**N° 3087**

**ASSEMBLÉE NATIONALE**

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale
le 11 juin 2020

**N° 506**

**SÉNAT**

SESSION ORDINAIRE DE 2019-2020

Enregistré à la présidence du Sénat
le 11 juin 2020

# DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

# RAPPORT

*relatif à l'***activité** *de la* **délégation parlementaire au renseignement pour l'année 2019-2020**

PAR

M. Christian CAMBON, Sénateur

Déposé sur le Bureau de l'Assemblée nationale
par Mme Françoise DUMAS,

*Première vice-présidente de la délégation*

Déposé sur le Bureau du Sénat
par M. Christian CAMBON,

*Président de la délégation*

# SOMMAIRE

Pages

# LISTE DES PRINCIPALES RECOMMANDATIONS

**RECOMMANDATIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT**

***Sur le bilan des lois de 2015 :***

**Recommandation n° 1 :** Modifier l'article L. 853-3 du code de la sécurité intérieure afin de renvoyer à la procédure d'avis de droit commun l'examen, par la CNCTR, des demandes de renouvellement des autorisations d'introduction dans un lieu d'habitation à des fins de maintenance ou de retrait de dispositifs techniques de surveillance.

**Recommandation n° 2 :** Allonger :
- à 4 mois la durée maximale d'autorisation de la technique de recueil de données de connexion par un dispositif de proximité prévue par l'article L. 851-6 du code de la sécurité intérieure ;
- à 6 mois la durée maximale d'autorisation d'exploitation des données recueillies dans le cadre d'une surveillance internationale, à l'exception des autorisations d'exploitation données à des fins de surveillance d'une personne située sur le territoire national.

**Recommandation n° 3 :** Confier à l'inspection des services de renseignement une mission de contrôle de la mise en œuvre, par les services du premier cercle ainsi que les services listés par décret en application de l'article L. 811-4 du code de la sécurité intérieure, de l'exigence de traçabilité définie par le législateur et, plus globalement, des dispositifs de contrôle interne instaurés pour sécuriser les procédures de demande et de traitement des techniques de renseignement. Communiquer à la délégation parlementaire au renseignement les résultats de cette inspection.

**Recommandation n° 4 :** Favoriser les mutualisations et les partages d'expérience sur la mise en œuvre de dispositifs de traçabilité. Étudier la possibilité de déployer le dispositif informatique de traitement des techniques de renseignement de la DGSI au sein des services du second cercle.

**Recommandation n° 5 :** Modifier l'article L. 853-2 du code de la sécurité intérieure afin de prévoir une modalité unique de collecte de données informatiques, plus conforme aux besoins opérationnels des services.

**Recommandation n° 6 :** Proroger, à titre expérimental, la technique dite de l'algorithme prévue par l'article L. 851-3 du code de la sécurité intérieure. N'envisager son extension aux données de navigation sur internet, et en particulier aux *URL*, que sous réserve d'un renforcement conséquent des garanties entourant la mesure et de la mise en place d'un contrôle parlementaire renforcé.

**Recommandation n° 7 :** Engager des négociations en vue de la conclusion d'un protocole d'assistance entre la DGSI et le SCRT dans la mise en œuvre de certaines techniques de renseignement. Envisager, à terme, la mise en place d'une unité de mutualisation commune à plusieurs services.

**Recommandation n° 8 :** *****

**Recommandation n° 9 :** Étendre à la finalité de préservation et de promotion des intérêts économiques, industriels et scientifiques majeurs de la Nation le champ de l'autorisation d'exploitation de données collectées dans le cadre d'une surveillance internationale, à des fins de surveillance d'une personne située sur le territoire national.

**Recommandation n° 10 :** Réviser l'échelle des durées de conservation des données collectées dans le cadre des techniques de renseignement afin de tenir compte des contraintes opérationnelles liées à l'exploitation des données, sans toutefois remettre en cause le principe de graduation prévu par le législateur en 2015.

**Recommandation n° 11 :** Étendre la technique de géolocalisation en temps réel, définie à l'article L. 851-4 du code de la sécurité intérieure, à l'entourage des personnes surveillées, sous réserve de l'application d'un contingent maximal d'autorisations délivrées simultanément.

**Recommandation n° 12 :** *****

**Recommandation n° 13 :** Encadrer législativement la conduite de tests par le GIC et les services de renseignement du premier cercle sur les matériels de collecte de renseignement, à l'instar du régime prévu par l'article L. 2371-2 du code de la défense.

**Recommandation n° 14 :** Créer une nouvelle interception de sécurité pour couvrir la surveillance des correspondances physiques (lettres, paquets, etc.), susceptible, selon les besoins opérationnels, d'être associée à une introduction dans un lieu privé.

**Recommandation n° 15 :** Donner un cadre légal aux conditions dans lesquelles les renseignements collectés par le biais de techniques de renseignement peuvent être partagées entre services de renseignement. Modifier, en conséquence, l'article L. 863-2 du code de la sécurité intérieure.

**Recommandation n° 16 :** Engager une réflexion sur le statut des renseignements techniques recueillis ou exploités grâce à l'assistance d'un service de renseignement étranger et sur le niveau de protection qui les entoure.

**Recommandation n° 17 :** Engager une réflexion en vue d'ouvrir un droit d'accès ponctuel aux fichiers de souveraineté à la CNCTR, lorsqu'elle est saisie de réclamations sur le fondement de l'article L. 833-4 du code de la sécurité intérieure, à l'instar des droits actuellement reconnus à la CNIL.

**Recommandation n° 18 :** Conférer à la formation spécialisée du Conseil d'État la possibilité de s'adjoindre le concours de personnels techniques, soit par la voie d'un recrutement, soit par la voie d'un appui technique des équipes, selon les cas, de la CNCTR ou de la CNIL, dans le cadre de l'instruction des recours dont elle est saisie.

**Recommandation n° 19 :** Adapter, pour les décisions rendues par la formation spécialisée, la procédure d'exécution de droit commun :
- en confiant à la formation spécialisée le soin d'instruire les requêtes tendant à assurer l'exécution des décisions qu'elle rend et en lui autorisant à se saisir d'office ;
- en permettant à la CNCTR ou à la CNIL, en cas d'inexécution constatée d'une décision du Conseil d'État, de saisir la formation spécialisée en vue d'engager une procédure d'exécution.

***Sur le renseignement pénitentiaire :***

**Recommandation n° 20 :** Inscrire à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 l'obligation pour le Gouvernement de respecter le délai maximum d'un mois pour répondre à une demande de transmission d'un document par la DPR et de motiver sa décision en cas de refus.

**Recommandation n° 21 :** Expertiser la possibilité de créer un régime indemnitaire dédié aux métiers du renseignement pénitentiaire.

**Recommandation n° 22 :** *****

**Recommandation n° 23 :** Élargir aux agents du renseignement pénitentiaire la possibilité de recourir à une identité d'emprunt dans l'exercice de leurs missions.

**Recommandation n° 24 :** Allonger la durée de conservation des enregistrements de téléphonie légale (article 727-1 du code de procédure pénale) et recourir à des outils de traduction et de transcription automatique de la parole pour améliorer l'exploitation des données conservées.

**Recommandation n° 25 :** Expertiser la possibilité pour le SNRP de recourir à la technique de l'algorithme si elle venait à être pérennisée par la loi.

**Recommandation n° 26 :** Ouvrir un quartier d'évaluation de la radicalisation (QER) et un quartier de prévention de la radicalisation (QPR) dédié aux femmes.

**Recommandation n° 27 :** Autoriser les procureurs de la République à accéder au FSPRT.

**Recommandation n° 28 :** Instaurer un régime de sûreté *ad hoc* pour les sortants de prison.

***Sur la maîtrise des risques :***

**Recommandation n° 29 :** Harmoniser les procédures d'habilitation des agents des services de renseignement, en systématisant l'entretien de sécurité et l'entretien avec un psychologue.

**Recommandation n° 30 :** Rationnaliser le nombre de services enquêteurs placés respectivement auprès du ministère de l'intérieur et du ministère des armées, en mutualisant leurs ressources humaines et techniques. Ces services devront conduire leurs enquêtes suivant une méthodologie homogène, établie par le SGDSN, en y associant Tracfin. Les effectifs du SGDSN chargés du pilotage de la politique de protection du secret devront être augmentés afin, notamment, de conduire des audits qualité réguliers en ce domaine.

**Recommandation n° 31 :** Informer les personnes habilitées des devoirs qui leur incombent à travers la remise d'un fascicule, concomitamment à leur décision d'habilitation.

**Recommandation n° 32 :** Enrichir le rapport d'activités visé à l'article 12 de l'IGI 1300 afin de renforcer le dialogue entre les HFDS, le SGDSN et les services enquêteurs, et ainsi mieux identifier les risques liés aux habilitations.

**Recommandation n° 33 :** Formaliser les délégations accordées par les ministres aux services de renseignement en matière d'habilitation de leurs agents, en évitant de cumuler les fonctions d'autorité d'habilitation et d'officier de sécurité. Cette faculté devra être prévue par l'IGI 1300 dans sa nouvelle rédaction.

**Recommandation n° 34 :** Notifier aux agents des services du second cercle leur obligation en matière de déclaration de changement de situation personnelle auprès de l'officier de sécurité dont ils relèvent. L'officier devra quant à lui saisir l'autorité d'habilitation de ces nouvelles informations (notice 94 A révisée), qui les transmettra au service enquêteur compétent en vue de l'émission d'un nouvel avis de sécurité.

**Recommandation n° 35 :** Engager l'actualisation du cadre réglementaire relatif à la protection du secret de la défense nationale, avec pour objectif d'homogénéiser les procédures qui l'entourent, en particulier en matière d'enquêtes administratives.

**Recommandation n° 36 :** Confier à l'académie du renseignement la conception d'outils de formation et de sensibilisation aux enjeux de lutte contre la radicalisation, en lien avec les services compétents.

**Recommandation n° 37 :** Mettre en place un audit externe des dispositifs de détection et de lutte contre la radicalisation mis en place dans les services de renseignement.

**Recommandation n° 38 :** Mettre en place sur les réseaux informatiques de la DRM, avec le soutien du COMCYBER, un système qualifié visant à analyser les flux en sortie de réseau pour repérer d'éventuelles fuites de données. Son exploitation et le traitement des alertes resteront assurés en interne.

**Recommandation n° 39 :** Procéder à un audit régulier des systèmes d'information des services de renseignement et, en tant que de besoin, accompagner ces services dans la démarche d'homologation visant à protéger le secret de la défense nationale.

**Recommandation n° 40 :** *****

**Recommandation n° 41 :** Contraindre l'ensemble des agents des services de renseignement à rendre compte à leur officier de sécurité des délits qu'ils ont commis dans un cadre extraprofessionnel, quelle qu'en soit la nature. Lors du renouvellement de leur habilitation, le service enquêteur prendra l'attache des services de police et de gendarmerie afin de recueillir des informations utiles sur les candidats et mettre en lumière toute omission de leur part.

**Recommandation n° 42 :** Informer la délégation parlementaire au renseignement des manquements déontologiques graves commis par leurs agents ou leurs anciens agents, et des procédures juridiques initiées à leur encontre.

**Recommandation n° 43 :** Compléter le dispositif de lanceur d'alerte créé par la loi de juillet 2015 et étudier la possibilité de confier une partie de ces missions à la DPR.

**Recommandation n° 44 :** Améliorer l'information de la délégation parlementaire au renseignement par la commission nationale de contrôle des techniques de renseignement. Prévoir dans la loi une transmission à la DPR des recommandations adressées par la CNCTR en application de l'article L. 833-6 du code de la sécurité intérieure et, le cas échéant, des signalements adressés au procureur de la République sur le fondement de l'article L. 861-3 du même code.

***Sur le renseignement spatial :***

**Recommandation n° 45 :** Soutenir les modes collaboratifs entre la recherche publique et le secteur privé afin de développer les démonstrateurs nécessaires pour conserver notre avance technologique et stratégique.

**Recommandation n° 46 :** Afin d'améliorer la compétitivité du lanceur Ariane 6, introduire un « *Buy European Act* » pour garantir un nombre de commandes institutionnelles nécessaires à la viabilité financière et commerciale du programme.

**Recommandation n° 47 :** Mettre fin à notre dépendance à l'égard des États-Unis en nous dotant de capacités propres – *a minima* européennes sinon nationales – d'observation et d'analyse de la situation de l'eEspace et lancer un programme français de développement d'un nouveau système plus performant de surveillance de l'espace pour succéder au démonstrateur GRAVES.

**Recommandation n° 48 :** Développer une capacité autonome d'imagerie radar.

**Recommandation n° 49 :** Favoriser un accès indépendant aux systèmes et aux données spatiales en développant une filière souveraine de la donnée spatiale, sur l'ensemble de la chaîne, de l'amont (collecte) à l'aval (usages), notamment en ce qui concerne nos capacités de stockage de données.

**Recommandation n° 50 :** Confirmer la trajectoire budgétaire permettant le renouvellement de nos capacités de renseignement spatial contribuant à la fonction stratégique prioritaire « connaissance et anticipation ».

