension récente des compétences de Tracfin et la croissance rapide du service au cours des dernières années, ont entraîné une évolution de sa structure qui doit aboutir en 2023. De plus en plus sollicité dans le cadre des investigations conduites par les autres services de renseignement en parallèle du développement de ses propres investigations, il importe de conforter le double rôle de Tracfin en tant que centre d'informations sur les flux financiers criminels et service de renseignement à part entière, tout en permettant à la structure de se stabiliser. La délégation estime que l'efficacité de l'information obtenue ne doit pas conduire à une croissance trop rapide qui pourrait limiter l'efficacité du service.

**Recommandation n° 3 : Accompagner la croissance de Tracfin afin de permettre un développement de ses compétences et une diffusion de son expertise en matière de blanchiment.**

Les actions des services de renseignement peuvent aboutir à une entrave, le cas échéant judiciaire. La judiciarisation suppose, outre la constitution de dossiers suffisamment étayés sur des infractions caractérisées et susceptibles d'entraîner une réponse pénale, que celle-ci soit proportionnée et de nature à mettre fin à l'action du réseau. Le moment de la



transmission d'informations à la justice est donc particulièrement sensible et nécessite des relations efficaces de travail entre magistrats et services de renseignement. La « culture » des différents services joue ici un rôle déterminant : certains, disposant de pouvoirs de police judiciaire et donc de l'expérience d'un travail quotidien avec les parquets, paraissant avoir avec la justice une relation plus fluide que ceux dont les liens avec les magistrats sont plus distants. Tous les services se sont cependant félicités des dispositions introduites dans la loi du 30 juillet 2021 permettant la transmission par les magistrats de pièces et éléments judiciaires aux services de renseignement. Une doctrine d'emploi en cours d'élaboration par la Chancellerie, en lien avec la CNRLT, devrait permettre la mise en œuvre de ces transmissions et, dès lors, de surmonter les réticences qui peuvent encore exister au sein de certains services.

\*\*\*\*\*

La délégation parlementaire au renseignement s'inquiète par ailleurs de l'ampleur des informations recueillies à l'étranger. En matière de lutte contre le trafic de stupéfiants, les informations provenant des autorités des pays producteurs et des services américains sont une source importante de saisie de drogues. \*\*\*\*\*

<b>Recommandation n° 4 : *****.</b>
-------------------------------------

## **2. L'importance des techniques de renseignement**

Les services spécialisés de renseignement disposent de moyens techniques importants et de facilités d'usage dont ne disposent pas nécessairement les services de police administrative et judiciaire. \*\*\*\*\*.

Le recours aux techniques de renseignement suppose cependant une innovation permanente et une grande vigilance dans la lutte contre la criminalité organisée. Les réseaux criminels disposent en effet de moyens techniques souvent similaires à ceux des services et d'informations sur les techniques de renseignement qui leur permettent la mise en place de contre-mesures, voire d'espionnage des services eux-mêmes. Les possibilités offertes par des matériels facilement accessibles dans le commerce ne font que renforcer cette course à l'armement technique entre services de renseignement et réseaux criminels. Il est donc essentiel que les services ne soient pas distancés et disposent toujours des matériels les plus performants. Cela suppose aussi bien les budgets adéquats pour les obtenir que les capacités pour les utiliser voire les améliorer, \*\*\*\*\*.

\*\*\*\*\*, la délégation souhaite qu'un assouplissement du statut de repentir puisse être examiné par la Chancellerie, en lien avec les services de renseignement.

**Recommandation n° 5 : Faire évoluer le régime applicable aux repentis \*\*\*\*.**

**Le rôle du renseignement pénitentiaire  
dans la lutte contre la criminalité organisée**

Le besoin de collecter des informations sur l'activité et les communications des personnes détenues n'est pas nouveau. En 2003, il avait conduit à la création d'un bureau du renseignement pénitentiaire (dit « EMS 3 ») au sein du département de l'état-major de sécurité de la direction de l'administration pénitentiaire, chargé « *de recueillir et d'analyser l'ensemble des informations utiles à la sécurité des établissements et des services pénitentiaires* » selon les termes de l'arrêté du 7 janvier 2003 portant organisation en bureaux de la direction de l'administration pénitentiaire, qui avait ainsi donné une structure à des pratiques mises en œuvre de façon informelle dès les années 1980. Disposant de moyens matériels et humains limités, il avait pour tâches principales la surveillance de certains détenus dits « difficiles » ainsi que la prévention de la radicalisation.

Les attentats commis par Mohamed Merah en 2012, puis ceux de Charlie Hebdo et du Bataclan de janvier et novembre 2015, ont profondément modifié les attentes à l'égard du renseignement pénitentiaire dans un contexte de prise de conscience du risque de radicalisation en prison et des lacunes du renseignement pénitentiaire en matière de lutte contre le terrorisme et le crime organisé. Ces réflexions ont conduit à une transformation de ce dernier afin de faire face aux nouvelles menaces et de garantir la continuité du renseignement avant, pendant et après le temps de détention :

- d'une part, la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, a habilité les services de l'administration pénitentiaire à faire usage des techniques de renseignement prévues au livre VIII du code de la sécurité intérieure, conduisant ainsi à ériger ce service en l'un des services de renseignement du second cercle ;

- d'autre part, la structuration du renseignement pénitentiaire a été réorganisée en trois niveaux :

\* au niveau national, le bureau du renseignement pénitentiaire, devenu Bureau central du renseignement pénitentiaire en 2017, a été transformé en service à compétence nationale par un arrêté du 29 mai 2019, avec pour mission de « *rechercher, collecter, exploiter, analyser et diffuser les informations et renseignements susceptibles de révéler des risques d'atteinte aux intérêts fondamentaux de la Nation, à la sécurité des établissements pénitentiaires, des établissements de santé destinés à recevoir des personnes détenues et des services pénitentiaires* » ;

\* sous l'autorité de ce dernier, des cellules interrégionales du renseignement pénitentiaire (CIRP), \*\*\*\*\* ;

\* enfin, \*\*\*\*\*.

Cette réorganisation s'est par ailleurs accompagnée d'un renforcement substantiel des effectifs et des moyens affectés au renseignement pénitentiaire (\*\*\*\*\*).

\*\*\*\*\*. Si la coopération avec les directions des centres permet de compenser les besoins en personnel, un renforcement des moyens de terrain est nécessaire, \*\*\*\*\*, au regard des enjeux et de la nécessité de placer les sources au plus près des détenus visés.

\*\*\*\*\*

## II. UNE COORDINATION ET UNE STRUCTURATION À RENFORCER ENTRE SERVICES DE RENSEIGNEMENT DU PREMIER ET DU SECOND CERCLES

### A. COORDONNER L'ACTION DE SERVICES AUX COMPÉTENCES COMPLÉMENTAIRES ET PARFOIS CONCURRENTES

#### 1. Le pilotage de la lutte contre la criminalité organisée est confié à la police judiciaire...

La stratégie nationale du renseignement, prévue par la loi du 18 décembre 2013, et la doctrine de renseignement criminel élaborée en 2021 s'adressent prioritairement aux six services spécialisés du premier cercle mais concernent également l'ensemble des services de police et de gendarmerie, des armées et autres entités de contrôle et de soutien concourant à la politique publique du renseignement.

Dans ce cadre, s'il apparaît que les enjeux prioritaires du renseignement sont d'abord orientés vers les menaces terroristes, l'anticipation des crises et la défense de l'économie du pays - \*\*\*\*\* - la lutte contre la criminalité organisée est mentionnée comme l'une des menaces transversales, avec la menace cyber, les ingérences et la prolifération des armements.

En ce qui la concerne, le pilotage de la lutte contre la criminalité organisée relève de la police judiciaire. À ce titre, la délégation a entendu l'ensemble des services et offices centraux de police judiciaire concernés par le sujet, ainsi que les services du premier cercle (notamment la DGSI, la DNRED, Tracfin et la DGSE) auxquels il est fait appel au titre de leurs capacités de renseignement technique et humain.

Pour les services de police et de gendarmerie mentionnés par la stratégie nationale du renseignement, l'audition du directeur central de la police judiciaire (DCPJ), M. Jérôme Bonet, a mis en évidence que **la notion de « criminalité organisée » recouvrait plusieurs situations infractionnelles** (acte individuel prémédité, crime professionnel perpétré par plusieurs individus, et crime syndiqué au sein d'une association permanente de malfaiteurs) et **plusieurs champs d'actions** qu'il s'agisse du trafic de stupéfiants, du blanchiment d'argent, des vols et trafics, de la traite d'êtres humains ou encore des délits environnementaux.

Au sein de la police nationale, la DCPJ a la charge de la répression de la criminalité organisée et de la délinquance spécialisée sous ses diverses formes. Selon la DCPJ, le trafic de stupéfiants représente 70 % de l'ensemble de cette criminalité.

D'autre part, le recours aux techniques de renseignement aux fins d'incrimination nécessite une relation étroite entre les services de renseignement et les services de police judiciaire<sup>1</sup>, mais le constat demeure que, malgré de nombreux échanges \*\*\*\*\*, **l'activité de renseignement en tant que telle n'est pas spécifiquement orientée vers la criminalité organisée.**

Au niveau de la DCPJ, il est fait état de deux besoins principaux :

- institutionnaliser la relation entre services de renseignement et services de police judiciaire ;
- renforcer les moyens de pilotage et de lutte contre une criminalité organisée qui intègre des moyens cyber et juridiques transfrontaliers toujours plus complexes.

**Recommandation n° 6 : Renforcer la fluidité du recours des offices, en tant que chefs de file dans leur domaine de compétence respectif, aux services de renseignement spécialisés du premier cercle.**

## **2. ...mais les moyens d'actions sont répartis entre différents offices centraux et services du second cercle...**

La table ronde consacrée aux offices a montré que **la réforme des offices et la doctrine de renseignement criminel élaborée en 2021 avaient permis de clarifier le rôle de chaque entité et de renforcer leur efficacité en leur conférant une fonction de chef de file** dans leurs domaines de compétences respectifs désignés par leur dénomination :

- l'Office anti-stupéfiant (Ofast) ;
- l'Office central pour la répression de la traite des êtres humains (OCRTEH) ;

---

<sup>1</sup> La DCPJ indique effectuer 1 500 demandes par an à des services de renseignement.

- l'Office central de lutte contre le crime organisé (OCLCO) ;
- l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) ;
- l'Office central de lutte contre la délinquance itinérante (OCLDI).