**Recommandation n° 51 :** Clarifier le positionnement du commandement de l'espace en matière de renseignement et constituer en son sein une formation spécialisée « renseignement ». Celle-ci pourrait produire du renseignement d'intérêt spatial au niveau opératif et tactique pour appuyer la planification et la conduite des opérations spatiales militaires.

**Recommandation n° 52 :** Restaurer un climat de confiance franco-allemand en élaborant une feuille de route commune au service d'une ambition spatiale commune européenne.

**Recommandation n° 53 :** Promouvoir au sein de la communauté internationale l'adoption rapide du code de bonne conduite proposé par l'Union européenne pour les activités humaines dans l'espace.

***Sur la cyberdéfense :***

**Recommandation n° 54 :** La DPR demande que les différents traitements de la menace cyber par les services de renseignement fassent l'objet d'un développement actualisé dans le PNOR et sous forme de plans d'actions comprenant des objectifs à atteindre et des modalités d'évaluation de la réalisation de ces objectifs. Elle demande à pouvoir prendre connaissance de ces documents et, régulièrement, des résultats obtenus au titre de sa mission d'évaluation de la politique publique de renseignement.

**Recommandation n° 55 :** Associer la DGSI et la DRSD à la réflexion sur la coordination institutionnelle et la définition d'une stratégie nationale de prévention et de sensibilisation aux risques cyber.

**Recommandation n° 56 :** Maintenir un niveau de financement suffisant pour garantir le niveau des investissements des services dans la cyberdéfense et leur permettre de recruter et de fidéliser des personnels de haut niveau.

**Recommandation n° 57 :** Poursuivre la mutualisation dans le développement des outils, la formation et les échanges de bonnes pratiques entre les services de renseignement.

**Recommandation n° 58 :** Associer les services de renseignement au travail prospectif d'élaboration d'une nouvelle stratégie industrielle de souveraineté en cybersécurité et orienter leur action dans sa mise en œuvre.

**Recommandation n° 59 :** Mettre en place, sous l'autorité du CNRLT, un outil d'évaluation et de suivi de la contribution des services de renseignement à la politique publique de cyberdéfense. L'inspection des services de renseignement pourrait participer à la conception de cet outil. Une fois ce travail méthodologique réalisé, la DPR souhaite que les résultats de cette évaluation et de ce suivi lui soient communiqués dans le rapport annuel d'activité des services.

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

**Recommandation générale n° 1 (à l'attention du Premier ministre) :** 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.

**Recommandation générale n° 2 :** *****

**Recommandation générale n° 3 :** *****

**Recommandation générale n° 4 (à l'attention du Premier ministre) :** Désigner par arrêté ou circulaire, non publié au *Journal officiel*, les entités et services susceptibles de bénéficier de fonds spéciaux. Cet arrêté ou circulaire, et les modifications apportées ultérieurement, seraient communiqués sans délai à la CVFS.

**Recommandation générale n° 5 (à l'attention du Premier ministre) :** Réaffirmer la possibilité pour la CVFS d'accéder aux rapports d'inspection et d'audit interne nécessaires à sa pleine information et à l'exercice de son contrôle, par la diffusion d'une instruction aux services.

**Recommandation générale n° 6 (à l'attention du CNRLT) :** Mettre en place, au sein de chaque service, des indicateurs *****.

**Recommandation générale n° 7 (à l'attention du CNRLT) :** Mettre en place une cellule interservices *****.

# INTRODUCTION GÉNÉRALE

Mesdames, Messieurs,

Si la période sous examen avril 2019 – avril 2020 a continué d'être marquée par la persistance de la menace terroriste sur le territoire national et sur les théâtres d'opérations extérieures, la défaite militaire de Daech au Levant a abaissé l'intensité de cette menace qui n'a pas disparu mais prend des formes nouvelles (propagande, inspiration d'action solitaire, *etc.*). Elle est aussi marquée par une dégradation des relations internationales et un affaiblissement des enceintes multilatérales de dialogue entre les États puissances, faisant renaître le spectre d'une nouvelle forme de guerre froide, qui se manifeste par des tensions dans les espaces communs étendus aujourd'hui à l'espace et au cyberespace et à l'utilisation de nouvelles formes ou de combinaisons d'actions, justifiant l'utilisation du terme de « guerre hybride » destinées à préparer des actions militaires ou à tester les défenses adverses. Ce tableau serait incomplet s'il n'incluait pas la persistance à un degré élevé de l'espionnage économique et des activités de la criminalité organisée.

## I. LA DPR S'EST DONNÉE CINQ AXES DE TRAVAIL

Ce contexte a incité la délégation à se donner plusieurs axes de travail :

- le premier pour consolider le cadre juridique de l'action des services de renseignement en tirant un premier bilan des lois de 2015 dans la perspective de leur actualisation éventuelle à l'occasion de l'examen du projet de loi nécessaire pour pérenniser la technique dite de « l'algorithme[1] » ;

- le second pour suivre la montée en puissance du service national du renseignement pénitentiaire créé en mai 2019 ;

- le troisième pour aborder dans la suite des travaux menés l'année dernière sur les ressources humaines, la question du contrôle interne et de la déontologie ;

[1] *Possibilité donnée aux services, à titre expérimental, pour une durée limitée et pour la seule finalité de la lutte contre le terrorisme, d'imposer aux opérateurs ou fournisseurs de communications électroniques, la mise en œuvre* « sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter les connexions susceptibles de révéler une menace terroriste ».

• le quatrième et le cinquième, à vocation plus prospective pour aborder, compte tenu des développements technologiques nouveaux, les nouveaux champs d'exercice des activités de renseignement, l'espace et le cyberespace.

À cela s'ajoute naturellement, les travaux conduits par la commission de vérification des fonds spéciaux (CVFS), présidée, cette année par M. Michel Boutant, sénateur, assurés par quatre membres de la délégation et dont le synthèse constitue la sixième partie de ce rapport. La délégation a entendu le rapport de la CVFS le 16 janvier 2019.

Au cours de l'année 2019-2020, la délégation parlementaire au renseignement (DPR) était ainsi composée :

pour le Sénat :

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

- M. Philippe Bas, sénateur Les Républicains, président de la commission des lois,

- M. François-Noël Buffet, sénateur Les Républicains, **second vice-président de la délégation**, désigné par le président du Sénat,

- M. Michel Boutant, sénateur Socialiste et républicain, désigné par le président du Sénat ;

pour l'Assemblée nationale :

- M. Jean-Jacques Bridey, député La République en Marche, premier vice-président de la délégation, président de la commission de la défense nationale et des forces armées, remplacé, à compter du 1er octobre 2019, par Mme Françoise Dumas, députée La République en Marche, **première vice-présidente de la délégation**, présidente de la commission de la défense nationale et des forces armées,

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

- M. Loïc Kervran, député La République en Marche, désigné par le président de l'Assemblée nationale,

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

*Depuis les dernières élections législatives et sénatoriales de juin et septembre 2017, la composition de la délégation n'a connu qu'un seul changement, consécutif à l'élection de Mme Françoise Dumas en qualité de présidente de la commission de la défense nationale et des forces armées de l'Assemblée nationale.*

L'organisation interne de la délégation a évolué cette année. En effet, comme l'avaient relevé MM. Philippe Bas, Christian Cambon et François-Noël Buffet dans la proposition de loi qu'il ont déposée au Sénat en 2018[1], la présidence tournante de la délégation, nécessairement assurée par un membre de droit – qui, en outre, préside une commission permanente – accroit sensiblement la charge de travail, déjà très importante, qui lui incombe. Pour répondre à cet écueil, le président de la délégation a alors proposé, à titre expérimental, un dispositif permettant de mieux répartir la charge de travail entre les membres de la délégation afin qu'elle ne repose pas uniquement sur le parlementaire qui la préside. À cet égard, un rapporteur a été nommé sur chacun des thèmes de travail choisis au titre de l'année écoulée. Une telle organisation des travaux a rendu la délégation plus agile en ce qu'elle lui a permis d'aborder un nombre plus conséquent de sujets, tout en impliquant davantage de membres. La mise en œuvre de ces nouvelles modalités d'organisation relevant du fonctionnement interne de la DPR, elle n'a pas nécessité l'adoption d'une disposition législative nouvelle.

Pour mener à bien ses travaux la délégation a donc confié à certains de ses membres, le suivi d'un axe de travail. C'est ainsi que M. François-Noël Buffet a étudié les évolutions possibles des lois de 2015, Mme Yaël Braun-Pivet, la montée en puissance du renseignement pénitentiaire, M. Loïc Kervran, le contrôle interne et la déontologie, M. Patrice Verchère, le renseignement dans l'espace et M. Christian Cambon, la contribution des services de renseignement à la cyberdéfense.

La plupart de ces travaux ont été conduits au sein de la délégation par des auditions au Sénat ou au sein des services (DGSE et DGSI). C'est ainsi que la délégation a entendu tous les directeurs des services du premier cercle de la communauté du renseignement, mais également ceux de la direction du renseignement de la préfecture de police de Paris et du service central du renseignement territorial, le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), à deux reprises, le président de la commission nationale de contrôle des techniques de renseignement (CNCTR), à deux reprises, le président de la formation spécialisée du Conseil d'État chargée du contentieux de la mise en œuvre des techniques de renseignement et le directeur du groupement interministériel de contrôle (GIC). En outre, elle a élargi ses auditions, notamment pour aborder la question de la cyberdéfense et du renseignement militaire dans l'espace, au chef d'état-major des armées, au commandant de la cyberdéfense, au directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI) et au principal rédacteur de la revue stratégique de la cyberdéfense publiée en février 2018, M. Louis Gautier, alors SGDSN.

---

[1] *Proposition de loi n° 470 (2019-2020) présentée par MM. Philippe Bas, Christian Cambon, François-Noël Buffet, Marc-Philippe Daubresse et Mme Martine Berthet, tendant à renforcer le contrôle parlementaire du renseignement.*

**Calendrier des réunions plénières de la délégation parlementaire au renseignement de mai 2019 à avril 2020**

**Réunion du 16 mai 2019 :**
- audition du préfet Pierre de Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme ;
- audition du général François Lecointre, chef d'état-major des armées.

**Réunion du 6 juin 2019 :**
- audition de M. Guillaume Poupard, directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- audition de M. Francis Delon, président de la commission nationale de contrôle des techniques de renseignement (CNCTR).

**Réunion du 20 juin 2019 :**
audition de M. Louis Gautier, ancien secrétaire général de la défense et de la sécurité nationale (SGDSN), coordonnateur de la revue stratégique de cyberdéfense publiée le 12 février 2018.

**Réunion du 11 juillet 2019 :**
- audition du préfet Pierre de Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme ;
- audition du général Jean-François Ferlet, directeur du renseignement militaire (DRM) ;
- audition du général Olivier Bonnet de Paillerets, commandant de la cyberdéfense (COMCYBER).

**Réunion du 3 octobre 2019 :**
- audition de M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC) ;
- audition de Mme Françoise Bilancini, directrice du renseignement de la préfecture de police (DRPP) ;
- audition de Mme Lucile Rolland, cheffe du service central du renseignement territorial (SCRT).

**Réunion du 8 octobre 2019 :**
audition de M. Christophe Castaner, ministre de l'intérieur, et de M. Laurent Nuñez, secrétaire d'État auprès du ministre de l'intérieur.

**Déplacement au siège de la direction générale de la sécurité intérieure (DGSI) du 10 octobre 2019 :**
audition du directeur général, M. Nicolas Lerner, et de plusieurs cadres de son service.

**Déplacement au siège de la direction générale de la sécurité extérieure (DGSE) du 7 novembre 2019 :**
audition du directeur général, M. Bernard Émié, et de plusieurs cadres de son service.

**Réunion du 19 novembre 2019 :**
audition de Mme Claire Legras, directrice des affaires juridiques du ministère des armées.

**Réunion du 28 novembre 2019 :**
- audition de Mme Corinne Cléostrate, directrice nationale du renseignement et des enquêtes douanières (DNRED) ;
- audition de Mme Maryvonne Le Brignonen, directeur de Tracfin.

**Réunion du 4 décembre 2019 :**
audition du général Éric Bucquet, directeur du renseignement et de la sécurité de la défense (DRSD).

**Réunion du 16 janvier 2020 :**
- audition de M. Edmond Honorat, président de la formation spécialisée du Conseil d'État en matière de contentieux du renseignement ;
- audition de M. Christian Protar, secrétaire général de l'inspection des services de renseignement (ISR), et de Mme Amélie Puccinelli, inspectrice de l'administration, sur les deux missions confiées à l'ISR relatives à la détection des processus de radicalisation dans les services de renseignement ;
- présentation du rapport de la commission de vérification des fonds spéciaux (CVFS) sur les comptes de l'exercice 2018.

**Réunion du 20 février 2020 :**
audition de M. Francis Delon, président de la commission nationale de contrôle des techniques de renseignement (CNCTR).

**Réunion du 26 février 2020 :**
audition de M. Gérald Darmanin, ministre de l'action et des comptes publics.

**Réunion du 5 mars 2020 :**
audition du préfet Pierre de Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme.

**Réunion de travail du 11 juin 2020 :**
examen et adoption du rapport annuel.

Ces auditions ont été complétées, en tant que de besoin, par des auditions et des déplacements réalisés à l'initiative des rapporteurs, mais ouvertes aux autres membres de la délégation.

**Calendrier des auditions et des déplacements thématiques**

***Le renseignement pénitentiaire (rapporteure : Mme Yaël Braun-Pivet, députée)***

**1er octobre 2019 :**
audition de MM. Stéphane Bredin, directeur de l'administration pénitentiaire, et Benoît Fichet, adjoint à la cheffe du service national du renseignement pénitentiaire.

**7 janvier 2020 :**
déplacement au centre pénitentiaire de Meaux, et audition de MM. Pascal Spenle, directeur du centre pénitentiaire de Meaux-Chauconin, et Olivier Hubac, service national du renseignement pénitentiaire.

**20 janvier 2020 :**
déplacement à la DGSI et audition de MM. Nicolas Lerner, directeur général de la sécurité intérieure, Amin Boutaghane, chef de l'unité de coordination de la lutte antiterroriste (UCLAT), et Benoît Fichet, adjoint à la cheffe du service national du renseignement pénitentiaire.

***Le renseignement spatial (rapporteur : M. Patrice Verchère, député)***

**8 octobre 2019 :**
audition du général Philippe Steininger, conseiller militaire du président du CNES.

**22 octobre 2019 :**
audition de M. Martin Briens, directeur de cabinet de la ministre des armées.

**18 décembre 2019 :**
audition de M. Jacques Lafaye, conseiller du président-directeur général de l'ONERA.

**22 janvier 2020 :**
audition de M. Patrick Pailloux, directeur technique de la DGSE.

**4 février 2020 :**
audition du général Jean-François Ferlet, directeur du renseignement militaire.

**18 février 2020 :**
- audition de M. Joël Barre, délégué général pour l'armement ;
- déplacement à l'ONERA et audition de M. Bruno Sainjon, président-directeur général, M. Jacques Lafaye, conseiller du président-directeur général, M. Antoine Roblin, directeur du département optique et techniques associées, Mme Hélène Oriot, directrice du département électromagnétique et radar, et M. Gilles Foulon, directeur du département traitement de l'information et système.

**24 février 2020 :**
audition de M. Jean-Marc Nasr, président d'Airbus Defence and Space SPS, du général (2S) Jean-Pierre Serra, vice-président International & Space Institutions d'Airbus Defence and Space, et de Mme Annick Perrimond-du Breuil, directeur des relations avec le parlement d'Airbus.

**4 mars 2020 :**
déplacement à Toulouse et visites :
- d'Airbus Space & Defense ; présentation du site par M. Benoît de Maupeou, responsable des relations avec la direction générale de l'armement pour les affaires spatiales ;
- du CNES ; présentation du site par M. Frédéric Pradeilles, directeur du numérique, de l'exploitation et des opérations, chef de l'établissement de Toulouse ;
- de l'entreprise Hémeria ; présentation du site par M. Nicolas Multan, directeur général.

*En raison de la crise sanitaire liée à la Covid-19 et du confinement qu'elle a provoqué, des auditions et déplacements ont dû être annulés, notamment une visite du site de Cannes de l'entreprise Thales Alenia Space, et un entretien avec le général Michel Friedling, commandant du commandement interarmées de l'espace.*

## II. LA DPR A ASSURÉ UN SUIVI DE L'ACTUALITÉ DU RENSEIGNEMENT

Outre ces travaux menés en continu la délégation a suivi l'actualité des services de renseignement.

C'est ainsi qu'elle s'est fait présenter, le 19 juillet 2019, par M. Pierre Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme, **la nouvelle stratégie nationale du renseignement** adoptée en conseil national du renseignement et qu'elle a été informée, le 19 novembre 2019 par Mme Claire Legras, directrice des affaires juridiques du ministère des armées, de la position française sur le **contentieux pendant devant la Cour de justice de l'Union européenne relatif à la conservation des données de connexion par les opérateurs de télécommunications** suite à un premier arrêt du 21 décembre 2016 (*Télé2 Sverige AB contre Post-och telestyrelsen*).

C'est ainsi également qu'elle a tenu au lendemain de **l'attentat perpétré le 3 octobre 2019 à la préfecture de police de Paris** à entendre, dès le 8 octobre, le ministre de l'intérieur, M. Christophe Castaner, et le secrétaire d'État, M. Laurent Nunez.

**Les travaux de la délégation**
**suite à l'attentat du 3 octobre à la préfecture de police de Paris**

Le ministre a répondu aux questions des membres de la délégation qui portaient sur la sécurité des services de renseignement et plus particulièrement de la DRPP, face aux risques éventuels de radicalisation de certains de leurs agents :

- la mise en œuvre des procédures d'habilitation des agents ;

- les conditions d'accès des agents aux informations sensibles à l'intérieur du service et notamment aux données numérisées et les modalités de cloisonnement mises en place pour éviter les intrusions de personnes qui n'auraient pas vocation à en connaitre ;

- les règles applicables en matière d'accès aux locaux du service et leur mise en œuvre ;

- les procédures mises en place par ce service pour détecter d'éventuels signes de radicalisation de ses agents et les procédures de transfert de signalement entre services dans les cas où la détection de signes est réalisée par un autre service, à raison d'activités en dehors du service ou de son ressort territorial, et leur mise en œuvre.

Ces questionnements ont orienté les travaux des missions confiées par le Premier ministre à l'inspection des services de renseignement, le 5 octobre, la première pour vérifier si, au cours des années que l'auteur des faits a passées à la DRPP, et en particulier celles qui auraient été concernées par un processus de radicalisation, les outils et procédures de détection et de signalement étaient en place, s'ils ont été convenablement mis en œuvre au regard des éléments perceptibles de cette radicalisation et s'ils ont donné lieu à des réactions appropriées.

La seconde qui porte sur l'ensemble des services de renseignement spécialement impliqués dans la lutte contre le terrorisme pour superviser un processus de réévaluation des situations individuelles le justifiant, vérifier les outils et les procédures de détection, de signalement et de traitement.

La délégation a reçu communication de ces rapports et elle a entendu les membres de l'inspection des services de renseignement qui les ont rédigés, le 16 janvier 2020.

Une procédure judiciaire étant en cours, la délégation n'a pas souhaité poursuivre au-delà ses investigations, mais elle a réorienté son thème de travail sur la maitrise des risques (dispositifs de contrôle interne et déontologie) et abordé systématiquement les questions évoquées lors des auditions et déplacements dans les services.

Au titre de ses activités internationales, la DPR a reçu au Sénat, le 2 mai 2019, la visite d'une délégation parlementaire autrichienne de la sous-commission des affaires intérieures du Conseil national, accompagnée, entre autres, du directeur du BvT (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*, équivalent de la DGSI). Dans un contexte de réforme du service de sécurité intérieure autrichien, cette sous-commission a effectué plusieurs déplacements à l'étranger afin de nourrir sa réflexion sur l'organisation et le fonctionnement de son instance de contrôle parlementaire du renseignement, en la comparant avec ses homologues étrangères.

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 17 octobre 2019, à l'Assemblée nationale.

Pour conclure ses travaux, la délégation avait prévu d'entendre les ministres ayant autorité sur des services de renseignement du premier cercle. Outre l'audition susmentionnée avec le ministre de l'intérieur, une audition a pu être organisée du ministre de l'action et des comptes publics, M. Gérald Darmanin. Des auditions du Premier ministre et de la ministre des armées étaient en cours de programmation lorsque les mesures de confinement consécutives à l'épidémie de Covid-19 sont intervenues. Ne disposant pas des locaux adaptés permettant la réalisation de ces auditions dans des conditions satisfaisant aux règles de distanciation physique et de protection du secret de la défense nationale, la délégation a renoncé à leur organisation. Elle devra se préoccuper à l'avenir des modalités qui lui

permettraient, en cas d'urgence, de poursuivre ses travaux dans des conditions satisfaisant ses exigences.

Cette situation l'invitera probablement à aborder dans ses prochains travaux les modalités et conditions selon lesquelles les services de renseignement ont pu assurer la continuité de leurs missions pendant cette période, mais aussi leurs capacités à apporter aux autorités politiques les informations nécessaires à la prise de décisions en cas de crise sanitaire grave. Les livres blancs sur la défense et la sécurité nationale de 2008 et de 2013, comme la revue stratégique de 2017, citent les pandémies comme des risques et menaces majeures, mais la stratégie nationale du renseignement est muette sur l'orientation de nos capteurs afin de connaître et anticiper ses risques et menaces.

Au cours de ses travaux, la DPR a trouvé, en général, une écoute attentive des différents services et interlocuteurs qui ont pu répondre à ses questions. Elle tient néanmoins à signaler l'impossibilité qui a été la sienne de prendre connaissance du rapport de l'inspection des services judiciaires suite à l'attentat perpétré à la prison de Condé-sur-Sarthe le 5 mars 2019. Une demande de communication a été adressée à Mme Nicole Belloubet, ministre de la justice, garde des sceaux, par le président de la délégation par une lettre en date du 20 septembre 2019 qui n'a obtenu aucune réponse. Cette demande a été réitérée par courriel en date du 24 février restée une nouvelle fois sans réponse et formulée au Premier ministre, par une lettre en date du 4 mars 2020, restée sans réponse également.

Aux termes de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958, « *la délégation peut solliciter du Premier ministre, communication de tout ou partie des rapport de l'inspection des services de renseignement ainsi que des rapports des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence* ».

Si un refus de communication motivé aurait pu constituer une réponse acceptable, ce long silence n'a pas permis à la délégation parlementaire au renseignement d'accomplir pleinement la mission de contrôle parlementaire de l'action du Gouvernement en matière de renseignement et d'évaluation de la politique publique en ce domaine que lui a confiée le législateur. Cette situation justifie la disposition adoptée par le Sénat par un amendement lors de l'examen au projet de loi de programmation militaire 2019-2025, issue d'une proposition de loi déposée le 11 mai 2018[1] par MM. Philippe Bas, Christian Cambon et François-Noël Buffet, tous trois membres de la DPR, qui visait à autoriser l'accès à certains documents, tout en préservant la capacité de l'exécutif à restreindre ce droit d'accès pour certaines informations, sous réserve d'en motiver le refus.

---

[1] *Proposition de loi n° 470 (2019-2020) présentée par MM. Philippe Bas, Christian Cambon, François-Noël Buffet, Marc-Philippe Daubresse et Mme Martine Berthet, tendant à renforcer le contrôle parlementaire du renseignement.*

Enfin la délégation a pris connaissance avec satisfaction du taux de mise en œuvre des recommandations de son rapport pour l'année 2018 qui s'élèvent à 22 sur 42, 7 étant réalisées partiellement, 11 étant en cours d'études et 2 non réalisées.

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 11 juin 2020 sous la présidence de M. Christian Cambon, président, la délégation parlementaire au renseignement a adopté le présent rapport relatif à son activité pour l'année 2019-2020 et l'ensemble des recommandations formulées. M. Michel Boutant a émis une réserve sur la recommandation n° 14, et M. Loïc Kervran sur les recommandations portant sur le bilan des lois de 2015 qui seraient en contradiction avec celles de la mission d'information commune de l'Assemblée nationale sur l'évaluation de la loi renseignement, dont il était le co-rapporteur.***

# CHAPITRE I :
# LA LOI RELATIVE AU RENSEIGNEMENT, UNE « RÉVOLUTION LÉGISLATIVE » RÉUSSIE

« *Signe de maturité de notre démocratie* » comme l'indiquait Philippe Bas, rapporteur du projet de loi pour le Sénat, la loi du 24 juillet 2015 a constitué une étape fondamentale dans l'histoire du renseignement.

Fondamentale en ce qu'elle a, pour la première fois, donné une légitimité à l'action de nos services, dont les agents ont pendant longtemps agi pour la sécurité et la défense de notre pays dans l'ombre et dans l'insécurité juridique la plus totale.

Fondamentale, ensuite, parce qu'elle a permis de consolider notre état de droit en dotant notre pays d'un cadre légal garantissant la protection des droits et libertés constitutionnels, sans pour autant porter atteinte à l'efficacité des services.

Le fait que cette loi ait été adoptée en 2015 n'est pas un hasard. Alors que notre pays était confronté à une diversité et à un niveau de menace sans précédent, jamais le besoin de sécuriser l'action de renseignement ne s'était fait autant ressentir.

Cinq ans après son entrée en vigueur, et avant que le législateur ne soit amené à se prononcer sur la pérennisation de la technique dite de l'algorithme dont l'expérimentation arrive à échéance au 31 décembre 2020, la délégation parlementaire au renseignement a souhaité dresser un bilan de sa mise en œuvre.

A cette fin, elle a, au cours de l'année passée, interrogé l'ensemble de la communauté des services de renseignement ainsi que des acteurs impliqués directement dans la mise en œuvre de la loi en vue de recueillir tant les données quantitatives que les appréciations qualitatives sur l'application du nouveau cadre légal.

Tous s'accordent, aujourd'hui, sur la nécessité de préserver l'équilibre atteint.

La délégation partage cette opinion, observant que si des modifications méritent sans doute d'être apportées pour parfaire le dispositif, elles se devront de rester ponctuelles. Une nouvelle réforme du cadre du renseignement, quelques années seulement après cette loi d'ampleur, ne pourrait d'ailleurs qu'être déstabilisatrice pour les services et, partant, pour l'efficacité de la politique de renseignement.