Si la lutte contre le trafic de stupéfiants représente le principal enjeu quantitatif, celle-ci requiert de plus en plus de compétences transversales dans la mesure où ce trafic draine des activités de blanchiment mais aussi de traite d'êtres humains. En revanche, la porosité entre ces trafics et le financement du terrorisme ne semble pas établie.

Ainsi, contrairement à ce que pourraient laisser entendre les différentes dénominations, ce n'est pas l'OCLCO qui traite l'ensemble des affaires de criminalité organisée, son périmètre d'action étant focalisé sur le « haut du spectre du banditisme » relatif aux associations de malfaiteurs, de recherche de fuyitifs et le trafic d'armes et de véhicules, considéré comme le « nerf de la guerre » des organisations criminelles.

Du fait du caractère transversal de la lutte contre la criminalité organisée et sa répartition entre les différents offices centraux, la délégation ne discerne pas de logique évidente de pilotage :

- la mise en œuvre des collaborations entre services peut être dictée par le terrain ou l'urgence pour solliciter des moyens techniques ou humains supplémentaires ;

- \*\*\*\*\*, le choix du service chef de file en cas d'intervention fait l'objet d'une répartition au cas par cas \*\*\*\*\* selon des critères plus factuels que juridiques, les circonstances et les moyens présents<sup>1</sup>.

En raison même de la grande variété des formes que prend la criminalité organisée, certains services ont développé des domaines d'expertise liées à l'expérience acquise par certains de leurs agents et donc très dépendantes des personnes. \*\*\*\*\*

**Recommandation n° 7 : Améliorer le recrutement et le traitement des sources humaines, en assurant la transmission des connaissances des agents recruteurs.**

La délégation n'a pas eu à connaître de problématiques de concurrence entre services. Toutefois, si ces pratiques semblent fonctionner sur la base d'une saine mutualisation des moyens, elles mettent en évidence des limites des services de police en matière de renseignement et leur dépendance aux ressources des services de renseignement spécialisés, \*\*\*\*\*.

---

<sup>1</sup> \*\*\*\*\*.

### **3. ...et nécessiteraient de mieux structurer le recours aux services de renseignement du premier cercle**

L'Ofast, qui apparaît en première ligne tant par le volume des affaires traitées – les gains à blanchir résultant du trafic de stupéfiants représenteraient 100 millions de dollars par semaine<sup>1</sup> –, présente un recours massif et structuré aux services de renseignement des premier et second cercles :

- premièrement \*\*\*\*\* ;
- deuxièmement \*\*\*\*\* ;
- troisièmement \*\*\*\*\* ;
- et enfin quatrièmement \*\*\*\*\*.

La mobilisation des moyens de renseignement se faisant selon deux types de cadre juridique : le code de procédure pénale et le code de la sécurité intérieure.

Mais la mobilisation du renseignement demeure encore disparate. \*\*\*\*\* , certains offices n'ont que des liens limités ou ponctuels avec les services de renseignement spécialisés, malgré leurs propres difficultés à développer en interne du renseignement technique ou humain.

**Recommandation n° 8 : Élever le niveau de priorité de la lutte contre la criminalité organisée dans le renseignement fourni par les services du premier cercle, dans le respect de leurs compétences.**

En outre, la relation entre les offices et les services spécialisés de renseignement gagnerait à une meilleure structuration et clarté des objectifs :

- \*\*\*\*\* ;
- \*\*\*\*\* ;
- \*\*\*\*\*.

### ***B. ÉLEVER LE NIVEAU DE RÉPONSE FACE À UNE CRIMINALITÉ ORGANISÉE TOUJOURS PLUS TECHNIQUE ET INTERNATIONALE***

Plutôt que la capacité de collaboration et de mutualisation des moyens, \*\*\*\*\* , de surveillance et de renseignement humain, ce sont les mutations opérées par les organisations criminelles elles-mêmes qui imposent de rehausser le niveau des moyens techniques et humains des offices comme des services spécialisés.

---

<sup>1</sup> Selon la DNRED, en 2020, 50 tonnes de stupéfiants ont été saisis (16 tonnes de cocaïne et 34 tonnes de cannabis).

## 1. Des enjeux techniques, *dark web* et cryptomonnaies

La question des outils est cruciale. La présentation par la DNRED des nouveaux moyens de « commercialisation » des produits de la criminalité organisée sur le *dark web* (vente de stupéfiants, de véhicules et de produits de vols ou de trafics en tous genres) en faisant appel aux cryptomonnaies comme moyens de paiement, a démontré la nécessité d'obtenir de nouveaux moyens techniques d'enquête et d'investigation. Ainsi, l'identification des trafiquants opérant sous des profils cachés peut mobiliser sur une longue période des moyens et des compétences techniques pendant plusieurs mois.

L'enjeu pour la DNRED est de pérenniser une « cyberdouane » dotée de moyens matériels et humains adéquats pour permettre la poursuite des démantèlements de plateformes de vente, ces dernières pouvant fournir plusieurs milliers de « clients » en stupéfiants, armes et faux papiers.

## 2. Des enjeux humains

À l'enjeu technique se greffe l'enjeu en ressources humaines pour exploiter les systèmes d'information, mais aussi pour continuer à assurer un renseignement humain qui demeure indispensable pour débusquer les réseaux de trafic de stupéfiants.

Les deux principales difficultés rencontrées par les services ont trait, d'une part, au niveau de recrutement des opérateurs, et d'autre part, à leur environnement juridique, toujours plus complexe :

- tous les services font part de la difficulté à recruter et fidéliser des personnels qualifiés dans la cybercriminalité. \*\*\*\*\* ;
- s'agissant plus particulièrement des services et offices à compétence judiciaire, \*\*\*\*\*.

<b>Recommandation n° 9 : Renforcer les moyens de lutte cyber face au développement des nouveaux modes d'action de la criminalité organisée.</b>
---

Les moyens financiers dont disposent les réseaux de criminalité organisée et les méthodes d'intimidation qu'ils sont susceptibles de mettre en œuvre à l'encontre des agents des services de sécurité intérieure, de renseignement et des autorités publiques, imposent un suivi, voire un renforcement, des mesures de lutte contre la corruption. L'ensemble des services entendus par la délégation a fait part du risque aigu existant en la matière et qui correspond à la nature même du crime organisé.

C'est d'ailleurs au titre de la lutte contre les menaces transversales et de la criminalité organisée que la corruption figure dans les enjeux prioritaires du renseignement : « *Suivant une logique de prédation et de pouvoir,*

la criminalité organisée tend à substituer son ordre crapuleux à la souveraineté des États par l'intimidation, la violence et **la corruption** [...] »<sup>1</sup>. La corruption est également citée, au même titre que la prolifération, l'espionnage industriel et scientifique, le chantage cyber et la subversion, parmi les menaces justifiant la mise en œuvre de la mission d'entrave du renseignement<sup>2</sup>.

Lors de son audition, M. Jérôme Bonet, directeur central de la police judiciaire, a considéré que la corruption constituait un « *vrai sujet qui n'est pas anecdotique* » tant elle se ramifie dans la sphère publique et privée comme un prérequis nécessaire au trafic de stupéfiants. La corruption de fonctionnaires est mentionnée dans le domaine des douanes mais aussi de l'administration fiscale. \*\*\*\*\*

Tant la DCPJ que la DNRED, dans le cadre de la visite de terrain effectuée au port du Havre, soulignent l'importance des sommes en jeu et la vulnérabilité des agents potentiellement visés. \*\*\*\*\*

Pour ne pas risquer d'atteindre la situation de « narco-État » observée dans certains pays du Nord de l'Europe où l'emprise des organisations criminelles vise le plus haut sommet de l'État, la DCPJ alerte sur le traitement insuffisamment frontal de la corruption. À ce titre, elle préconise trois axes de lutte :

- faire de la corruption un véritable item des politiques publiques économiques de lutte contre la fraude ;
- renforcer la prévention en s'inspirant de l'expérience anti-mafia qu'a menée l'Italie dans l'opération *mani pulite* ;
- élargir le champ d'application des déclarations d'intérêts aux agents en charge de la lutte contre la criminalité organisée.

Dans le secteur privé, notamment celui des dockers, la DNRED décrit l'échelle des montants corruptifs comme allant de quelques milliers d'euros à plus de 100 000 euros pour des opérations pouvant apparaître anodines telles que le prêt d'un badge d'accès ou le déplacement d'un container. Dès l'acceptation d'une somme d'argent par un agent public ou privé, l'organisation « verrouille » les agents corrompus. Ceux-ci peuvent par ailleurs faire l'objet de chantage, voire d'assassinat<sup>3</sup>, de la part d'autres individus ou organisations les soupçonnant d'avoir perçu une forte somme d'argent. Le trafic de drogue apparaît comme un puissant générateur de déstabilisation des institutions publiques – à commencer par l'échelon local – et doit, par conséquent, être également abordé sous l'angle de la lutte contre la fraude et la corruption.

---

<sup>1</sup> Stratégie nationale du renseignement (page 7).

<sup>2</sup> Stratégie nationale du renseignement (page 9).

<sup>3</sup> La pression qu'exercent les trafiquants de drogue sur les dockers est apparue au grand jour lorsqu'en juin 2020, un docker, délégué CGT, avait été enlevé puis retrouvé mort sur un parking de l'agglomération havraise.



Il s'agit donc, avant tout, de garantir la sécurité des agents, des élus et de leur entourage, par la mise en œuvre rigoureuse de protocoles permettant de séparer leur vie personnelle de leur activité professionnelle liée à la lutte contre le crime organisé.

Mais, face à l'ampleur croissante des réseaux, il appartient également aux services d'assurer un contrôle accru des agents et des autorités face au risque de corruption. Cette mission nécessairement délicate doit faire l'objet d'une coordination entre les services concernés par la lutte contre la criminalité organisée.

**Recommandation n° 10 : Développer les mesures de prévention de la corruption des agents et des autorités publiques.**



## CHAPITRE II : L'ENCADREMENT DES ÉCHANGES ENTRE LES SERVICES DE RENSEIGNEMENT FRANÇAIS ET LEURS HOMOLOGUES ÉTRANGERS

La délégation note avec satisfaction le progrès des travaux conduits par la CNRLT pour la définition d'un cadre susceptible de répondre aux obligations fixées par la Cour européenne des droits de l'Homme (CEDH) dans ses arrêts *Big Brother Watch* et autres c. Royaume-Uni, et *Centrum för rättvisa* c. Suède, de mars 2021. Elle note que les réticences des services sur le principe même d'un tel encadrement ont été surmontées, la condamnation prochaine de la France ne faisant aucun doute non plus que la nécessité d'un cadre législatif. \*\*\*\*\*

Cette solution, \*\*\*\*\*, est équilibrée. Elle appelle cependant une évolution du contrôle parlementaire et ne répond pas à l'ensemble des questions. S'agissant du contrôle parlementaire, la DPR ne peut actuellement connaître des échanges avec les services étrangers ; cette interdiction ne serait plus compatible avec l'évolution du cadre légal \*\*\*\*\*. Elle devrait donc disparaître ou, *a minima*, fortement évoluer. S'agissant des questions non résolues, figure celle du contrôle de l'utilisation des informations fournies à des services étrangers. \*\*\*\*\*.

Se pose enfin la question du calendrier de la réforme : la CNRLT souhaite attendre l'arrêt condamnant la France pour prévoir un régime répondant exactement aux exigences de la Cour et n'allant pas au-delà. La DPR s'interrogeait initialement sur l'opportunité d'une telle option, le Royaume-Uni ayant, par exemple, fait évoluer sa législation avant d'être condamné, et ce régime ayant été validé par la Cour. Néanmoins le calendrier parlementaire et celui possible de la Cour européenne des droits de l'homme paraissent converger. L'arrêt de la Cour concernant la France pourrait être rendu à l'automne après la reprise de la session ordinaire, ce qui paraît un délai acceptable pour faire évoluer le droit existant. Dans l'attente de l'avis qui sera rendu par la CNCTR sur le dispositif proposé, et sous réserve des évolutions nécessaires du contrôle parlementaire qui doivent être mises en place parallèlement, la DPR estime que celui-ci constitue une réponse satisfaisante à son souhait que le cadre juridique du renseignement soit conforme aux obligations internationales de la France.

\*

\*

\*

La CEDH a été saisie de trois affaires contestant chacune des éléments du régime des pouvoirs d'enquête du Royaume-Uni en vertu de la loi de 2000 sur la régulation des pouvoirs d'enquête (RIPA), s'agissant de leur licéité au regard des articles 8 et 10 de la Convention européenne des droits de l'homme (CEDH). Ces affaires portaient en particulier sur l'interception de masse, le partage international de renseignements et l'acquisition ciblée de données de communication<sup>1</sup>.

Le présent chapitre s'attachera à présenter la réponse du Royaume-Uni à l'arrêt de la CEDH ainsi que le cadre juridique allemand en vigueur en matière d'échanges de renseignements.

## I. LES AJUSTEMENTS OPÉRÉS PAR LE ROYAUME-UNI APRÈS L'ARRÊT DE LA CEDH

Suite à l'arrêt rendu par la CEDH, le Royaume-Uni a adressé au Conseil des ministres du Conseil de l'Europe, le 25 novembre 2021, une communication sur le plan d'action<sup>2</sup> relatif à l'affaire *Big Brother Watch* et autres c. Royaume-Uni.

Dans ce document, le pays indique que :

— la loi sur la régulation des pouvoirs d'enquête de 2000 (*Regulation of Investigatory Powers Act - RIPA*), en cause dans la plainte, a été largement remplacée, en 2016, par la loi sur les pouvoirs d'enquête (*Investigatory Powers Act - IPA*). Cette dernière inclut des garanties renforcées, au premier rang desquelles un « double verrouillage » puisque les mandats doivent être autorisés par un secrétaire d'État et approuvés par un juge du bureau du commissaire aux pouvoirs d'enquête (*investigatory powers commissioner's office - IPCO*)<sup>3</sup>. L'IPCO assure, en outre, une surveillance solide et indépendante de la façon dont les pouvoirs sont utilisés ;

— le règlement sur la conservation et l'acquisition de données de 2018 a également renforcé les garanties relatives au régime des données de communication dans le cadre de l'IPA, en introduisant un seuil d'infraction grave (*serious crime threshold*) et une autorisation indépendante des demandes de données de communication pertinentes ;

— ainsi, l'adoption en 2016 de l'IPA a remédié à la majorité des violations constatées par la CEDH. En particulier, l'appréciation de la Cour selon laquelle « l'autorisation devrait à tout le moins indiquer les types ou catégories de sélecteurs à utiliser »<sup>4</sup> en matière d'interception en masse, a été

---

<sup>1</sup> [https://hudoc.echr.coe.int/fre#{%22tabview%22:\[%22notice%22\],%22itemid%22:\[%22001-210280%22\]}](https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22notice%22],%22itemid%22:[%22001-210280%22]})

<sup>2</sup> [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=0900001680a4cd00](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a4cd00)

<sup>3</sup> L'IPCO est l'autorité de surveillance de l'utilisation des pouvoirs d'enquête.

<sup>4</sup> Point 354.

corrigée par l'ajout d'objectifs opérationnels donnant au secrétaire d'État et à l'IPCO plus de détails concernant l'utilisation d'un mandat d'interception en masse.

S'agissant des deux violations non corrigées par l'IPA, le gouvernement britannique précise qu'il s'agit de :

— la nécessité de mettre en place des garanties renforcées « *lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles* » ;

— et la nécessité « *que l'utilisation de sélecteurs forts se rapportant à des personnes identifiables soit soumise à une autorisation interne préalable comportant une vérification séparée et objective de la conformité de la justification avancée aux principes susmentionnés* ».

Dans son plan d'action, le gouvernement britannique envisage que cela pourrait être corrigé notamment en amendant l'IPA, le code de pratique des interceptions ainsi que les orientations et systèmes internes. En attendant l'entrée en vigueur de ces modifications, des mesures temporaires pourront être mises en œuvre. Le gouvernement indique avoir consulté l'IPCO au sujet de ces violations.

S'agissant de la question de la conservation des données, la Cour a estimé « *qu'il aurait été souhaitable que les durées de conservation plus courtes indiquées par le Gouvernement au cours de la présente procédure soient reflétées dans des dispositions législatives et/ou d'autres mesures d'ordre général* ». Le gouvernement britannique a précisé qu'il y avait de bonnes raisons derrière des durées de conservation différentes pour les différentes organisations et types de communications, et que chaque cas avait été approuvé par l'IPCO. Ainsi, il a déclaré ne pas vouloir y apporter de modifications.

En conclusion, le gouvernement britannique indique que les modifications identifiées seront présentées devant le Parlement s'agissant de l'IPA, et lors d'une consultation publique s'agissant du code de pratique.

### Interception suite à une demande étrangère

L'article 52 de l'IPA est la base juridique en matière d'interception de données suite à une demande provenant d'un autre pays<sup>1</sup>. Il dispose qu'une communication peut être interceptée pour le compte d'une demande provenant de l'étranger si quatre conditions sont réunies :

- l'interception est effectuée par l'opérateur de télécommunications, ou en son nom, sur un service dont il est le fournisseur ;

- l'interception fait suite à une demande formulée par les autorités compétentes d'un pays ou d'un territoire en dehors du Royaume-Uni, conformément à un accord international « pertinent », c'est-à-dire auquel le Royaume-Uni est partie et qui a été considéré comme « pertinent » par les autorités ;

- l'interception a pour but d'obtenir des informations sur un individu situé en dehors du territoire britannique, ou supposé être en dehors du territoire britannique ;

- toute autre condition posée par le secrétaire d'État dans un règlement est respectée.

Dans le cas où la demande émane d'un pays ou territoire dans lequel la personne visée par l'interception est passible de la peine de mort, l'accord international ayant servi comme base à la demande ne peut être considéré comme « pertinent », à moins que le secrétaire d'État n'ait sollicité une garantie écrite de non-utilisation des informations obtenues en vertu de l'accord dans le cadre d'une procédure pour une infraction entraînant la peine de mort.

Le code de pratique des interceptions<sup>2</sup>, quant à lui, reprend dans son paragraphe 12.9 les conditions posées par l'article 52 précité, et précise dans son paragraphe 12.10 que le secrétaire d'État doit désigner les accords internationaux auxquels l'article 52 s'appliquera (c'est-à-dire les accords internationaux « pertinents ») et qu'il peut aussi adopter des règles fixant des conditions supplémentaires à remplir avant d'accéder à la demande.

Enfin, selon le site de l'IPCO, la « *surveillance des pouvoirs d'interception de masse a évolué pour refléter l'arrêt de la Cour européenne des droits de l'homme dans l'affaire Big Brother Watch et autres c. Royaume-Uni* »<sup>3</sup>.

<sup>1</sup> <https://www.legislation.gov.uk/ukpga/2016/25/section/52>

<sup>2</sup> [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/715480/Interception\\_of\\_Communications\\_Code\\_of\\_Practice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf)

<sup>3</sup> <https://www.ipco.org.uk/what-we-do/inspections/carrying-out-an-inspection/bulk-powers/>

## II. LE CADRE LÉGISLATIF EN VIGUEUR EN ALLEMAGNE EN MATIÈRE D'ÉCHANGE D'INFORMATIONS

### A. LA CONSTITUTION DE FICHIERS COMMUNS

Aux termes de la loi sur le service national de renseignement du 20 décembre 1990 (*Gesetz über den Bundesnachrichtendienst – BNDG*)<sup>1</sup>, « Le Service fédéral de renseignement peut, à des fins d'échange et d'évaluation conjointe de données personnelles, gérer des fichiers communs avec des organismes publics étrangers ou y participer. Ces données doivent se référer à des situations de risque déterminées ou à certaines catégories de personnes. » La coopération n'est toutefois possible que dans la mesure où :

- il existe pour l'Allemagne un intérêt considérable en matière de politique étrangère et de sécurité ;
- le respect des principes fondamentaux de l'État de droit est assuré dans les pays participants ;
- il est garanti que le principe de réciprocité sera appliqué.

Si cette coopération s'effectue avec un pays membre de l'Union Européenne, de l'Association européenne de libre-échange (AELE) ou de l'OTAN, l'approbation émane des services de la Chancellerie. S'il s'agit d'un pays tiers, l'approbation doit alors émaner du directeur de la Chancellerie<sup>2</sup>. La commission de contrôle parlementaire doit être informée de cette coopération.

Le cadre de la coopération doit être préalablement consigné par écrit dans une déclaration d'intention, qui doit inclure :

- les objectifs de la coopération ;
- des précisions sur le partage des données ;
- l'indication que les données ne devront être utilisées que pour ces objectifs ;
- que le service de renseignement fédéral (*Bundesnachrichtendienst*, ci-après BND) se réserve le droit de demander des informations sur l'utilisation qui a été faite des données transmises dans le fichier partagé.