La délégation a mené ses travaux parallèlement à la conduite d'un groupe de travail interministériel, piloté par la coordination nationale du

renseignement et de la lutte contre le terrorisme (CNRLT). Cette coïncidence des calendriers explique qu'elle n'ait pu parfois obtenir l'ensemble des informations qui lui auraient été nécessaires, les perspectives d'évolution du cadre légal étant encore en cours de maturation au sein des instances de l'État.

Elle espère toutefois pouvoir contribuer, par ses recommandations, à la conduite d'une réforme juste et pertinente de la loi de 2015, au bénéfice tant de la protection des droits de nos concitoyens que de l'efficacité des services de renseignement.

# I. LA LOI RENSEIGNEMENT, UN CADRE LÉGAL PROTECTEUR DU DROIT AU RESPECT DE LA VIE PRIVÉE ET SÉCURISANT POUR LES SERVICE DE RENSEIGNEMENT

## *A. APPELÉE DE SES VŒUX TANT PAR LES PARLEMENTAIRES QUE PAR LES SERVICES DE RENSEIGNEMENT, LA LOI DE 2015 A RÉPONDU À UN BESOIN URGENT DE SÉCURITÉ JURIDIQUE*

### 1. Un encadrement jusqu'alors partiel et non homogène de l'activité de renseignement

Jusqu'en 2015, la France ne disposait pas, contrairement à nombre de ses voisins européens, d'un arsenal juridique complet permettant d'encadrer l'activité des services de renseignement.

Sans que l'on puisse parler d'un contexte de non-droit, **le législateur ne s'était en effet saisi que partiellement de la matière, laissant de côté un large pan des actions conduites par les services**. Seules trois techniques de renseignement avaient ainsi fait l'objet, successivement, d'un encadrement légal, sans qu'aucune logique globale n'ait toutefois jamais été adoptée.

La première pierre du dispositif de contrôle de l'activité des services de renseignement fût posée par la loi n° 91-646 du 10 juillet 1991 *relative au secret des correspondances émises par la voie des télécommunications*, qui tirant les conséquences de deux arrêts de la Cour européenne des droits de l'homme ayant condamné la France pour atteinte au droit au respect de la vie privée[1], a soumis les **interceptions de sécurité** à une procédure d'autorisation préalable du Premier ministre et à un contrôle, initialement *a posteriori,* d'une commission indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Par la suite, les activités de renseignement ont fait l'objet de plusieurs réformes, mais de portée relativement réduite.

[1] *CEDH, arrêté Kruslin c/ France, 1990.*

Par deux lois successives datant de 2006 et de 2013[1] a été instauré un régime spécifique encadrant le recours aux **accès administratifs aux données techniques de connexion,** qui consistent en la communication de certaines données de connexion traitées par les opérateurs de communications électroniques (identifiants de connexion, numéros d'abonnement, liste des numéros appelés ou entrant, durée et date des communications effectuées par une personne, *etc*.).

D'abord accessibles aux seuls services dépendant du ministère de l'intérieur puis étendus à tous les services de renseignement, ces accès ont été soumis à une procédure d'autorisation préalable par une « personnalité qualifiée », ainsi qu'au contrôle *a posteriori* de la CNCIS, à l'instar des interceptions de sécurité.

Par la même loi de programmation militaire du 18 décembre 2013, un régime similaire mais plus contraignant a enfin été défini pour la **géolocalisation en temps réel**, qui ont été soumises à l'accord préalable du Premier ministre lui-même.

### 2. Un souci partagé d'instaurer un cadre d'action protecteur des libertés et sécurisant pour les agents

Proposée tant par les pouvoirs publics[2] que par plusieurs rapports parlementaires[3], notamment issus de la délégation, l'instauration d'un cadre juridique englobant plus largement l'activité des services de renseignement répondait à une **double nécessité** : d'une part, assurer la protection des droits et libertés individuels, en particulier le droit au respect de la vie privée ; d'autre part, garantir une plus grande sécurité juridique pour les agents des services de renseignement.

*a) Un besoin impérieux de sécurité juridique*

L'absence de corpus juridique encadrant l'ensemble de l'activité des services de renseignement constituait, sur le plan de la protection des droits et libertés fondamentales, une **faille importante dans notre État de droit**.

De fait, elle représentait une source importante de fragilité juridique et exposait la France à des **risques non négligeables de condamnation** par la Cour européenne de sauvegarde des droits de l'homme et des libertés fondamentales, au regard de l'atteinte portée à la vie privée et familiale, telle que protégée par l'article 8 de la Convention. Si la Cour reconnait, selon une

---

[1] *Loi n° 2006-64 du 20 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers, au contrôle a posteriori et loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019.*

[2] *Livre blanc de la défense et de la sécurité nationale de 2008.*

[3] *En particulier, le rapport de M. Jean-Jacques Urvoas, fait au nom de la délégation parlementaire au renseignement (2014).*

jurisprudence constante, que « *l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales* », elle exige, au regard de l'atteinte portée aux libertés individuelles, la **définition, par la loi, de garanties suffisantes et adéquates contre les abus[1].**

Comme le relevait Philippe Bas, président de la commission des lois lors de l'examen du projet de loi relatif au renseignement, l'exercice des missions des services de renseignement « *ne [faisait] pas l'objet d'un cadre spécifique, aboutissant à un paradoxe : certaines techniques de renseignement mises en œuvre [étaient] aux limites de la légalité voire en contradiction avec la loi pénale, sans que les citoyens disposent de garanties réelles pour la préservation de leur vie privée puisqu'aucune condamnation pénale n'est prononcée, faute de poursuites ou de preuves* ».

Au-delà d'être source de contentieux, l'incomplétude du cadre légal était également **peu satisfaisante sur le plan opérationnel**, dès lors qu'elle empêchait toute exploitation des renseignements collectés par le biais de la mise en œuvre d'une technique « non légale » dans le cadre d'éventuelles procédures judiciaires. Or l'on sait, en matière de terrorisme notamment, l'importance de tels renseignements pour engager une action pénale efficace voire prévenir, dans certains cas, la commission d'infraction.

*b) Un besoin de légitimité et de sécurité pour les services de renseignement*

Le second argument principal invoqué à l'appui de la définition d'un encadrement légal du renseignement résidait dans le besoin d'assurer une **protection renforcée des agents des services de renseignement**.

Faute de cadre juridique complet et homogène, ceux-ci étaient en effet susceptibles de voir leur responsabilité pénale engagée au titre d'infractions d'atteinte à la vie privée dès lors qu'ils recouraient, dans le cadre de leurs missions, à des méthodes attentatoires aux libertés individuelles et non encadrées par le législateur.

Comme le rappelait Jean-Jacques Urvoas, alors président de la délégation parlementaire au renseignement, le régime général de protection pénale prévu par l'article 122-4 du code pénal[2], permettant de couvrir les agents publics commettant des actes illégaux commandés par l'autorité légitime, « *n'offr[ait] qu'une protection très parcellaire qui ne résisterait guère à un contentieux* ».

---

[1] *CEDH, arrêt Klass et autres c/ Allemagne,*

[2] *L'article 122-4 du code pénal prévoit que « n'est pas pénalement responsable la personne qui accomplit un acte commandé par l'autorité légitime, sauf si cet acte est manifestement illégal ».*

### *B. LA LOI DE 2015 A CRÉÉ UN CADRE UNIFIÉ ET COHÉRENT, DESTINÉ À ENGLOBER L'ENSEMBLE DE L'ACTIVITÉ DE RENSEIGNEMENT*

Fruit d'un travail collaboratif entre le Gouvernement et les assemblées parlementaires, la loi du 24 juillet 2015 a introduit, au sein du code de la sécurité intérieure, un cadre légal unique destiné à couvrir de manière plus complète l'activité des services de renseignement et à donner un fondement légal à de nouvelles techniques et méthodes plus intrusives, rendues nécessaires par l'évolution technologique.

Outre une définition rénovée et élargie de leurs missions, elle a fixé une procédure d'autorisation unifiée, largement inspirée du régime des interceptions de sécurité, renforcé le contrôle externe de la collecte de renseignements et ouvert des voies de recours juridictionnels aux citoyens, qui faisaient jusqu'alors largement défaut.

#### 1. Une définition précise, dans la loi, des finalités du renseignement

De manière à encadrer les atteintes portées à la vie privée, la loi relative au renseignement a **listé, de manière exhaustive, les finalités** pour lesquelles les services de renseignement sont autorisés à recourir à des techniques intrusives.

Désormais énumérées à l'article L. 811-3 du code de la sécurité intérieure, ces finalités renvoient à la protection des intérêts fondamentaux de la Nation, tels que fixés à l'article 410-1 du code pénal et sont au **nombre de sept** :

**1° L'indépendance nationale**, l'intégrité du territoire et la défense nationale ;

**2° Les intérêts majeurs de la politique étrangère**, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

**3° Les intérêts économiques, industriels et scientifiques** majeurs de la France ;

**4° La prévention du terrorisme** ;

**5° La prévention** :

- des atteintes à la **forme républicaine** des institutions ;

- des actions tendant au maintien ou à la reconstitution de **groupements dissous** en application de l'article L. 212-1 du code de la sécurité intérieure ;

- des **violences collectives** de nature à porter gravement atteinte à la paix publique ;

**6° La prévention de la criminalité et de la délinquance** organisées ;

**7° La prévention de la prolifération des armes de destruction massiv**e.

Parallèlement, la loi est venue **préciser les conditions de recours aux techniques de renseignement selon les services de renseignement concernés**. Pour ce faire, elle a introduit une distinction entre :

– les **six services spécialisés**, dits **services du « premier cercle »** du renseignement, à savoir la DGSE, la DGSI, la DRM, la DRSD, la DNRED et Tracfin, qui sont autorisés à mettre en œuvre l'ensemble du panel des techniques de renseignement autorisées par la loi, à l'exception de Tracfin[1] ;

– les **autres services**, identifiés comme constitutifs **d'un « second cercle »** de la communauté du renseignement, autorisés, par décret, à recourir à certaines techniques de renseignement pour des finalités s'inscrivant dans le cadre de leurs missions[2].

Pour l'essentiel, ces services bénéficient d'un accès aux techniques de renseignement pour les finalités de prévention du terrorisme, de lutte contre la criminalité organisée et, dans certains cas, de protection de l'indépendance nationale et de lutte contre les violences collectives. Aucun d'entre eux n'est en revanche autorisé à y recourir pour la protection des intérêts économiques, industriels et scientifiques, la préservation des intérêts de la politique étrangère et la prévention de la prolifération des armes de destruction massive, finalités qui, par nature, relèvent des services spécialisés du renseignement.

**Le « second cercle » de la communauté du renseignement**

Le « second cercle » de la communauté du renseignement, dont le périmètre est défini par l'article R. 811-2 du code de la sécurité intérieure, inclut aussi bien des services de renseignement que des services de police judiciaire qui, dans le cadre de certaines de leurs activités, peuvent être amenés à collecter du renseignement avant même qu'une procédure judiciaire ne soit engagée.

Son périmètre a été modifié à la suite de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, qui a ouvert la possibilité d'y inclure le bureau national du renseignement pénitentiaire, depuis devenu service national du renseignement pénitentiaire.

[1] *En application de l'article R. 853-1 du code de la sécurité intérieure, Tracfin ne peut mettre en œuvre les techniques de captation de paroles et d'images ainsi que de captation et de recueil de données informatiques.*

[2] *Art. L. 811-4 du code de la sécurité intérieure.*

Il inclut à ce jour :

- plusieurs services relevant de la **direction centrale de la police judiciaire** (le service central des courses et jeux, l'office anti-stupéfiants, la sous-direction de la lutte contre la criminalité organisée, la sous-direction de la lutte contre la criminalité financière, la sous-direction antiterroriste, la sous-direction de la lutte contre la cybercriminalité, les services déconcentrés de la police judiciaire) ;

- plusieurs services relevant de la **direction centrale de la police aux frontières**, dont l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre ;

- plusieurs services de la **direction centrale de la sécurité publique**, en particulier le service central du renseignement territorial et ses différentes antennes ;

- plusieurs services relevant de la **direction générale de la gendarmerie nationale**, en particulier la sous-direction de l'anticipation opérationnelle ;

- plusieurs services de la préfecture de police de Paris, en particulier la direction du renseignement ;

- le service national du renseignement pénitentiaire ;

- les sections de recherche de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement.

Pour solliciter la mise en œuvre d'une technique de renseignement, les services doivent donc respecter **deux conditions** : leur demande doit, d'une part, être motivée par l'une des finalités énumérées par la loi et, d'autre part, s'inscrire pleinement dans l'exercice des missions qui leur sont reconnues par les lois et règlements.

### 2. Un cadre procédural commun et rénové

L'un des principaux piliers de la loi relative au renseignement réside dans l'harmonisation des régimes applicables aux différentes techniques de renseignement et dans la définition d'une **procédure d'autorisation préalable unique des techniques mises en œuvre sur le territoire national.**

L'autorisation est **délivrée par le Premier ministre, après avis** d'une autorité administrative indépendante nouvellement créée en remplacement de la CNCIS, la **Commission nationale de contrôle des techniques de renseignement (CNCTR)**[1]**.**

Sur le plan procédural, la demande de technique de renseignement est **formulée par le ministre de tutelle** du service de renseignement concerné, soit, alternativement, le ministre de la défense, le ministre de l'intérieur, le ministre de la justice ou les ministres chargés de l'économie, du budget et des douanes. La demande doit préciser la ou les techniques demandées, le service pour lequel elle est présentée, la ou les finalités

[1] *Art. L. 821-1 du code de la sécurité intérieure.*

poursuivies, le ou les motifs des mesures, la durée de validité de l'autorisation ainsi que les personnes, les lieux ou véhicules concernés[1].

L'ensemble des demandes formulées par les services est centralisé au niveau d'un service du Premier ministre, le groupement interministériel de contrôle (GIC), qui est chargé de les transmettre à la CNCTR.

**Une fois saisie, cette dernière est amenée à se prononcer selon deux procédures distinctes, mobilisées selon le degré d'intrusivité de la technique demandée**.

Dans la majorité des cas, l'avis est rendu selon la **procédure de droit commun**, c'est-à-dire par un membre de la commission, parmi ceux issus du Conseil d'État et de la Cour de cassation, dans un délai maximal de 24 heures.

La CNCTR peut également être amenée à se prononcer en **formation collégiale, restreinte ou plénière**, soit lorsque les cas présentent une complexité particulière ou posent une question nouvelle ou sérieuse[2], soit lorsque la loi le prévoit spécifiquement. Sont notamment concernées les demandes portant sur des professions protégées (parlementaire, magistrat, avocat, journaliste)[3] et les demandes d'introduction dans un lieu d'habitation[4]. La CNCTR est, dans cette hypothèse, tenue de se prononcer en 72 heures.

**L'organisation de la CNCTR**

**Instance collégiale**, la CNCTR est composée, conformément à l'article L. 831-1 du code de la sécurité intérieure, de **9 membres**, dont :

- **quatre parlementaires**, deux députés et deux sénateurs désignés par leur assemblée respective ;

- **deux membres du Conseil d'État** nommé par le vice-président ;

- **deux magistrats de la Cour de cassation** nommés conjointement par le premier président et le procureur général de la cour ;

- **une personnalité qualifiée** nommée par le Président de la République, sur proposition du président de l'Autorité de régulation des communications électroniques et des postes (ARCEP).

La CNCTR peut siéger en **deux formations collégiales** :

- en **formation plénière**, qui rassemble l'ensemble des 9 membres de la commission ;

- en **formation restreinte**, qui réunit les deux membres du Conseil d'État, les deux magistrats de la Cour de cassation et la personnalité qualifiée.

[1] *Art. L. 821-2 du même code.*
[2] *Art. L. 832-3 du code de la sécurité intérieure.*
[3] *Art. L. 821-7 du code de la sécurité intérieure.*
[4] *Art. L. 853-3 du code de la sécurité intérieure.*

De manière à ne pas nuire à l'efficacité et à la réactivité des services de renseignement, le législateur a enfin prévu une **procédure d'exception**, permettant au Premier ministre, **en cas d'urgence absolue**, de se prononcer sans l'avis préalable de la CNCTR[1].

### 3. Un élargissement du panel de techniques ouvertes aux services de renseignement

Alors que le cadre juridique antérieur n'autorisait, formellement, que trois types de techniques de renseignement, la loi relative au renseignement **a, comme l'avait recommandé la délégation dans son rapport d'activité de 2014, considérablement élargi le panel des techniques accessibles aux services**, y intégrant des méthodes plus modernes mais également plus intrusives.

Au demeurant, les techniques dont l'usage était déjà ouvert aux services de renseignement ont été, pour certaines d'entre elles, étendues. En particulier, la possibilité de mettre en œuvre des interceptions de sécurité a été élargie à l'entourage des personnes surveillées.

Afin de tenir compte des écarts dans le degré d'atteinte à la vie privée, le législateur, tout en soumettant chacune de ces techniques au cadre légal général, a prévu des **garanties différenciées**, à deux niveaux :

– d'une part, **dans la durée maximale de l'autorisation délivrée** par le Premier ministre qui varie, selon les techniques, de 48 heures pour les plus attentatoires aux libertés à 4 mois pour les autres ;

– d'autre part, **dans l'étendue des finalités** pour lesquelles la technique est autorisée. C'est ainsi que les techniques jugées très intrusives, à l'instar de l'accès en temps réel aux données de connexion ou de l'algorithme, ne peuvent être autorisées qu'aux seules fins de prévention du terrorisme.

[1] *Art. L. 821-5 du code de la sécurité intérieure.*

## Les techniques de renseignement destinées à surveiller le territoire national[1]

| Technique | Description | Finalités autorisées | Durée maximale d'autorisation |
|---|---|---|---|
| **Accès aux données de connexion (L. 851-1 CSI)** | Identification des numéros d'abonnement ou données de connexion d'une personne par réquisition auprès d'un opérateur | Toutes les finalités prévues à l'article L. 811-3 | 4 mois, renouvelables pour une donnée équivalente |
| **Recueil des données de connexion en temps réel (L. 851- 2 CSI)** | Recueil, en temps réel, des données de connexion d'une personne *via* l'opérateur | Prévention du terrorisme | 4 mois, renouvelables pour une durée équivalente |
| **Dispositif de détection d'une menace terroriste par analyse des "signaux faibles" (dite technique de l'algorithme) (L. 851-3 CSI)** | Traitement automatisé de données destiné à détecter, par l'analyse automatisée de données anonymes, des connexions susceptibles de révéler une éventuelle menace terroriste. | Prévention du terrorisme | 2 mois pour la 1ère autorisation puis renouvelables pour une durée de 4 mois |
| **Géolocalisation en temps réel d'un téléphone portable (L. 851-4 CSI)** | Suivi en temps réel des déplacements d'un individu | Toutes les finalités prévues à l'article L. 811-3 | 4 mois, renouvelables pour une durée équivalente |
| **Localisation en temps réel de personnes, véhicules ou objets ("balises") (L. 851-5 CSI)** | Suivi en temps réel des mouvements d'une personne, d'un véhicule ou d'un objet grâce à la pose d'une balise | Toutes les finalités prévues à l'article L. 811-3 | 4 mois, renouvelables pour une durée équivalente |

[1] *Les autres techniques de renseignement sont décrites plus loin dans le développement du présent rapport, ayant fait l'objet de plusieurs modifications à l'issue de l'adoption de la loi du 24 juillet 2015.*

| Technique | Description | Finalités autorisées | Durée maximale d'autorisation |
|---|---|---|---|
| **Recueil de données par IMSI-CATCHER (L. 851-6 CSI)** | Recueil de données de connexion par un dispositif de proximité, mentionné au 1° de l'article 226-3 du code pénal[1] | Toutes les finalités prévues à l'article L. 811-3 | 2 mois renouvelables |
| **Interceptions de sécurité (L. 852-1 CSI)** | Enregistrement du contenu des communications téléphoniques d'une personne ou de son entourage. | Toutes les finalités prévues à l'article L. 811-3 | 4 mois renouvelables pour une durée équivalente |
| **Interceptions de correspondance avec dispositif de type "Imsi-catcher" (L. 852-1 CSI)** | Accès au contenu des correspondances par le biais d'un dispositif de proximité mentionné au 1° de l'article 226-3 du code pénal, par exemple un IMSI-catcher | Trois finalités : indépendance, intégrité du territoire et défense nationale ; prévention du terrorisme; prévention des atteintes à la form des institutions républicaines. | 48 heures renouvelables pour une durée équivalente |
| **Captation, enregistrement et transmission de paroles et d'images (L. 853-1 CSI)** | Utilisation de dispositifs en vue de capter, d'enregistrer et de transmettre des paroles prononcées à titre confidentiel ou privé ou d'images dans un lieu privé. | Toutes les finalités prévues à l'article L. 811-3 | 2 mois renouvelables pour une durée équivalente ou 30 jours si intrusion dans un lieu privé ou un véhicule. |
| **Captation et recueil de données informatiques (L. 853-2 CSI)** | Utilisation de dispositifs techniques permettant :<br>- soit d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre;<br>- soit d'accéder à ces mêmes données telles qu'elles s'affichent sur l'écran pour l'utilisateur, telle qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues ou transmises par ses périphériques. | Toutes les finalités prévues à l'article L. 811-3 | 30 jours pour l'intrusion dans un système informatique.<br><br>2 mois pour la captation de données sur écran. |

[1] *Ce dispositif technique est similaire à une antenne-relais mobile factice qui se substitue, dans un périmètre donné, aux antennes relais des opérateurs permettant ainsi au service de disposer d'informations sur les terminaux qui s'y sont connectés.*

### 4. Un encadrement précis des conditions de collecte, d'exploitation et de conservation des données

*a) Le maintien du principe de centralisation des données collectées*

Le principe de **centralisation des données collectées** dans le cadre d'une technique de renseignement, qui s'appliquait, depuis 1991, aux interceptions de sécurité et aux accès administratifs aux données de connexion, n'a pas été remis en cause par la loi du 24 juillet 2015. L'article L. 822-1 du code de la sécurité intérieure confie ainsi au Premier ministre l'organisation de la traçabilité des techniques mises en œuvre et la définition des modalités de centralisation des renseignements collectés.

Loin de constituer une simple modalité pratique de mise en œuvre des techniques de renseignement, la centralisation est **un élément essentiel de leur contrôle** : elle est une garantie du respect de la vie privée dans les opérations de collecte et d'exploitation des renseignements, en permettant de s'assurer qu'aucune technique n'est effectuée irrégulièrement ; elle facilite également, *a posteriori*, le contrôle des opérations menées. Comme le relevait déjà la délégation dans son rapport d'activité de 2014 précité, « *le principe de centralisation constitue une condition déterminante pour l'effectivité d'un contrôle des techniques de collecte du renseignement en même temps que pour la modernité/modernisation de celles-ci* ».

Dans les faits, ce rôle de centralisation est **confié au groupement interministériel de contrôle (GIC)** qui, depuis 2016, a acquis le statut de service à compétence nationale et vu ses prérogatives élargies de manière significative.

Outre la centralisation des demandes de techniques de renseignement, le GIC joue un rôle central dans leur mise en œuvre et dans l'exploitation des données collectées. À ce titre, il est notamment chargé :

– **de mettre en œuvre, pour le compte des services de renseignement, les techniques d'accès aux données de connexion[1] et les interceptions de sécurité** auprès des opérateurs de communications électroniques et des fournisseurs de services sur internet, le GIC bénéficiant, pour cette mission, d'un pouvoir de réquisitions ;

– **de centraliser l'exploitation des données ainsi recueillies** auprès de ces opérateurs et fournisseurs. Les données collectées, conservées par le GIC sur ses systèmes d'informations, ne peuvent ainsi être exploitées par les services de renseignement qu'en son sein et sous son contrôle ;

[1] *Sont exécutés par le GIC les recueils de données de connexion en temps différé et en temps réel et les géolocalisations en temps réel.*

– de **centraliser la conservation des données collectées par le biais des autres techniques de renseignement, qui sont mises en œuvre par chaque service de manière décentralisée[1].**

*b) Un encadrement strict de la conservation des données, adapté selon le degré d'atteinte à la vie privée*

Conformément à la jurisprudence de la CEDH, la loi relative au renseignement a strictement **encadré la conservation des données** et informations collectées à l'occasion d'une technique de renseignement.

Des **durées de conservation différenciées** ont été instaurées en fonction du degré d'atteinte à la vie privée par la technique concernée et du degré de sensibilité des données concernées.

Les informations collectées dans le cadre de linterception d'une correspondance ainsi que les enregistrements de paroles prononcées à titre privé font l'objet de la protection la plus forte et ne peuvent être conservés que pendant 30 jours à compter de leur recueil.

A l'inverse, les données de connexion, à l'exception de celles collectées par le biais d'un algorithme, ont une durée de conservation bien supérieure, pouvant aller jusqu'à 4 ans.

**5. Un dispositif de contrôle renforcé**

Corollaire de l'élargissement des compétences des services de renseignement, le **renforcement du dispositif de contrôle** est un axe majeur de la loi du 24 juillet 2015.

Créée en remplacement de la CNCIS, la CNCTR a été **chargée du contrôle externe de la légalité de l'ensemble des techniques** de renseignement autorisées par la loi et **mises en œuvre sur le territoire national**. Elle est garante, à ce titre, du respect du cadre défini par le législateur afin d'assurer le respect des libertés individuelles et, en particulier, de la vie privée.

Le contrôle qu'elle exerce *a posteriori* revêt, en pratique, plusieurs dimensions. Il lui appartient, bien entendu, de contrôler l'existence d'une autorisation, mais elle est également chargée de s'assurer du respect du contenu de l'autorisation délivrée au service ainsi que des règles de conservation et de destruction des données collectées.

Pour assurer sa mission, **la CNCTR bénéficie de prérogatives renforcées** par rapport à la CNCIS.