La constitution de fichiers communs nécessite de prendre un acte (*dateianordnung*) à cet effet, devant contenir des informations telles que :

- l'intitulé du fichier ;

---

<sup>1</sup> <https://www.gesetze-im-internet.de/bndg/BJNR029790990.html>

<sup>2</sup> Le Directeur de la Chancellerie est nommé par le Chancelier et peut être soit un secrétaire d'État, soit un ministre fédéral en charge des missions particulières (*Bundesminister für besondere Aufgaben*). C'est le cas du directeur actuel.

- sa finalité ;
- les conditions de conservation, de communication et d'utilisation ;
- la fourniture ou l'alimentation en données, y compris la possibilité par le service étranger participant d'inscrire, pour une personne, des données complémentaires à celles déjà présentes ;
- le droit d'accès ;
- le délai de réexamen et la durée de conservation ;
- pour chaque consultation du fichier commun, la consignation par le BND du moment de la consultation ainsi que du service l'ayant fait ;
- la base juridique du fichier de données ;
- les services étrangers autorisés à saisir et à consulter les données ;
- l'information immédiate aux services étrangers participants en cas d'indice d'inexactitude des données saisies ainsi que la vérification et, si nécessaire, la modification, la correction ou la suppression des données par le service les ayant entrées ;
- la responsabilité du BND s'agissant des demandes de dommages et intérêts des personnes concernées.

Cet acte nécessite l'approbation de la Chancellerie et, préalablement à son adoption, le commissaire fédéral à la protection des données et à la liberté de l'information<sup>1</sup> doit être entendu.

L'inscription de données personnelles par le BND dans les fichiers communs avec les services étrangers n'est possible qu'à une double condition : les données sont communicables à tous les pays participants ; le BND est également autorisé à entrer les données dans ses propres fichiers. Autant le BND que les services partenaires peuvent accéder directement et utiliser les données personnelles stockées dans la mesure où cela est nécessaire pour atteindre les objectifs pour lesquels le fichier a été créé. Toute inscription dans le fichier, ainsi que tout accès, doit être enregistré dans un journal dont les données doivent être conservées jusqu'à la fin de la deuxième année civile suivant leur inscription, puis supprimées immédiatement.

En cas de transmission par le BND de données à caractère personnel, les dispositions de la loi fédérale sur la protection constitutionnelle s'appliquent, en particulier ses paragraphes 23 à 26.

## **B. LA TRANSMISSION D'INFORMATIONS**

Outre la constitution de fichiers communs, la BNDG autorise le BND à transmettre, à des fins d'information politique ou de détection précoce des

---

<sup>1</sup> Équivalent de la CNIL.



menaces, des données personnelles désignées dans le cadre de la coopération politique internationale à des services étrangers ou à des organismes supranationaux et intergouvernementaux, s'il existe des indices concrets que cela est nécessaire pour la poursuite d'infractions telles que des infractions prévues par le code pénal (espionnage, menace contre l'État de droit, formation d'associations criminelles ou terroristes, etc.), la loi sur l'asile, la loi sur les armes ou encore la loi sur les nouvelles substances psychoactives<sup>1</sup>.

Le BND peut également transmettre des données à caractère personnel à des fins de détection précoce des menaces, dans le but d'un traitement ultérieur du suivi, dans la mesure où, sur la base de certains faits, il peut être présumé que cela est nécessaire :

- pour éviter un danger touchant des intérêts particulièrement importants ou une atteinte particulièrement grave aux droits des personnes ;
- ou pour la sécurité du *Bund* ou des *Länder*, pour la préservation des intérêts essentiels du *Bund* en matière de politique étrangère ou pour la sécurité de l'État destinataire.

Au-delà des infractions susmentionnées, le BND peut transmettre des informations à caractère personnel à des fins d'information politique s'il existe des indices concrets laissant présager que la transmission est nécessaire pour prévenir un danger imminent pour : le corps, la vie ou la liberté d'une personne ; les biens collectifs essentiels ; ou la sécurité du *Bund*, des *Länder*, d'un État membre de l'Union européenne, de l'AELE ou de l'OTAN.

S'agissant des transmissions d'informations à un pays tiers, elles ne sont par nature pas autorisées, sauf cas exceptionnels et sur autorisation préalable de la Chancellerie.

Le BND collabore avec d'autres services étrangers dans le cadre du renseignement sur les transmissions, et une extension de cette coopération est possible en matière de données à caractère personnel sauf s'il s'agit de ressortissants allemands, d'entités juridiques nationales ou de personnes résidant sur le territoire. La coopération est autorisée à des fins :

- d'identification précoce des dangers importants pour la sécurité intérieure et extérieure de l'Allemagne, la défense ou l'intérêt général, pour pouvoir contrer ces menaces ;
- de maintien de la capacité d'action de l'Allemagne en matière de politique extérieure et de sécurité ;
- et de garantie que les missions du BND, qui seraient considérablement plus compliquées, voire impossibles, sans une telle coopération, sont accomplies.

---

<sup>1</sup> Pour la liste complète, voir le paragraphe 100b du code de procédure pénale allemand [https://www.gesetze-im-internet.de/stpo/\\_100b.html](https://www.gesetze-im-internet.de/stpo/_100b.html)

Les détails de la coopération doivent préalablement avoir été définis par écrit dans une déclaration d'intention entre le BND d'une part, et le service étranger concerné d'autre part. Cette déclaration doit inclure des éléments tels que l'objectif de la coopération, sa durée et une garantie du service étranger que : les données transmises ne seront utilisées que pour répondre à la finalité indiquée et ne seront transmises à des tiers qu'avec l'accord du BND ; toutes les données transmises alors qu'elles n'auraient pas dû (à l'instar des données concernant des ressortissants allemands ou des personnes protégées) seront supprimées ; les données ne seront pas utilisées de façon contraire aux principes de l'État de droit, notamment à des fins de persécution politique ; le service étranger fournira sur demande au BND des informations sur l'utilisation des données ; toute demande de suppression de la part du BND sera suivie d'effet ; le cas échéant, les données de trafic ne seront pas stockées plus de six mois.

La coopération doit viser à obtenir des informations en matière de :

- détection précoce des menaces en matière de terrorisme international ou d'extrémisme violent ou ayant pour but la mise en œuvre planifiée et secrète de convictions politiques, religieuses ou idéologiques ;
- détection précoce des menaces liées à la prolifération illégale d'armes de destruction massive et d'armes de guerre ainsi que le commerce extérieur illicite de marchandises et de services techniques d'importance considérable ;
- protection de l'armée fédérale et des forces armées des partenaires à la coopération ;
- situations de crise à l'étranger et de leurs répercussions ;
- situation des risques et de sécurité des ressortissants allemands et étrangers ;
- opérations politiques, économiques ou militaires à l'étranger, revêtant une importance considérable en matière de politique extérieure et de sécurité ;
- activités de renseignement concernant l'Allemagne ou ses partenaires de coopération ;
- lutte contre la criminalité organisée internationale ;
- création ou obtention de compétences importantes pour le BND ou ses partenaires de coopération ;
- attaques internationales criminelles, terroristes et visant un État au moyen de programmes malveillants contre la confidentialité, l'intégrité et la disponibilité des systèmes d'information ;
- ou toute situation similaire.

La déclaration d'intention nécessite l'approbation de la Chancellerie fédérale si la coopération a lieu avec des services des États membres de l'Union européenne, de l'AELE ou de l'OTAN ; dans tout autre cas, l'accord du directeur de la Chancellerie est requis. La commission de contrôle parlementaire doit être informée de la déclaration d'intention lors de sa réunion suivante. Toute transmission de donnée personnelle dans le cadre d'une coopération doit être enregistrée.

Enfin, s'agissant des relations reposant sur la confidentialité (à l'instar de celles des journalistes et de leurs sources), les mesures visant à collecter des données, à l'insu des personnes concernées, stockées sur des systèmes informatiques étrangers à l'étranger, ne sont *a priori* pas applicables, sauf si la personne concernée est auteur ou participant à une infraction ou que cela est nécessaire pour prévenir un danger sur : le corps, la vie ou la liberté d'une personne ; les biens collectifs essentiels ; ou la sécurité du *Bund*, des *Länder*, d'un État membre de l'Union européenne, de l'AELE ou de l'OTAN. C'est le BND qui, en traitant les données collectées, détermine si elles nécessitent une protection en tant que relation confidentielle ou non. Dans l'hypothèse d'une relation confidentielle, les données ne peuvent être utilisées que si elles répondent aux exceptions d'application ; dans le cas contraire, elles doivent être supprimées. La décision permettant au BND de juger quelles relations relèvent de la catégorie des relations confidentielles et quelles relations n'en relèvent pas, doit être documentée.



## **CHAPITRE III : L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT EN 2020 ET EN 2021**

En application de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, la délégation parlementaire au renseignement est destinataire d'un rapport annuel d'activité des services spécialisés de renseignement, incluant une synthèse des crédits qui leur sont consacrés. Ce rapport lui a été transmis par la Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT), tardivement, le 11 janvier 2022 au titre de l'année 2020.

Ce document souligne les enjeux d'actualité liés à la politique publique du renseignement, et présente plusieurs indicateurs sur l'activité des services et les ressources qui leur sont allouées. Les développements ci-après sont fondés sur les données contenues dans ce rapport annuel, ainsi que sur les données contenues dans une version intermédiaire du rapport d'activité 2021, transmise par la CNRLT le 16 mai 2022 (la version définitive ne sera finalisée qu'après la publication du présent rapport d'activité de la DPR).

### **I. LES ENJEUX D'ACTUALITÉ LIÉS A LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT**

#### ***A. LES CONSÉQUENCES DE LA CRISE SANITAIRE SUR L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT***

L'année 2020 a été marquée par la crise sanitaire qui a eu des incidences sur l'organisation des services – avec deux périodes de confinement – et l'orientation du travail de renseignement. Les services ont été contraints de prioriser leurs activités.

La plupart d'entre eux ont pu s'appuyer sur un plan de continuité d'activité (PCA) reposant le plus souvent sur une identification des missions prioritaires. Du fait de la spécificité des missions, le recours au télétravail est resté marginal ;\*\*\*\*\*.

\*\*\*\*\*

Par ailleurs, la crise sanitaire a réorienté les actions de recherches :

\*\*\*\*\*.

\*\*\*\*\*

Enfin, cette crise a conduit certains services de renseignement à s'engager dans de nouvelles démarches innovantes : \*\*\*\*\*.

## ***B. LES MENACES PRÉPONDÉRANTES DEPUIS 2020***

Trois thématiques prépondérantes se sont dégagées au cours de l'année 2020 : la lutte antiterroriste, les ingérences étrangères et les menaces hybrides.

### **1. La lutte antiterroriste**

La France est confrontée à la fois à une menace endogène et à la résurgence d'une menace exogène.