Elle dispose ainsi d'un « ***accès permanent, complet et direct*** *aux relevés, registres, renseignements collectés, transcriptions et extractions, ainsi*

[1] *La DGSI et la DGSE disposent d'une autorisation de stocker elles-mêmes les données collectées par le biais de certaines techniques de renseignement.*

*qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements* ». Elle est donc autorisée, sur ce fondement, à accéder lorsqu'elle le souhaite, et **sans intermédiation**, à l'ensemble des documents et lieux mentionnés.

La CNCTR est également autorisée à **solliciter du Premier ministre tous les éléments nécessaires à l'exercice de ses missions**, à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux ou qui pourraient conduire à révéler l'identité de sources, de même qu'à **se voir communiquer les rapports de l'inspection des services de renseignement et des autres services d'inspection ministériels**.

Pour garantir l'exercice de son contrôle, le législateur a introduit un délit d'entrave afin de sanctionner ceux qui s'opposeraient à son action[1].

En cas d'irrégularité constatée dans le cadre de l'exercice de son pouvoir de contrôle, la CNCTR peut émettre des recommandations au service concernée, ainsi qu'au ministre de tutelle et au Premier ministre.

Elle dispose enfin d'un **pouvoir de saisine du juge administratif**, en vertu de l'article L. 833-8 du code de la sécurité intérieure, lorsque les suites données par le Premier ministre à ses recommandations sont jugées insuffisantes.

### *C. DES MODIFICATIONS DE LA LOI ONT ÉTÉ APPORTÉES À PLUSIEURS REPRISES DEPUIS 2015 POUR ASSURER TANT LA CONSTITUTIONNALITÉ QUE L'EFFICACITÉ DE L'ACTIVITÉ DE RENSEIGNEMENT*

#### 1. La censure immédiate des dispositions relatives à la surveillance internationale

##### *a) La validation a priori de la loi renseignement par le Conseil constitutionnel, à l'exception des dispositions relatives à la surveillance internationale*

Saisi *a priori* par le Président de la République du projet de loi relatif au renseignement sur le fondement du deuxième alinéa de l'article 61 de la Constitution, le Conseil constitutionnel en a **validé, dans sa décision n° 2015-713 DC du 23 juillet 2015, l'essentiel des dispositions**.

---

[1] *En application de l'article L. 833-3 du code de la sécurité intérieure,* « est puni d'un an d'emprisonnement et de 15 000 euros d'amendes le fait d'entraver l'action de la commission : 1° Soit en refusant de communiquer à la commission les documents et les renseignements qu'elle a sollicités (…) ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ; 2° Soit en communiquant des transcriptions ou des extractions qui ne sont pas conformes au contenu des renseignements collectés (…) ; 3° soit en s'opposant à l'exercice des missions confiées à ses membres aux agents habilités ».

Seules **trois d'entre elles** ont été déclarées **contraires à la Constitution**.

En premier lieu, le juge constitutionnel a **censuré la procédure d'urgence opérationnelle**[1], introduite par le législateur pour assurer l'effectivité de l'action des services de renseignement dans certaines situations, en leur laissant la possibilité de procéder directement à la mise en œuvre de certaines techniques sans l'avis préalable du Premier ministre. Il a en effet considéré qu'en dérogeant à la procédure d'autorisation de droit commun ainsi qu'à la délivrance d'un avis préalable de la CNCTR et en ne prévoyant pas non plus d'information ni du Premier ministre, ni du ministre de tutelle, les dispositions contestées portaient « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* ».

En deuxième lieu, le Conseil constitutionnel a **censuré les dispositions relatives au rattachement budgétaire des crédits de la CNCTR**, considérant que la loi empiétait sur le domaine exclusif des lois de finance et était donc contraire à l'article 34 de la Constitution.

Enfin, s'il a validé l'ensemble des techniques destinées à être mises en œuvre sur le territoire national, le Conseil constitutionnel a, en revanche, **estimé que le législateur n'avait pas épuisé sa compétence s'agissant de l'encadrement des techniques de surveillance internationale**, c'est-à-dire de surveillance des communications émises ou reçues depuis l'étranger.

Sans se prononcer sur le fait de savoir si l'atteinte au droit au respect de la vie privée portée par ces techniques de surveillance internationale était manifestement excessive, le Conseil constitutionnel a estimé « *qu'en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés (...), ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées (...) et de leurs conditions de mise en œuvre, le législateur n'a[vait] pas déterminé les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* ». Il a, en conséquence, **déclaré le régime de la surveillance internationale contraire à la Constitution.**

*b) La définition rapide d'un nouveau cadre juridique de la surveillance internationale*

D'initiative parlementaire, la loi n° 2015-1556 du 30 novembre 2015 *relative aux mesures de surveillance des communications électroniques internationales* est venue préciser le cadre légal des techniques de surveillance internationale afin de combler le vide juridique créé par la censure constitutionnelle.

Ainsi que l'a rappelé le Conseil constitutionnel dans sa décision précitée, les techniques de surveillance internationale, bien que tournées vers

[1] *Cette procédure était codifiée à l'article L. 821-6 du code de la sécurité intérieure.*

le recueil de renseignements à l'étranger, n'en sont pas moins susceptibles de porter également sur des communications émises ou reçues depuis le territoire national et doivent, en conséquence, être entourées de garanties de nature à assurer la protection des droits et libertés constitutionnellement garantis.

Le législateur a, tout d'abord, **strictement défini le champ d'application des mesures de surveillance internationale.** Par principe, en sont exclues les communications dites mixtes, c'est-à-dire qui renvoient à des numéros d'abonnement ou des identifiants techniques rattachables au territoire national. Ainsi, il n'est pas possible d'exploiter les données légalement recueillies au titre de la surveillance internationale pour apprécier la menace que présenterait un résident français en France du fait de ses liens hors du territoire national.

Une exception à ce principe a toutefois été posée. Peuvent ainsi faire l'objet d'une mesure de surveillance internationale les personnes qui communiquent depuis l'étranger en utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national et qui soit faisaient préalablement l'objet d'une autorisation d'interception de sécurité avant de quitter le territoire national, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation.

**Un cadre procédural spécifique a également été défini**. Désormais fixé par les articles L. 854-1 et suivants du code de la sécurité intérieure, le régime de la surveillance internationale repose sur :

1° **La délivrance de deux autorisations successives par le Premier ministre.**

La première porte sur **l'autorisation d'interception** et consiste à définir les réseaux de communications électroniques sur lesquels la surveillance internationale peut être réalisée par les services. Les mesures de surveillance internationale ne portent en effet pas spécifiquement sur des cibles individuellement identifiées, mais sur des objets collectifs (zones géographiques, organisations, groupes).

La seconde vise à **autoriser l'exploitation des données collectées sur ces mêmes réseaux. Elle est délivrée par le Premier ministre**, à la demande du ministre de tutelle concerné. À la différence des techniques de surveillance nationale, ces demandes ne sont **pas soumises, par la loi, à l'avis préalable de la CNCTR.** Toutefois, dans la pratique, à la demande du Premier ministre, la CNCTR a accepté d'exercer un contrôle *a priori* sur ses demandes, effectif depuis mai 2016[1] ;

2° Un **régime spécifique d'exploitation, de conservation et de destruction des renseignements collectés**. Celui-ci prévoit des principes communs avec le régime de droit commun, notamment s'agissant de la

[1] *Délibérations classifiées adoptées en formation plénière les 28 avril et 19 mai 2016.*

traçabilité et de la centralisation des données collectées. Il s'en différencie en revanche fortement s'agissant des durées de conservation des données, qui sont beaucoup plus longues en raison, d'une part, des délais de traduction des correspondances interceptées, qui sont souvent en langue étrangère et, d'autre part, de la situation des personnes sous surveillance, sur lesquelles les capacités d'intervention de l'État français sont plus réduites ;

3° Un **contrôle *a posteriori* par la CNCTR**, qui dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité ainsi qu'aux renseignements collectés, aux transcriptions et extractions réalisées ;

4° Un **contrôle juridictionnel plus limité que dans le droit commun**, les possibilités de recours contre une technique de surveillance internationale n'étant pas ouvert aux particuliers.

### 2. Une redéfinition du périmètre de l' « exception hertzienne »

*a) La censure constitutionnelle*

Les mesures d'interception des communications empruntant la voie hertzienne ont, dès la mise en place du régime d'encadrement des interceptions de sécurité en 1991, été **exclues de tout contrôle par le législateur**, au motif qu'elles étaient assimilables à une surveillance générale du domaine radioélectrique, ne visaient pas de communications individualisables et ne pouvaient pas, dès lors, être de nature à porter atteinte au secret des correspondances.

De fait, les communications empruntant la voie hertzienne utilisent le champ électromagnétique pour transmettre un message et se caractérisent par le fait qu'elles **se propagent dans l'espace public et peuvent, à ce titre, être captées par quiconque dispose d'une antenne émettrice**.

La loi du 24 juillet 2015 n'a pas remis en cause cette exclusion du champ légal des communications hertziennes, communément appelée l' « exception hertzienne », qui a été consacrée à l'article L. 811-5 du code de la sécurité intérieure.

Saisi d'une question prioritaire de constitutionnalité, le Conseil constitutionnel, dans une décision d'octobre 2016[1], a toutefois censuré les dispositions de cet article L. 811-5, considérant que sa rédaction, en permettant « *aux pouvoirs publics de prendre des mesures de surveillance et de contrôle de toute transmission empruntant la voie hertzienne, sans exclure que puissent être interceptées des communications ou recueillies des données individualisables* », *portait « une atteinte manifestement disproportionnée au droit au respect de la vie privée et au respect des correspondances résultant de l'article 2 de la Déclaration de 1989* ».

[1] *Décision n° 2016-590 QPC du 21 octobre 2016.*

*b) La création d'une nouvelle technique de surveillance hertzienne par la loi du 30 octobre 2017*

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a remédié à cette censure. Comme le relevait le rapporteur du projet de loi au Sénat, Michel Mercier, « *la définition d'un nouveau cadre juridique [était] indispensable pour permettre la poursuite de la surveillance des communications radio, notamment internationales, qui, bien que ne constituant qu'une part très réduite des flux mondiaux de communications, demeurent utilisées par des acteurs stratégiques pour les services de renseignement et les forces armées françaises* »[1].

Il a été introduit, à cette fin, un nouveau régime juridique dans le code de la sécurité intérieure, qui distingue deux types de surveillance :

- les **mesures de surveillance concernant les données échangées au sein d'un réseau empruntant exclusivement la voie hertzienne mais conçu pour une utilisation privative** constituent désormais une technique de renseignement à part entière, dite « d'interception par voie hertzienne » et sont soumises au droit commun de la mise en œuvre des techniques de renseignement . Sont notamment concernées par ce régime les communications dites « PMR », c'est-à-dire les communications radio de « point à point », comme les dispositifs *talkies-walkies* ;

- en revanche, les autres communications électroniques empruntant la voie hertzienne, écoutables par toute personne disposant d'un appareil de réception radio, continuent de pouvoir faire l'objet d'une surveillance sans autorisation préalable.

### 3. La nouvelle réforme de la surveillance internationale pour mieux appréhender les menaces transversales

La **loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire** pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense a fait évoluer, une nouvelle fois, le cadre légal des techniques de surveillance internationale, afin d'y intégrer de **nouveaux besoins opérationnels** des services de renseignement.

Afin de tenir compte du caractère plus transfrontalier des menaces, elle a, en particulier, **élargi les conditions d'exploitation des données recueillies dans le cadre des techniques de surveillance internationale pour surveiller des personnes disposant d'un identifiant rattachable au territoire national.**

Mettant fin à l'imperméabilité qui prévalait jusque-là entre les régimes de surveillance nationale et internationale, elle a :

---

[1] *Rapport n° 629 (2016-2017) du 12 juillet 2017 de M. Michel Mercier, fait au nom de ma commission des lois du Sénat sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme.*

– d'une part, autorisé l'exploitation de données collectées dans le cadre d'une surveillance internationale pour **effectuer des vérifications ponctuelles concernant un numéro ou un identifiant rattachable au territoire national**, à des fins de « levée de doute ».

Les services ne sont pas autorisés, sur ce fondement, à surveiller une personne en continu, mais peuvent procéder à des **rapprochements, ponctuels et non répétés dans le temps**, d'un identifiant rattachable au territoire national avec des données collectées dans le but de **détecter une éventuelle corrélation** ;

– d'autre part, **créé un nouveau régime d'exploitation des données collectées dans le cadre d'une surveillance internationale à des fins de surveillance d'une personne située sur le territoire national**[1].

Ce régime d'exploitation ne peut être mis en œuvre que pour cinq des sept finalités de la politique publique du renseignement[2]. Par ailleurs, sur le plan procédural, dans la mesure où le dispositif concerne des personnes résidant sur le territoire national, le régime d'autorisation se rapproche du régime de droit commun encadrant la mise en œuvre des techniques de renseignement sur le territoire national (autorisation du Premier ministre après avis de la CNCTR, nombre d'autorisations en vigueur simultanément contingenté, contrôle *a posteriori* de la CNCTR).

## II. CINQ ANS APRÈS : UN BILAN GLOBALEMENT SATISFAISANT, MAIS DES BESOINS PONCTUELS D'AJUSTEMENT

### *A. LA MISE EN ŒUVRE DE LA LOI DE 2015 A CONSTITUÉ UN DÉFI JURIDIQUE, HUMAIN ET TECHNOLOGIQUE MAJEUR, AUJOURD'HUI EN PHASE D'ACHÈVEMENT*

L'entrée en vigueur de la loi relative au renseignement a constitué, pour les services de renseignement de même que pour les structures afférentes, en particulier le GIC, un défi juridique, humain et technique sans précédent, qui n'a pas été sans impact sur leur fonctionnement et leur organisation.

Les progrès accomplis sont significatifs et ont permis, en quelques années, une appropriation satisfaisante du nouveau cadre légal.

---

[1] *Ce dispositif permet notamment de surveiller les communications émises depuis la France vers l'étranger et qui peuvent difficilement être surveillées par le biais d'une technique de renseignement nationale (par exemple lorsqu'une personne effectue ses communications vers l'étranger dans un cybercafé).*

[2] *L'indépendance nationale, l'intégrité du territoire et la défense nationale ; les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; la prévention du terrorisme ; la prévention de la criminalité et de la délinquance organisée ; la prévention de la prolifération des armes de destruction massive.*

Il n'en demeure pas moins que des investissements demeurent nécessaires pour parfaire l'efficacité du GIC, désormais au cœur du processus de mise en œuvre des techniques de renseignement, ainsi que pour respecter les principes de centralisation et de traçabilité des opérations imposés par le législateur.

### 1. Un cadre juridique lourd et complexe, mais désormais bien assimilé par les services

#### *a) Une appréhension progressive du cadre légal par les services de renseignement*

Au regard de la révolution législative que représentait la loi du 24 juillet 2015, les services de renseignement ont, tous, connu une phase d'appréhension du nouveau cadre légal, tant en terme d'appropriation technique, par les agents de renseignement, du nouveau cadre juridique que d'absorption de la charge de travail induite par les nouvelles procédures d'autorisation et de contrôle.

**Sur le plan humain, l'impact de la loi demeure difficile à estimer** avec précision compte tenu de l'implication de nombreux acteurs, à des niveaux hiérarchiques différents, dans le processus de mise en œuvre d'une technique de renseignement. Interrogés par la délégation, les services ont d'ailleurs été, pour la plupart, dans l'incapacité de fournir des éléments quantitatifs sur les besoins humains nouveaux générés par les nécessités de gestion de la procédure d'autorisation des techniques de renseignement.

La DGSE afourni une évaluation partielle du coût humain, indiquant que 20 ETP étaient entièrement dédiés à l'application du cadre légal, chiffre qui n'inclut cependant pas les exploitants et l'ensemble de la chaîne hiérarchique de la direction du renseignement chargés de rédiger et de valider les demandes de techniques.

Dans les faits, l'adoption, concomitamment à l'entrée en vigueur de la loi du 24 juillet 2015, de plusieurs plans successifs de lutte contre le terrorisme ayant renforcé de manière sensible les ressources humaines de la plupart des services de renseignement, a, sans aucun doute, facilité l'absorption des nouvelles charges induites.

Certains services ont d'ailleurs profité de cette croissance d'effectifs pour renforcer, voire créer des services juridiques chargés de la gestion des techniques de renseignement. La DNRED a ainsi recruté un agent dédié à cette tâche tandis que la DGSI, plus consommatrice en techniques de renseignement, a renforcé sa structure d'appui et de contrôle des techniques de renseignementDe la même manière, compte tenu de l'éparpillement de ses structures sur le territoire national, le SCRT a créé une structure dédiée au niveau de son administration centrale, appelée le guichet unique, composée

de 15 fonctionnaires et qui centralise toutes les demandes de techniques de renseignement formulées par les antennes territoriales.

Au-delà du volume, un **effort important de sensibilisation, d'information et de formation des agents** au nouveau cadre légal a également dû être conduit pour garantir une parfaite appropriation technique du nouveau cadre juridique. C'est ainsi que la DGSI a engagé la formation de plus de 2 500 agents, enquêteurs, opérateurs et responsables hiérarchiques confondus, sur des sessions d'une durée de 2 jours et demie. Le SCRT a, quant à lui, confié à son guichet unique la conduite d'actions de formation régulières auprès des agents territoriaux.

Ainsi que l'a souligné la DGSE, l'effort de formation n'a pas été seulement ponctuel ; il a également été nécessaire, pour les services, de pérenniser des dispositifs de formation de manière à former les personnels aux évolutions du cadre légal ainsi que les nouveaux arrivants.

Enfin, de manière complémentaire aux efforts conduits par chaque service en interne, le développement à compter de 2016, par le GIC, ***** a permis d'accompagner les services dans l'appréhension de ce nouveau cadre légal et de fluidifier les échanges entre les différents acteurs impliqués. C'est sur cette application que les demandes sont désormais saisies par les services et validées par les ministres de tutelle, que la CNCTR donne un avis et que le Premier ministre accorde ou non son autorisation. Cet outil permet en outre aux différents acteurs d'interagir, par exemple de solliciter, de la part des services, la fourniture d'éléments complémentaires à l'appui de leurs demandes.

Consultés par la délégation, **les services de renseignement font état d'un processus désormais fluidifié et normalisé**.

Certains directeurs de service entendus par la délégation **n'excluent pas que la charge procédurale ait pu conduire des services opérationnels à faire des choix en opportunité** et **à renoncer, de manière ponctuelle, à la mise en œuvre de techniques de renseignement**. La délégation observe qu'ont notamment fait part de cette difficulté les services de taille plus réduite disposant des marges de manœuvre les plus faibles sur le plan humain et de services juridiques moins étoffés.

La DGSE a également évoqué une forme de renoncement, mais d'une autre nature, lié moins à la lourdeur des procédures d'autorisation mises en place qu'à la complexité des différents outils et à la nécessité de combiner plusieurs techniques pour atteindre l'objectif recherché. A été donné l'exemple de cas dans lesquels des analystes ont pu renoncer à demander la mise en œuvre d'une technique de renseignement, anticipant des difficultés d'exploitation en raison de leur volume ou du délai restreint de conservation.

Pour autant, il apparaît **exclu, pour la grande majorité des acteurs interrogés par la délégation, que la charge procédurale induite par la loi de**

**2015 ait pu générer une forme d'« autocensure »** généralisée et nuire à l'efficacité de la politique publique de renseignement. En témoigne d'ailleurs l'augmentation constante du nombre de demandes de techniques de renseignement depuis l'entrée en vigueur de la loi (*cf. infra*).

Sur le plan juridique, les services de renseignement paraissent également disposer d'une **bonne maîtrise du cadre légal**. Tous reconnaissent que l'instauration d'un dialogue permanent et constructif avec la CNCTR, lors de l'exercice de son contrôle *a priori*, a permis aux agents d'acquérir une meilleure compréhension des principes nouveaux définis par le législateur.

La **baisse continue, depuis 2015, des avis défavorables de la CNCTR** en est, pour partie, le reflet. Leur taux dans le total des demandes adressées par les services, hors demandes d'accès aux données de connexion, est ainsi **passé de 6,9 % en 2016 à 1,4 % en 2019**.

**Evolution du taux d'avis défavorables rendus par la CNCTR**

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

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

Ces statistiques consolidées masquent, certes, des différences importantes entre services. Certains connaissent ainsi des taux très faibles, systématiquement inférieurs à 1 % (en 2018, 0,45 % pour la DGSI, 0,2 % pour le SCRT, 0,2 % pour la DRPP, 1,3 % pour la DNRED, 0 % pour la DRM), alors que la DGSE et la DRSD présentent des taux bien plus élevés, respectivement de 7 % et de 4,2 % au cours de la même année.

*****

*b) Des souhaits d'assouplissement de la procédure d'autorisation, qui devront être mis en œuvre dans le strict respect de la vie privée et du secret des correspondances*

Ceci étant, plusieurs acteurs ont émis des **souhaits de simplification de la procédure d'autorisation** des techniques de renseignement.

La délégation n'exclut pas, par principe, ces évolutions et demeure ouverte aux modifications du cadre législatif de nature à alléger la charge des services de renseignement comme des autres acteurs impliqués dans la procédure, dès lors toutefois qu'elles ne conduisent pas à fragiliser

l'équilibre atteint entre efficacité de l'action de renseignement et protection des droits constitutionnellement garantis.

A la lumière de ces éléments, plusieurs pistes lui paraissent mériter d'être étudiées.

Il en est tout d'abord ainsi de la proposition formulée par la CNCTR de **simplifier la procédure d'autorisation de l'introduction dans un lieu d'habitation à des fins de retrait d'un dispositif de surveillance**[1]. En l'état du droit, les demandes d'introduction dans un lieu d'habitation, qu'elle qu'en soit l'objectif, sont **examinées par la CNCTR en formation collégiale**. Si cette procédure se justifie au moment de la pose d'un équipement de surveillance, au regard de l'atteinte portée à la vie privée, elle apparaît en revanche **source de complexité** lorsque la demande d'introduction dans un lieu d'habitation est formulée **pour le retrait d'un dispositif** et ne donne, dans les faits, jamais lieu à un avis défavorable. La CNCTR propose, en conséquence, de renvoyer à la procédure de droit commun, soit un de ses membres statuant seul, l'examen des demandes d'introduction dans un lieu d'habitation à des fins de retrait d'un dispositif de surveillance.

La délégation observe que cette analyse rejoint en partie une demande formulée par le service central du renseignement pénitentiaire (SCRP), qui regrette d'être contraint, en cas de problème de maintenance sur un équipement de surveillance placé dans une cellule de détenu, de devoir formuler systématiquement une nouvelle demande d'introduction dans un lieu d'habitation[2].

De l'avis de la délégation, l'allongement de la durée des autorisations de pénétration dans un lieu privé, et, *a fortiori,* dans un lieu d'habitation, serait incertain sur le plan constitutionnel au regard de la forte protection accordée par le Conseil constitutionnel au droit de propriété et au droit au respect de la vie privée.

En revanche, suivant le même raisonnement que la CNCTR, **elle estime possible d'alléger la procédure d'examen des demandes d'introduction dans un lieu d'habitation formulées à des fins de maintenance, en supprimant l'obligation d'avis en formation collégiale**. Bien qu'elle ne soulagerait pas les services de la nécessité de formuler une nouvelle demande, une telle évolution législative permettrait, *a minima*, de raccourcir les temps de procédure, l'avis de la CNCTR étant alors rendu en 24 heures, contre 72 heures dans le cadre d'une procédure d'avis rendu en formation collégiale.

---

[1] *En vertu de l'article L. 853-3 du code de la sécurité intérieure, ne peuvent donner lieu à une introduction dans un lieu privé que les techniques de balisage, de captation de paroles prononcées à titre privé, de captation d'images dans un lieu privé ou de recueil et de captation de données informatiques.*

[2] *En droit, la durée de l'autorisation d'introduction dans un lieu privé pour placer un dispositif de surveillance est limitée à 30 jours, alors que celle des techniques de renseignement qu'elle accompagne atteint deux mois.*

**Recommandation n° 1 : Modifier l'article L. 853-3 du code de la sécurité intérieure afin de renvoyer à la procédure d'avis de droit commun l'examen, par la CNCTR, des demandes de renouvellement des autorisations d'introduction dans un lieu d'habitation à des fins de maintenance ou de retrait de dispositifs techniques de surveillance.**

Sans remettre en cause la gradation des techniques de renseignement mise en place par le législateur en 2015, la délégation considère par ailleurs **envisageable d'allonger la durée d'autorisation de certaines techniques de renseignement**.

Pourrait notamment être concernée la **technique de recueil de données de connexion par un dispositif de proximité de type *IMSI-catcher***, dont la durée, actuellement limitée à 2 mois, pourrait être portée à 4 mois, soit la durée de droit commun. L'atteinte portée à la vie privée et au secret des correspondances par cette technique, qui ne permet pas d'accéder au contenu des correspondances, mais uniquement aux données de connexion, n'est en effet pas plus forte que dans le cadre d'une pose de balise ou d'une géolocalisation en temps réel, dont les durées maximales d'autorisation sont de 4 mois.

De la même manière, la délégation considère **possible d'envisager, comme le souhaitent notamment la DRM et la DGSE, un allongement de la durée d'autorisation d'exploitation des données collectées dans le cadre d'une surveillance internationale**, qui fait déjà l'objet de garanties plus lâches au regard de la nature des données concernées. Actuellement fixée à 4 mois, elle pourrait par exemple être élevée à 6 mois, ce qui ne nécessiterait qu'un renouvellement par an, contre deux aujourd'hui.

S'agissant en revanche de la nouvelle autorisation d'exploitation des données de surveillance internationale à des fins de surveillance d'une personne située sur le territoire national[1], la délégation juge nécessaire de maintenir la durée maximale d'autorisation à 4 mois, afin d'éviter toute distorsion avec les garanties entourant les autres techniques de renseignement soumises à autorisation sur le territoire national.