En 2020, six attentats ont été commis sur le sol français et 40 % des techniques de renseignement autorisées ont concerné la finalité 4 (prévention du terrorisme). Quatre de ces six attentats ont pour auteurs des ressortissants étrangers. L'identification et le suivi des combattants terroristes étrangers évoluant toujours en zone syro-irakienne, constitue l'une des priorités des services de renseignement ; l'objectif commun à tous les pays européens est de prévenir leur entrée dans l'espace Schengen.

En 2020, la France a pris à sa charge près du tiers des signalements au Système d'information Schengen (SIS). \*\*\*\*\*

Enfin, une attention particulière est portée aux personnes radicalisées atteintes de troubles psychiatriques, trois des six auteurs d'attentats en 2020 étant sujets à des troubles avérés du comportement. \*\*\*\*\*. Sur le plan organisationnel, un travail d'identification et de partage de bonnes pratiques s'est développé entre les agences régionales de santé (ARS) et les préfetures, à travers la saisine des cellules de prévention de la radicalisation et d'accompagnement des familles (CPRAF).

### **2. Les ingérences étrangères**

En 2020, les risques d'ingérence et les actions d'influence étrangères se sont accrus, nonobstant les effets liés à la crise sanitaire.

\*\*\*\*\*. Outre les sphères traditionnelles que sont la défense et la recherche scientifique, l'ingérence concerne également les champs politique et économique. \*\*\*\*\*

\*\*\*\*\*

### 3. Les menaces hybrides

Depuis l'été 2019, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) préside un groupe de travail interministériel sur les menaces hybrides. Cette notion renvoie aux différentes activités coercitives compromettant la sécurité, mêlant des méthodes conventionnelles et non conventionnelles, qui peuvent être diplomatiques, militaires, économiques ou techniques.

**Pour prévenir au mieux ces multiples menaces, la période récente a été marquée par un renforcement du travail interservices, plus particulièrement autour des sujets suivants :**

- le renforcement de la coopération en matière de **contre-espionnage** ;
- dans le domaine technique, l'accélération des mutualisations et la poursuite de **l'interconnexion interservices** ; \*\*\*\*\* ;
- **l'approfondissement de travaux menés en commun sur des aires géographiques** \*\*\*\*\*.

### 4. Les sujets d'intérêt de l'année 2021

Au cours de l'année 2021, l'orientation de la politique publique du renseignement a porté plus spécifiquement sur :

- \*\*\*\*\* ;
- \*\*\*\*\* ;
- la préparation de la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement ;
- les nouveaux mécanismes de pilotage issus de la refonte du PNOR.

#### ***C. LE DÉVELOPPEMENT DE NOMBREUX LEVIERS DE COOPÉRATION AU SEIN DE LA COMMUNAUTÉ DU RENSEIGNEMENT***

Au cours de l'année 2020, les coopérations interservices se sont maintenues en distanciel, malgré la pandémie, \*\*\*\*\*.

Les coopérations opérationnelles thématiques se sont poursuivies à un rythme soutenu en dépit du contexte sanitaire, et se sont déployées en cohérence avec les finalités du Plan national d'orientation du renseignement (PNOR). Elles concernent les sujets suivants :

- **l'indépendance nationale et l'intégrité du territoire**, \*\*\*\*\*.
- L'année 2020 a été marquée par la création de nouveaux espaces d'échanges \*\*\*\*\* ;

– **la cyberdéfense.** Alors que l’année 2020 a confirmé la montée en puissance des actions cyber-offensives par des acteurs étatiques et non étatiques, un mécanisme interministériel a été mis en place \*\*\*\*\* ;

– **les intérêts majeurs de la politique étrangère et l’exécution des engagements européens,** \*\*\*\*\* ;

– **la prévention de toute forme d’ingérence étrangère,** \*\*\*\*\* ;

– **la défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France,** \*\*\*\*\* ;

– **la prévention du terrorisme,** \*\*\*\*\* ;

– **la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et de violences collectives,** \*\*\*\*\*. Après avoir pris une place importante dans l’activité des services de renseignement relevant du ministère de l’intérieur avec le mouvement des Gilets jaunes en 2019, cette thématique s’est révélée moins prégnante en 2020 en raison de la crise sanitaire, laquelle a eu une incidence directe sur l’organisation de mouvements de contestation. Pour autant, la volonté de coopération sur cette finalité demeure forte \*\*\*\*\* ;

– **la prévention de la criminalité ou de la délinquance organisée,** \*\*\*\*\* ;

– **la prévention de la prolifération des armes de destruction massive,** \*\*\*\*\*. Les organes d’échange et de coopération en la matière se sont développés et adaptés au contexte international. \*\*\*\*\* ;

– \*\*\*\*\* ;

– enfin, \*\*\*\*\*.

#### ***D. LA PRISE EN COMPTE DE LA DIMENSION EUROPÉENNE DE L’ACTIVITÉ DE RENSEIGNEMENT, EN AMONT DE LA PRÉSIDENTE FRANÇAISE DE L’UNION EUROPÉENNE***

À la suite du discours de la Sorbonne du 26 septembre 2017 (« Initiative pour l’Europe » du Président de la République), est né le Collège du renseignement en Europe. Inauguré le 5 mars 2019 par le Président de la République Emmanuel Macron, une lettre d’intention en date du 26 février 2020, signée par vingt-trois pays à Zagreb, a explicité la vision, les missions et la gouvernance du Collège (structure intergouvernementale), dont les activités se déclinent autour de trois axes : l’organisation de séminaires thématiques ; des actions de sensibilisation à l’attention d’acteurs extérieurs au renseignement ; un programme académique spécialisé au bénéfice des professionnels du renseignement.



Dans la perspective de la présidence française de l'Union européenne du premier semestre 2022, les services de renseignement ont indiqué être intéressés par les besoins en renseignement d'intérêt européen émanant des utilisateurs finaux, pour définir des orientations.

L'appareil diplomatique de la France a été sensibilisé aux activités des services qui concernent l'Europe. \*\*\*\*\*.

## II. LE BILAN STATISTIQUE DE L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT AU COURS DE L'ANNEE 2020

### A. LES DONNÉES RELATIVES À L'AIDE À LA DÉCISION

L'aide à la décision vise à apporter aux hautes autorités de l'Etat une information fiable sur les menaces et les risques dont l'effet serait significatif sur le territoire, la population ou les institutions, ainsi qu'un éclairage sur la situation d'ensemble du pays en vue de faciliter la conduite de la politique nationale. Elle prend généralement la forme d'un document de synthèse qui permet de prendre connaissance des renseignements recueillis par les services :

— **14 802 notes ont été produites en 2020** par les services spécialisés de renseignement, soit une légère baisse par rapport à 2019 (15 123), et une augmentation par rapport à 2018 (13 607) ;

— **6 962 dossiers thématiques**, plus exhaustifs, ont été produits en 2020 (contre 5 390 en 2019).

La production écrite totale des services spécialisés est ainsi en **progression de 6,1 %** en un an.

\*\*\*\*\*

**45 % de la production écrite ont concerné les finalités 1** (indépendance nationale, intégrité du territoire et défense nationale) **et 2** (intérêts majeurs de la politique étrangère, exécution des engagements internationaux de la France et prévention de toute forme d'ingérence étrangère). La finalité 4 (prévention du terrorisme) est en légère progression, à 20 % (+ 2 %), tandis que la production relative à la protection des intérêts économiques, industriels et scientifiques majeurs poursuit sa progression à 22 % (+ 3 %).

**S'agissant des services de renseignement n'appartenant pas au premier cercle, leur production écrite accuse une baisse de 13 % en 2020** avec 114 705 notes et dossiers thématiques (contre 131 866 en 2019) ; cette baisse s'explique, pour partie, par les deux périodes de confinement. \*\*\*\*\*.

Le coordonnateur national du renseignement et de la lutte contre le terrorisme transmet au Président de la République et au Premier ministre les

renseignements devant être portés à leur connaissance, notamment au travers d'un « **Bulletin quotidien du renseignement** ». En 2020, la part consacrée aux sujets de défense des intérêts majeurs de la politique étrangère et des engagements internationaux, et de défense des intérêts économiques, industriels et scientifiques majeurs, a progressé jusqu'à atteindre 54 %, alors que la part relative à la prévention du terrorisme est passée de 16 % en 2019 à 12 % en 2020. Il est également à noter une **très forte hausse des renseignements relatifs à la prévention des ingérences étrangères qui ont été transmis (+ 144 %)**.

À partir de 2021, une nouvelle typologie des notes a été mise en place afin d'harmoniser les diffusions des services de renseignement du premier cercle, rendant inopérantes les comparaisons avec les données des années précédentes.

Cette nouvelle typologie, en vigueur à compter de 2021, est la suivante :

— **note de renseignement** : transmettre un ou plusieurs renseignements nouveaux, exploités et analysés ;

— **note de réaction** : expertiser une information récente et médiatisée, susceptible de faire réagir les autorités ;

— **note d'évaluation** : fournir une synthèse et une analyse de renseignements sur une thématique, un pays, une zone géographique, afin d'évaluer une situation présente par rapport au passé et, éventuellement, apporter une expertise sur son évolution à venir ;

— **note profil** : fournir une synthèse de renseignements et une appréciation sur une personne physique ou morale susceptibles d'intéresser les autorités ;

— **capsule** : fournir un instantané quotidien des nouveaux renseignements (bruts ou élaborés) susceptibles d'intéresser les hautes autorités.

Ce changement de périmètre a un impact sur le nombre de productions, comme en attestent les statistiques suivantes :

**PRODUCTIONS ÉCRITES DES SERVICES SPÉCIALISÉS DU PREMIER CERCLE,  
PAR NATURE**

	2017	2018	2019	2020	2021
<b>Notes de renseignement</b>	10 032	7 639	8 729	9 421	7 072
<b>Notes de réaction</b>	1 379	209	242	156	331
<b>Notes d'évaluation</b>	9 253	8 573	7 330	8 592	1 515
<b>Notes profil</b>	494	403	383	246	311
<b>Capsules</b>	0	0	0	0	4 026
<b>Autres notes</b>	25	2 315	2 348	2 198	4 201
<b>Total</b>	<b>21 183</b>	<b>19 139</b>	<b>19 032</b>	<b>20 613</b>	<b>17 456</b>

**PRODUCTIONS ÉCRITES DES SERVICES DU SECOND CERCLE, PAR NATURE**

	2017	2018	2019	2020	2021
<b>Notes de renseignement</b>	4 834	6 924	5 488	52 050	39 089
<b>Notes de réaction</b>	4 247	4 840	3 418	4 311	119
<b>Notes d'évaluation</b>	59 323	60 535	55 056	1 846	34
<b>Notes profil</b>	424	1 619	1 034	1 254	1 529
<b>Capsules</b>	0	0	0	0	1
<b>Autres notes</b>	0	561	3 955	3 274	1 122
<b>Total</b>	<b>68 828</b>	<b>74 479</b>	<b>68 951</b>	<b>62 735</b>	<b>41 894</b>

La répartition de ces productions écrites par thèmes fait apparaître qu'au cours de l'année 2021, les services spécialisés du premier cercle ont concentré leur activité de façon équivalente sur quatre thématiques que sont : la lutte contre le terrorisme, l'anticipation des crises et des risques de ruptures majeures, la défense et la promotion de l'économie et des technologies, et la lutte contre les menaces transversales.

Quant aux services du second cercle, ils sont, sans surprise, moins concernés par la lutte contre les menaces transversales.

***B. LES DONNÉES RELATIVES À LA PRÉVENTION ET À LA RÉDUCTION  
DES VULNÉRABILITÉS***

La prévention et la réduction des vulnérabilités recouvrent une large gamme d'activités qui peuvent se répartir entre les activités d'enquête, les activités de sensibilisation et les activités de signalement des vulnérabilités

détectées aux autorités administratives, judiciaires voire internationales compétentes.

\*\*\*\*\*

### **C. LES DONNÉES RELATIVES À L'ENTRAVE ET LA NEUTRALISATION DES MENACES**

L'entrave et la neutralisation des menaces ont pour objet de faire cesser des situations dont l'existence fait peser une menace ou un risque manifeste et susceptible d'avoir un effet significatif sur le territoire ou les institutions du pays – y compris à l'étranger –, ou sur nos intérêts.

Aux fins d'entrave et de neutralisation des menaces, les services spécialisés de renseignement disposent d'un large éventail d'instruments à caractère administratif ou judiciaire, qui touchent aux personnes, aux lieux, aux biens et aux fonds.

En 2020, \*\*\*\*\*

\*\*\*\*\*

Deux outils ont particulièrement été utilisés : les demandes d'interdictions administratives de territoire (\*\*\*\*\*) et les propositions de gels d'avoir (\*\*\*\*\*)).

Comme en 2019, la prévention du terrorisme concentre la majeure partie des activités d'entrave et de neutralisation dont la part a continué d'augmenter, \*\*\*\*\*.

S'agissant des mesures à caractère judiciaire, la DGSI est le seul service spécialisé disposant d'une compétence judiciaire : \*\*\*\*\*.

**S'agissant des services du second cercle, les activités d'entrave et de neutralisation ont fléchi \*\*\*\*\*, du fait de l'instauration de l'état d'urgence sanitaire** qui a restreint, selon les périodes, les déplacements des personnes, et a rétabli des contrôles aux frontières. En revanche, grâce à une meilleure fluidité des échanges avec le juge des libertés et de la détention, les services ont pu utiliser avec plus d'efficacité la visite de lieux privés (\*\*\*\*\*) et la saisie de biens (\*\*\*\*\*). Les propositions de fermeture administrative ont également progressé d'un tiers.

\*\*\*\*\*

### III. LE HAUT NIVEAU DE RESSOURCES ACCORDÉES AUX SERVICES DE RENSEIGNEMENT CONFIRME LA PRIORITÉ DONNÉE A LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

#### A. DES RESSOURCES BUDGÉTAIRES QUI SE STABILISENT À UN NIVEAU ÉLEVÉ

##### 1. Les crédits en fonds normaux

S'agissant des fonds normaux, **14 programmes budgétaires** contribuent au financement de la politique publique du renseignement, répartis dans 6 missions : direction de l'action du Gouvernement ; défense ; sécurités ; administration générale et territoriale de l'État ; gestion des finances publiques ; justice.

\*\*\*\*\*

En exécution budgétaire, **l'enveloppe totale des crédits en fonds normaux consacrés au renseignement s'est établie, en 2020, à 2,853 milliards d'euros, soit une hausse de 4,9 % par rapport à 2019, mais s'est légèrement rétractée à 2,745 milliards d'euros en 2021.** En 2017, l'exécution budgétaire était de 2,397 milliards d'euros, soit un différentiel de 348 millions d'euros sur le quinquennat.

Les dépenses engagées en fonds normaux par les services spécialisés du premier cercle, se sont élevées à 1,816 milliard d'euros en 2021, en légère baisse par rapport à l'année précédente (1,85 milliard d'euros). Cependant, le niveau de dépenses est en augmentation de 363 millions d'euros par rapport à l'exercice budgétaire 2017.

Les dépenses de personnel demeurent le premier poste budgétaire (55 %), mais leur croissance se stabilise en 2020. Les dépenses d'intervention sont, quant à elles, en forte hausse (+ 53,5 %).

##### 2. Les crédits en fonds spéciaux

\*\*\*\*\*

Il convient de distinguer les ressources totales disponibles en fonds spéciaux, des ressources perçues au cours de l'exercice qui correspondent à la dotation inscrite en loi de finances initiale, complétée le cas échéant par des abondements en cours d'exercice (décrets de transfert, DDAI). \*\*\*\*\*

\*\*\*\*\*

## **B. LA MISE EN ŒUVRE PROGRESSIVE D'UNE POLITIQUE DE RESSOURCES HUMAINES CONSACRÉE À LA FILIÈRE DU RENSEIGNEMENT**

Créé en 2018, le Comité des ressources humaines des services de renseignement (CRHSR) a vu l'un de ses chantiers majeurs aboutir en 2020, à savoir l'élaboration du **répertoire interministériel des emplois du renseignement (RIER)** dont l'objectif est de développer une approche par compétences et de favoriser la mobilité interservices. Le RIER s'apparente à une cartographie des métiers emblématiques et spécifiques du monde du renseignement, structuré autour de **quatre filières professionnelles** : renseignement d'origine humaine ; renseignement d'origine technique ; entrave ; appui. Il est constitué de 29 fiches présentant chacune un emploi-référence.

En 2021, les effectifs des services de renseignement (premier et second cercles) s'élevaient à **20 266 agents**, soit une augmentation de 10 % depuis 2017. Les effectifs sont stables par rapport à l'année 2020, dans un contexte marqué par des difficultés de recrutement et de fidélisation des agents.

### **RESSOURCES HUMAINES PAR SERVICE**

*Nombre d'agents au 31 décembre de l'exercice*

*Tableau \*\*\*\*\**

La DGSE, la DGSi et le SCRT concentrent à eux trois plus de 70 % des effectifs.

Alors qu'en 2021 les effectifs de la DGSE, de la DRM et de la DNRED étaient en légère baisse, Tracfin, la DGSi et la DRSD ont enregistré une hausse du nombre de leurs agents.

**Le nombre d'agents civils contractuels a continué de croître en 2021**, passant de \*\*\*\*\* agents en 2017, à \*\*\*\*\* agents en 2021. Les contractuels sont beaucoup plus nombreux dans les services du premier cercle (\*\*\*\*\*) que dans ceux du second cercle (\*\*\*\*\*) .

35,9 % des agents des services de renseignement sont des agents de catégorie A, 51,4 % des agents de catégorie B et 12,7 % de catégorie C. Au sein du premier cercle, la part des agents de catégorie A continue de croître tandis que la prépondérance des agents de catégorie B demeure très nette dans les services du second cercle.

**Les femmes représentent environ 30 % des effectifs** ; si leur nombre a progressé ces dernières années, le taux de féminisation n'a cependant pas évolué de façon significative (+ 1,7 % en 5 ans), le nombre d'hommes ayant lui aussi augmenté à la faveur de la montée en puissance des effectifs.

S'agissant de la pyramide des âges, **la catégorie des 35-50 ans est prépondérante (52,7 %)**. Pour la première fois, la part des agents de moins de 35 ans a très légèrement diminué en 2020, après une période de hausse continue.

62 % des effectifs ont une ancienneté de moins de 6 ans dans leur service. **Mais la question de la fidélisation est plus prégnante au sein des services du second cercle** où 90,4 % des agents ont une ancienneté inférieure à 6 ans, et seulement 5,7 % supérieure à 12 ans.

**L'analyse des flux révèle un ralentissement du flux entrant (+ 4,7 %) et une augmentation du flux sortant (+ 18,3 %)**. Cette hausse des départs appelle une attention particulière car elle souligne une difficulté de fidélisation des agents et pourrait, à terme, induire une perte de savoir-faire pour les services.

**Les départs pour motif de sécurité (perte d'habilitation) sont en forte hausse pour l'ensemble des services : ils atteignent 44 départs en 2020, contre 19 en 2019.** Ce phénomène est à mettre en lien avec le renforcement des procédures de sécurité mises en place pour les recrutements, à la suite de l'attaque terroriste survenue à la DRPP en octobre 2019.

Le turn-over s'établit désormais à 11 % pour l'ensemble de l'appareil de renseignement.

S'agissant de la **mobilité interservices**, elle a concerné 145 personnels en 2020, ce qui représente une progression significative et continue depuis 2018 (49 agents concernés) et 2019 (94 agents). Ce type de mobilité interservices est essentiellement l'apanage du premier cercle.

Les indicateurs relatifs à la formation des ressources humaines indiquent qu'en 2020, 17 381 journées de formation ont bénéficié à 9 023 agents relevant des services du premier cercle. Après une progression constante, l'accès à la formation a marqué le pas en 2020, s'élevant à seulement 62 %, soit une baisse de 14,2 % ; cette situation s'explique par une difficulté à organiser des formations lorsque des contraintes sanitaires sont en vigueur. Au cours de l'exercice 2020, 22 actions de formation ont été menées par l'Académie du renseignement, contre 31 en 2019 ; l'évolution est, là aussi, la conséquence directe des restrictions sanitaires. En revanche, l'ouverture des formations de l'Académie du renseignement aux agents du second cercle s'est maintenue en 2020, représentant 20,2 % des participants, soit une proportion similaire à celle constatée en 2019.

### ***C. UN RECOURS AUX RESSOURCES TECHNIQUES À INTERPRÉTER À LA LUMIÈRE DE LA CRISE SANITAIRE***

**Une très nette augmentation des demandes d'identification** au titre de l'article L. 851-1 alinéa 2 du code de la sécurité intérieure (+ 45 %) a été

constatée en 2020, même si la comparaison avec l'année 2019 doit être relativisée si l'on tient compte des années précédentes.

\*\*\*\*\*

En 2020, le nombre de demandes de mise en œuvre d'une technique de recueil de renseignements (hors techniques prévues aux articles L. 851-2 et L. 851-3 du code de la sécurité intérieure), soumise à autorisation sur le territoire national, est **en recul, pour la première fois depuis 2017** (- 12 %). La **chute du nombre de demandes d'introduction dans un lieu privé** est également à relever (2 021, contre 3 599 l'année précédente, soit une baisse de 43,8 %), de même que pour la technique de captation d'images (- 64 %) qui fait généralement l'objet d'une demande d'introduction dans un lieu privé.

\*\*\*\*\*

Seule la technique de géolocalisation en temps réel a connu une croissance sensible (+ 10 %), toutefois moins élevée que les années précédentes (+ 46 % en 2019, par exemple).

S'agissant des demandes d'autorisation d'exploitation des communications ou des seules données de connexion, interceptées dans le cadre des mesures de surveillance des communications électroniques internationales, elles sont en nette augmentation : 4 324 demandes d'autorisation d'exploitation en 2020, soit + 103 % par rapport à 2019. La hausse se justifie par la nouvelle possibilité offerte par le code de la sécurité intérieure (CSI) d'autoriser l'exploitation de communications ou des données de connexion de numéros d'abonnement ou d'identifiants rattachables au territoire national, dont l'utilisateur communique depuis ce territoire (environ 70 % des demandes).

\*\*\*\*\*

L'analyse par finalité souligne la **prédominance de la finalité 4** (prévention du terrorisme) totalisant 15 817 demandes, soit 42 % du total (contre 30 % en 2019). La finalité 3 (intérêts économiques, industriels et scientifiques majeurs de la France) a subi une baisse très importante (- 62 %)

\*\*\*\*\*



**RÉPARTITION DES TECHNIQUES DE RENSEIGNEMENT PAR FINALITÉ DU CSI**  
(tous services confondus)

	2020	2021
<b>Finalité 1 :</b> Indépendance nationale, intégrité du territoire et défense nationale	822	1 761
<b>Finalité 2 :</b> Intérêts majeurs de la politique étrangère et engagements internationaux	6 044	7 184
<b>Finalité 3 :</b> Intérêts économiques, industriels et scientifiques majeurs	3 083	4 122
<b>Finalité 4 :</b> Prévention du terrorisme	15 817	16 043
<b>Finalité 5a :</b> Prévention des atteintes à la forme républicaine des institutions	16	9
<b>Finalité 5b :</b> Prévention des reconstitutions de groupements dissous	15	75
<b>Finalité 5c :</b> Prévention des violences collectives	5 340	6 044
<b>Finalité 6 :</b> Prévention de la criminalité et de la délinquance organisées	5 415	6 526
<b>Finalité 7 :</b> Lutte contre la prolifération des armes de destruction massive	677	812
<b>Finalité art. L. 855-1 CSI :</b> Sécurité pénitentiaire & prévention des évasions	15	43
<b>TOTAL</b>	<b>37 244</b>	<b>42 619</b>

Enfin, les services de renseignement ont recours à d'autres formes de recueil de renseignements qui ne sont pas soumises à une régime juridique d'autorisation préalable, qu'il s'agisse du renseignement humain, opérationnel (filatures, surveillances), en sources ouvertes, partenarial, ou technique (électromagnétique, cybernétique, etc.). Les sources ouvertes constituent aujourd'hui une base d'informations déterminante pour les services de renseignement, \*\*\*\*\*. De même, la plateforme Pharos a connu une forte croissance du nombre de signalements au lendemain de l'attentat commis contre Samuel Paty le 16 octobre 2020.



## **CHAPITRE IV : LE RAPPORT GÉNÉRAL DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX SUR L'EXERCICE 2020**

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 cours de l'année 2021, sa composition était la suivante :

- M. Loïc Kervran, député (Agir ensemble) du Cher, président ;
- Mme Agnès Canayer, sénateur (Les Républicains) de la Seine-Maritime ;
- M. Claude de Ganay, député (Les Républicains) du Loiret ;
- M. Yannick Vaugrenard, sénateur (Socialiste, Écologiste et Républicain) 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. De mai à décembre 2021, elle a procédé à 23 déplacements au cours desquels elle s'est rendue :

- au Groupement interministériel de contrôle (GIC) les 26 mai et 19 novembre 2021 ;
- à la Direction du renseignement et de la sécurité de la défense (DRSD) le 23 juin 2021 ;
- à la Direction générale de la sécurité intérieure (DGSI) les 30 juin et 15 novembre 2021, ainsi qu'à la direction zonale de Lyon le 8 décembre 2021 ;
- à la Direction du renseignement militaire (DRM) les 1<sup>er</sup> juillet, 7 juillet, et 17 septembre 2021 ;
- à Tracfin le 8 juillet 2021 ;
- au Service national du renseignement pénitentiaire (SNRP) le 8 juillet 2021 ;

— à la Direction nationale du renseignement et des enquêtes douanières (DNRED) le 21 juillet et le 9 décembre 2021 ;

— à la Direction générale de la sécurité extérieure (DGSE) les 22 septembre, 1<sup>er</sup>, 4, 8, 15, 22 et 28 octobre, le 30 novembre et le 7 décembre 2021 ;

— à la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) le 8 décembre 2021.

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

## I. PRESENTATION GENERALE DES FONDS SPECIAUX EN 2020

### A. DES RESSOURCES STABLES

Les services spécialisés de renseignement et le GIC ont disposé, en 2020, d'un montant total de ressources en fonds spéciaux de \*\*\*\*\*, similaire à celui de 2019.

La CVFS se félicite de l'augmentation des fonds spéciaux inscrits, en loi de finance initiale, au programme 129 « Coordination du travail gouvernemental ». En effet, la commission avait, à plusieurs reprises, invité les services du Premier ministre à relever le niveau de ces crédits pour mettre fin à une insincérité budgétaire chronique, qui se traduisait par le versement régulier de décrets de transfert et de décrets pour dépenses accidentelles et imprévisibles (DDAI) au titre de projets pluriannuels pour lesquels les dépenses sont prévisibles.

Même si des décrets de transferts continuent d'être accordés \*\*\*\*\*, la commission salue le non recours à des DDAI en 2020, témoignant d'un effort de sincérité tenant compte des besoins réels et de l'évolution de l'activité opérationnelle des services.

### RESSOURCES EN FONDS SPÉCIAUX - ÉVOLUTION 2019/2020 (EN M€)

*Tableau \*\*\*\*\**

Si l'enveloppe globale est stable, \*\*\*\*\*.

Les trois services les plus consommateurs en fonds spéciaux (\*\*\*\*\*), concentrent près de 97 % du montant total de la dotation annuelle, tandis que la montée en puissance des plus « petits » services se confirme, \*\*\*\*\*.

## **B. UNE REDUCTION DES DEPENSES DANS UN CONTEXTE DE CRISE SANITAIRE**

Pour la deuxième année consécutive, le niveau des dépenses poursuit sa baisse \*\*\*\*\*.

Plusieurs raisons expliquent cette baisse, à commencer par la pandémie de Covid-19 qui a impacté l'activité des services de renseignement, \*\*\*\*\*.

Si le volume de la baisse globale des dépenses résulte pour l'essentiel des deux plus gros services \*\*\*\*\*, d'autres services poursuivent, à une échelle différente, leur montée en puissance s'agissant du recours aux fonds spéciaux : \*\*\*\*\*.

### **ÉVOLUTION DES DÉPENSES EN FONDS SPÉCIAUX (EN M€)**

*Tableau \*\*\*\*\**

### **RÉSULTAT D'EXERCICE PAR SERVICE (EN €)**

*Tableau \*\*\*\*\**

En 2020, comme pour les années précédentes, **les dépenses en fonds spéciaux n'ont pas été intégralement couvertes par le montant de la dotation annuelle**. Le déficit constaté en fin d'exercice est toutefois inférieur à l'exercice précédent, \*\*\*\*\*.

\*\*\*\*\*

### **TRÉSORERIE DE L'EXERCICE 2017 À L'EXERCICE 2020 (EN M€)**

*Tableau \*\*\*\*\**

S'agissant de la trésorerie en fonds spéciaux des différents services de renseignement et du GIC, celle-ci s'est établie à la fin de l'année 2020 quasiment au même niveau que l'année précédente, à près de \*\*\*\*\*, ce qui, au total, représente près d'une année de dotation en fonds spéciaux. Il faut toutefois distinguer la trésorerie gagée, en baisse significative \*\*\*\*\*, de la trésorerie disponible qui, elle, progresse \*\*\*\*\*. La trésorerie immobilisée progresse également \*\*\*\*\*.

### **C. LA NATURE DES DEPENSES**

L'analyse par agrégats des dépenses en fonds spéciaux confirme \*\*\*\*\*.

#### **DÉPENSES PAR AGRÉGATS (EN €)**

*Tableau \*\*\*\*\**

## **II. LES OBSERVATIONS COMMUNES A L'ENSEMBLE DES SERVICES**

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

S'il existe des spécificités propres à chaque structure, il n'en demeure pas moins que des réflexions et des problématiques communes conduisent la commission à formuler un certain nombre d'observations générales issues des contrôles sur place et sur pièces effectués au titre du contrôle sur l'exercice 2020.

La commission salue des progrès sur plusieurs sujets, s'agissant notamment de la montée en puissance et de la maturité des procédures de contrôle interne. La commission a ainsi été informée d'enquêtes internes diligentées à la suite d'incidents intervenus \*\*\*\*\*. Dans un précédent rapport, la commission avait souhaité être systématiquement informée de ces situations, ce qui en l'espèce a été le cas.

Des évolutions positives sont également constatées s'agissant \*\*\*\*\* de la diffusion de plus en plus large d'une culture des fonds spéciaux au sein des services de renseignement, à l'échelon central comme dans les implantations territoriales et dans nos postes à l'étranger.

Pour autant, les contrôles réalisés sur place et sur pièces soulignent l'existence de marges de progression et conduisent la commission à formuler plusieurs observations.

### **A. LA PERSISTANCE D'ENTORSES A LA DOCTRINE D'EMPLOI DES FONDS SPECIAUX**

Constatant des pratiques hétérogènes d'un service à l'autre, la commission réitère la nécessité de clarifier la doctrine d'emploi des fonds spéciaux, qui doit toujours respecter deux critères consubstantiels : la confidentialité et/ou l'urgence opérationnelle.

Or, la commission a observé lors de ses contrôles que des dépenses d'une nature pourtant similaire avaient pu être effectuées en fonds normaux dans un service et en fonds spéciaux dans un autre. C'est notamment le cas de l'achat d'un logiciel \*\*\*\*\*. En l'espèce, s'il peut exister une marge d'interprétation pour décider ou non du recours aux fonds spéciaux, la CNRLT pourrait utilement s'assurer de la cohérence et du bien-fondé du recours aux fonds spéciaux pour l'acquisition de logiciels.

**Recommandation générale n° 1 (à l'attention de la CNRLT) : Au vu de pratiques différentes d'un service à l'autre, s'assurer de la cohérence et du bien-fondé du recours aux fonds spéciaux pour l'acquisition de logiciels.**

Plus problématique encore : la pratique de dépenses en fonds spéciaux sans aucun lien, ni direct ni indirect, avec leur doctrine d'emploi. Il en est ainsi, par exemple, de l'achat en fonds spéciaux \*\*\*\*\* ; des entorses manifestes à la doctrine d'emploi des fonds spéciaux qui appellent un remboursement de la dépense en fonds normaux.

La commission a également relevé des anomalies quant à l'exigence d'anonymisation liée à l'usage des fonds spéciaux, \*\*\*\*\*.

De façon plus générale, la CVFS met également en garde les bénéficiaires de fonds spéciaux contre toute interprétation extensive du critère d'urgence opérationnelle ou tentation d'utiliser les fonds spéciaux pour se dispenser de procédures internes trop lentes et trop contraignantes.

**Recommandation générale n° 2 : En lien avec la CNRLT, établir dans chaque service une procédure interne permettant de caractériser l'urgence opérationnelle sur la base d'éléments factuels (date de la demande, délais de procédure, etc.).**

## **B. DES OBSTACLES A L'EXIGENCE DE DEMARQUAGE ET D'ANONYMISATION**

Bien que des progrès aient été réalisés ces dernières années, la plupart des services de renseignement restent confrontés à \*\*\*\*\*. Or, la raison d'être du recours aux fonds spéciaux est précisément d'éviter la traçabilité des dépenses.

À l'occasion de ses contrôles, la commission a relevé plusieurs cas de figure :

- \*\*\*\*\* ;
- \*\*\*\*\* ;
- \*\*\*\*\* .

Face à ces difficultés, la CNRLT pourrait utilement constituer un groupe de travail interservices pour \*\*\*\*\*.

**Recommandation générale n° 3 (à l'attention de la CNRLT) :  
Constituer un groupe de travail interservices chargé de \*\*\*\*\*.**

**C. LA NECESSITE D'INVENTORIER LES MATERIELS ACQUIS EN FONDS SPECIAUX**

Les dépenses en fonds spéciaux liées à l'acquisition de matériels démarqués progressent \*\*\*\*\*.

La commission souligne la nécessité pour les services de renseignement de systématiser la mise en place, \*\*\*\*\*, d'un inventaire de ces matériels, depuis leur acquisition jusqu'à leur éventuelle cession ou destruction. Il est en effet essentiel de pouvoir disposer d'un inventaire exhaustif du matériel acquis par le service et de s'assurer du démarquage des dépenses liées au maintien en condition opérationnelle desdits matériels.

**Recommandation générale n° 4 : Mettre en œuvre, dans chaque service, un inventaire des matériels acquis en fonds spéciaux, \*\*\*\*\*.**

**D. METTRE FIN AUX ANGLES MORTS DU CONTRÔLE DE LA CVFS**

À plusieurs reprises au cours de ses contrôles, la CVFS s'est vue opposer une fin de non-recevoir à l'exercice de ses missions. \*\*\*\*\* :

– d'une part, \*\*\*\*\* ;

– d'autre part, \*\*\*\*\*. Or, la commission, dont les membres sont habilités au niveau « Très secret », ne saurait se voir opposer une quelconque limitation à l'exercice de leur mission qui concerne le contrôle sur la totalité des dépenses effectuées en fonds spéciaux.

**E. POURSUIVRE LE MOUVEMENT DE BASCULEMENT DE FONDS SPÉCIAUX EN FONDS NORMAUX**

\*\*\*\*\* ont initié ces dernières années d'importants mouvements de basculement en fonds normaux de certaines dépenses jusqu'alors engagées en fonds spéciaux. \*\*\*\*\*.

Jusqu'à présent, ces transferts de fonds spéciaux vers les fonds normaux se sont toujours faits à fonds normaux constants, sans revalorisation des crédits budgétaires alloués aux services, alors que les sommes en question deviennent, au fil des années, de plus en plus significatives : \*\*\*\*\*.

Afin que le processus de basculement de fonds spéciaux vers les fonds normaux puisse se poursuivre et s'achever dans de bonnes conditions, il est souhaitable que celui-ci s'accompagne d'une revalorisation à due



proportion des crédits budgétaires alloués aux services et structures concernés.

**Recommandation générale n° 5 : Accompagner le processus en cours de basculement de fonds spéciaux vers les fonds normaux d'une revalorisation à due proportion des crédits budgétaires alloués aux services et structures concernés.**

#### **F. HARMONISER LES DONNEES COMPTABLES ET BUDGETAIRES TRANSMISES A LA CVFS**

Dans son dernier rapport portant sur l'exercice 2019, la commission avait relevé une difficulté liée à la fiabilité des données comptables et budgétaires qui lui sont transmises soit par les services, soit par la CNRLT.

Cette année encore, la commission a constaté des divergences, parfois significatives, \*\*\*\*.

De même, il a été relevé que pour un même exercice comptable, certains services communiquaient d'une année sur l'autre des données différentes à la CVFS.

Aussi la commission souhaite-t-elle connaître les raisons de ces écarts et estime nécessaire d'harmoniser les pratiques et les périmètres comptables afin de pouvoir disposer de données consolidées et comparables d'un exercice à l'autre.

**Recommandation générale n° 6 (à l'attention de la CNRLT) : Harmoniser les pratiques et les périmètres comptables afin de pouvoir disposer de données consolidées et comparables d'un exercice à l'autre et fournir à la CVFS les raisons des écarts constatés.**

### **III. LE SUIVI DES RECOMMANDATIONS DE 2019**

Dans son précédent rapport sur l'utilisation des fonds spéciaux au cours de l'exercice 2019, la CVFS avait émis 4 recommandations générales dont le suivi exercé par la commission, en lien avec la CNRLT, permet d'apporter les informations suivantes :

• **Recommandation générale n° 19.01 (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.**

Lors de l'exercice 2021, aucune avance n'a été demandée ; seul un ajustement des enveloppes entre trois services a été effectué en cours d'exercice, sous la supervision de la CNRLT.

*Cette recommandation est donc considérée comme mise en œuvre.*

• **Recommandation générale n° 19.02 (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.**

Une première étape a été mise en œuvre puisqu'un important travail de consolidation des données a été engagé de façon bilatérale entre les services bénéficiaires et la CNRLT. Cela a permis de fiabiliser les tableaux transmis et de simplifier les échanges.

La seconde étape visant à établir un guide permettant d'assurer une harmonisation de la manière de remplir les tableaux, sera menée dans le cadre du groupe de travail mis en place sur les fonds spéciaux.

*Cette recommandation reste donc partiellement ouverte.*

• **Recommandation générale n° 19.03 (à l'attention de la CNRLT) :**  
\*\*\*\*\*.

Une consultation informelle a été initiée par la CNRLT pour recueillir les premiers avis. Ce sujet doit être abordé dans le cadre du groupe de travail mis en place sur les fonds spéciaux, au début de l'année 2022.

*Cette recommandation reste donc partiellement ouverte.*

• **Recommandation générale n° 19.04 (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.**

Le sujet des possibilités de démarquage existantes dans le logiciel Chorus a été abordé dans le cadre des réunions de partage de bonnes pratiques organisées \*\*\*\* en 2019.

Cependant, le plan de charge en 2021 n'a pas permis de constituer ce groupe de travail spécifique et, pour gagner en efficacité, notamment dans le suivi des recommandations de la CVFS, la CNRLT a opté pour la constitution d'un groupe de travail sur les fonds spéciaux, dont le périmètre dépassera le cadre de cette recommandation.

Ce groupe de travail a été lancé en janvier 2022 ; il vise à instaurer un espace d'échanges et répond à un triple objectif :

- mettre en avant les bonnes pratiques pour assurer leur diffusion ;
- élaborer des documents de cadrage garantissant une cohérence entre les services et dans le temps (rédaction de « guides ») ;
- mettre en place un travail commun sur des sujets d'expertise pour mutualiser les connaissances et favoriser l'identification de solutions

innovantes (problématique Chorus, possibilités offertes par le droit de la commande publique, etc.).

*Cette recommandation, en cours de mise en œuvre, reste donc partiellement ouverte.*

### 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.
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 : turn-over 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	*****	*****

N°	Objet	Observations de la CVFS
17.05	*****	*****
18.01	Effectuer un « resoclage » de la dotation en fonds spéciaux inscrites au programme 129 pour tenir compte des besoins réels et de l'évolution de l'activité opérationnelle des services.	<p>La CVFS salue l'effort de resoclage entrepris par les services du Premier ministre, *****. En outre, aucun décret pour dépenses accidentelles et imprévisibles n'a été accordé aux services depuis lors, ce qui contribue à la sincérisation du montant de ces crédits.</p> <p>La recommandation reste néanmoins ouverte pour s'assurer de sa mise en œuvre en 2021, c'est-à-dire hors contexte particulier (crise sanitaire, notamment).</p>
18.02	*****	*****
18.04	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, 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.	<p>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.</p> <p>La recommandation est néanmoins maintenue pour s'assurer de sa mise en œuvre.</p>

N°	Objet	Observations de la CVFS
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. *****.

\*

\* \*

*Délibéré par la commission de vérification des fonds spéciaux lors de sa réunion du 14 décembre 2021.*



**ANNEXE :**  
**REPRISE DES RECOMMANDATIONS DE LA DÉLÉGATION**  
**PARLEMENTAIRE AU RENSEIGNEMENT**  
**AU 30 SEPTEMBRE 2022**

**Rapport 2018**

Complètement prise en compte	23	36
Partiellement prise en compte	10	
En cours de prise en compte	3	
Non prise en compte	1	
Non cotée	10	
<b>TOTAL</b>	<b>47</b>	

**Rapport 2019-2020**

Complètement prise en compte	23	37
Partiellement prise en compte	6	
En cours de prise en compte	8	
Non prise en compte	12	
Non cotée	10	
<b>TOTAL</b>	<b>59</b>	

**Rapport 2020-2021**

Complètement prise en compte	6	18
Partiellement prise en compte	2	
En cours de prise en compte	10	
Non prise en compte	2	
Non cotée	0	
<b>TOTAL</b>	<b>20</b>	