[1] *Introduite par la loi de programmation militaire pour les années 2019 à 2025, cette autorisation d'exploitation est prévue par le V de l'article L. 854-2 du code de la sécurité intérieure.*

**Recommandation n° 2 : Allonger :**

**- à 4 mois la durée maximale d'autorisation de la technique de recueil de données de connexion par un dispositif de proximité prévue par l'article L. 851-6 du code de la sécurité intérieure ;**

**- à 6 mois la durée maximale d'autorisation d'exploitation des données recueillies dans le cadre d'une surveillance internationale, à l'exception des autorisations d'exploitation données à des fins de surveillance d'une personne située sur le territoire national.**

Au regard des arguments formulés précédemment, la délégation demeure en revanche circonspecte sur la proposition de **simplification de la procédure d'autorisation des demandes d'accès en temps différé à certaines données de connexion[1] formulée par la CNCTR.**

Compte tenu de la faible atteinte à la vie privée de ce type de techniques, la CNCTR estime n'avoir que peu de valeur ajoutée dans la conduite de son contrôle, qui se limite, pour l'essentiel, à un contrôle de l'erreur manifeste d'appréciation. Elle suggère, en conséquence, que la responsabilité du contrôle *a priori* soit confiée au GIC, déjà chargé, de manière centralisée, du recueil des données de connexion auprès des opérateurs, à l'exception des demandes portant sur des personnes bénéficiant par la loi, en raison de leur profession ou du mandat qu'elles exercent, d'une protection particulière (journalistes, avocats, magistrats, parlementaires).

Au regard du volume de dossiers concernés, qui représentent, depuis cinq ans, plus de la moitié du total de demandes traitées par la CNCTR, cette évolution serait, certes, de nature à alléger la charge de la commission et à libérer des ressources pour le renforcement d'autres formes de contrôles. Force est néanmoins de constater d'une part, qu'elle n'aurait que peu d'impact pour les services de renseignement eux-mêmes, qui continueraient de formuler leur demande, d'autre part, qu'elle induirait un **transfert de charge vers le GIC, déjà soumis à des tensions importantes en termes de personnels** (*cf. infra*).

Sur le fond, la délégation **s'interroge au demeurant sur la sécurité juridique, du point de vue constitutionnel, de cette évolution, qui conduirait à confier à une même entité, le GIC, à la fois un rôle de contrôleur et un rôle d'opérateur.**

---

[1] *Données d'identification des numéros d'abonnement ou de connexion à un service de communications électroniques, ainsi qu'aux données de recensement de l'ensemble des numéros d'identification ou d'abonnement d'une personne.*

### 2. Une montée en puissance du GIC qui mérite d'être poursuivie

Au regard de sa position centrale dans le processus de mise en œuvre des techniques de renseignement (*cf.* partie I), le GIC a, à l'instar des services de renseignement, connu une profonde refonte de son organisation de travail à compter de 2015 et changé de dimension, passant, selon les propos de son directeur, d'une simple « officine de mise en œuvre des écoutes » à l'instrument principal du Premier ministre pour assurer la gestion, la mise en œuvre et la traçabilité de techniques de renseignement intrusives.

L'enjeu, pour cette structure, était double : d'une part, assurer la centralisation des demandes de techniques issues d'un nombre élargi de services de renseignement ; d'autre part, en tant qu'opérateur, faire face à l'augmentation massive du nombre de techniques à mettre en œuvre pour le compte des services et, partant, du volume de données collectées.

*a) Un service profondément réorganisé, mais encore sous-doté en effectifs*

Pour accompagner la mise en œuvre du cadre légal, le GIC a été profondément restructuré depuis 2015.

Erigé au statut de service à compétence nationale fin 2016[1], il s'est réorganisé pour absorber pleinement ses nouvelles missions. Il est désormais composé de trois départements, respectivement chargés de la technique, des activités opérationnelles, c'est-à-dire du traitement des flux de demandes adressées par les services, et du fonctionnement.

Déjà sous-doté pour assurer ses missions historiques, il a parallèlement bénéficié, dès 2015, d'un **schéma d'emploi ambitieux**.

D'un effectif de départ de 132 ETP en 2015, la cible à horizon cinq ans a été fixée, en 2015, à 223 ETP, avant d'être revue à la hausse de 20 ETP dès 2016 compte tenu de l'augmentation considérable du recours aux techniques de renseignement par les services dès l'entrée en vigueur de la loi.

Le GIC a, de fait, connu une **augmentation sensible de ses effectifs**, qui ont atteint, en juin 2020, **229 personnels.**

Cette évolution numéraire s'est accompagnée d'une **montée en gamme des personnels recrutés,** rendue nécessaire par le besoin d'automatiser les processus et de déployer de nouvelles structures informatiques pour absorber les flux croissants de techniques. Précédemment composé de personnels relevant majoritairement des catégories B et C de la fonction publique au regard de ses missions d'exécution, le GIC a ainsi réorienté sa structure d'emploi vers des profils

[1] *Décret n° 2016-1772 du 20 décembre 2016.*

techniques plus qualifiés relevant de la catégorie A (informaticiens, experts réseaux, ingénieurs, chefs de projets).

Bien qu'il soit parvenu à changer d'échelle en seulement quelques années, le service est confronté, depuis deux ans, à des **difficultés de recrutement,** en particulier dans les secteurs des finances, des achats et de la logistique, qui se traduisent par un écart croissant entre les effectifs prévisionnels et les effectifs réalisés et on conduit à reporter à 2021 le schéma d'emploi initialement prévu pour 2020.

**Schéma d'emploi et effectifs réels du GIC depuis 2015 (en ETP)**

| | **2015** | **2016** | **2017** | **2018** | **2019** | **2020** *(au 1er juin)* |
|---|---|---|---|---|---|---|
| Effectifs prévisionnels | 132 | 160 | 200,6 | 215,6 | 230,6 | 243,6 |
| Effectifs réalisés (au 31 décembre) | 132 | 151 | 201 | 194 | 218 | 229 |

Le présent rapport n'a pas pour ambition de formuler des recommandations pour faire face à ces difficultés, qui ont déjà fait l'objet, l'an passé, de développements détaillés par la délégation.

Il n'en demeure pas moins que la croissance continue des demandes de techniques de renseignement ainsi que les **besoins nouveaux qui pourraient découler tant des évolutions envisagées de la loi de 2015 que des évolutions techniques** susceptibles d'être rendues nécessaires, par exemple par l'entrée en vigueur de la 5G, l'incitent à rappeler ses inquiétudes quant aux difficultés de recrutement et à la sous-dotation en personnels de cette structure et à réitérer, en conséquence, ses recommandations.

*b) Des capacités techniques freinées par des difficultés d'hébergement*

Parallèlement à l'augmentation de ses effectifs, l'évolution du rôle du GIC dans l'environnement du renseignement a nécessité **d'importants investissements dans le but de déployer de nouvelles infrastructures techniques**, rendues nécessaires non seulement par les nouvelles exigences légales introduites par la loi de 2015, mais également par l'augmentation du flux de techniques à mettre en œuvre et, de manière incidente, à l'augmentation du volume de données stockées.

Outre la **dématérialisation du circuit d'instruction des demandes de technique de renseignement** précédemment évoqué, le GIC a engagé, dès 2016, d'importants **programmes de développements techniques**, afin de

faciliter la collecte et la centralisation du renseignement, pour les techniques qu'il est chargé de mettre en œuvre de même que pour certaines des techniques déployées directement par les services (*cf. infra*).

Parallèlement, dans le cadre de son activité historique de recueil de données de connexion et d'interceptions de sécurité, le groupement est confronté à une **nécessité de moderniser et d'adapter en permanence ses dispositifs d'accès aux communications** à l'évolution des normes techniques.

Enfin, pour faire face à l'augmentation exponentielle du volume de données qu'il est amené à stocké, **ses capacités techniques, initialement situées sur son site parisien, ont dû être étendues à un second site, situé en province.**

Cette extension immobilière demeure toutefois, pour l'heure, très insuffisante. Au-delà de la capacité d'accueil des nouvelles recrues, elle **fragilise également les infrastructures de stockage et de traitement,** le manque de place conduisant les équipes informatiques du groupement à des pratiques de développement non conformes aux règles de l'art.

Il a été indiqué à la délégation que cette situation était **en phase d'être résolue**. Il a en effet été procédé, à la fin de l'année 2018, à l'acquisition d'un nouveau bâtiment. D'importants travaux de rénovation étant programmés, notamment en vue d'accueillir un nouveau centre de données, il ne pourra toutefois être ouvert qu'en 2021, ce qui, d'ici là, risque de contraindre les conditions de travail du GIC.

### 3. L'enjeu de la centralisation et de la traçabilité des données collectées : des efforts à poursuivre en dépit des progrès accomplis

Au-delà de l'appréhension du nouveau cadre légal, l'entrée en vigueur de la loi du 24 juillet 2015 a posé un défi technique majeur à la communauté du renseignement : celui de la centralisation des données collectées et de la traçabilité des opérations d'exploitation, qui, comme évoqué précédemment, constituent une garantie majeure imposée par le législateur pour assurer un contrôle effectif du respect du cadre légal par la CNCTR.

*a) Des progrès accomplis en matière de centralisation des données collectées*

La CNCTR a, à plusieurs reprises, rappelé les conditions d'une centralisation réussie et, ce faisant, de la conduite, par ses membres, d'un contrôle effectif de la mise en œuvre des techniques de renseignement :

- l'existence de systèmes d'information et de réseaux de communication solides et sécurisés ;

• le développement d'outils de consultation et d'exploitation à distance des données collectées, pour éviter que la centralisation ne soit qu'un leurre et que ne soient conservées parallèlement, de manière décentralisée, des copies des données ;

• la limitation et le regroupement des lieux de stockage.

Pour satisfaire ces exigences, **deux modèles distincts** ont été suivis.

A l'instar de ce qui se faisait jusqu'alors, le GIC a, assez logiquement, conservé la mission de centraliser la conservation et l'exploitation des données qu'il est amené lui-même à collecter dans le cadre des techniques de renseignement dont il assure la mise en œuvre pour le compte des services, à savoir les accès aux données de connexion, les interceptions de sécurité et la géolocalisation en temps réel.

Pour faciliter l'exploitation au plus près du terrain, y compris par les antennes territoriales des services de renseignement, le GIC a accompagné le mouvement de centralisation du déploiement de nouveaux centres d'exploitation sur le territoire national. 7 nouveaux sites ont été ouverts depuis 2016, qui se sont ajoutés aux 28 sites qui préexistaient à l'adoption de la loi de 2015.

La **centralisation des données collectées de manière décentralisée, dans le cadre de techniques dites de proximité**, constitue **un enjeu technique plus important au regard de l'éparpillement des structures de collecte.**

En l'espèce, il a été acté, dès l'entrée en vigueur de la loi, que la DGSI et la DGSE, au regard tant de leurs capacités techniques que des volumes de données collectées, déploieraient et assureraient la gestion de leurs propres dispositifs de centralisation pour les techniques de balisage, de captations de paroles et d'images ainsi que de recueil et de captation de données informatiques. La CNCTR fait le constat que d'importants efforts ont été conduits par ces deux services pour se conformer à ses exigences. Des progrès demeurent toutefois encore à accomplir, en particulier par la DGSE, pour assurer la centralisation au niveau de son administration centrale des renseignements collectés par le biais de techniques de proximité.

S'agissant des autres services spécialisés du renseignement et des services du second cercle, le GIC s'est engagé à leur apporter son assistance dans la construction des dispositifs de centralisation.

D'ores et déjà, d'importants chantiers ont pu être engagés, et, pour certains, achevés. Depuis janvier 2017, un **système centralisé de conservation centralisée des données collectées dans le cadre de la technique de balisage**, associé à une plateforme de consultation à distance, est ainsi opérationnel et pleinement utilisé par l'ensemble des services de renseignement, hors DGSE et DGSI.

Le GIC a également initié, en 2017, le développement d'un **dispositif technique destiné à centraliser**, au sein de son propre système d'information, **les paroles et les images captées** sur le fondement de l'article L. 853-1 du code de la sécurité intérieure, qui pourront être exploitées par les agents de renseignement au sein des centres territoriaux du GIC voire, à terme, à distance depuis leurs propres locaux. Ce dispositif est aujourd'hui déployé à la DNRED, au SCRT, à la sous-direction de l'anticipation opérationnelle de la gendarmerie, à la DRPP, au SNRP ainsi qu'à la direction centrale de la police judiciaire. Selon les informations communiquées à la délégation, l'automatisation du transfert des données collectées en vue de leur centralisation dans les systèmes d'information du GIC demeure encore partielle : seules les paroles et images recueillies sur des systèmes compatibles avec les plateformes du GIC sont téléchargées « en ligne », les autres l'étant, manuellement, par les services.

Parallèlement à ces actions, ceux des services de renseignement qui n'ont pas souhaité ou n'ont pas pu reposer sur les dispositifs déployés par le GIC se sont attelés au développement d'applications informatiques unifiées et sécurisées afin de permettre une conservation et une exploitation centralisée, au niveau de leurs administrations centrales, des données collectées dans le cadre de techniques de renseignement.

En dehors de la DGSE et de la DGSI, qui ont déployé leurs propres systèmes de centralisation, cela concerne principalement la DRM qui, afin de se conformer aux nouvelles règles de contrôle, a adapté et rapatrié dans des entrepôts les données interceptées qui étaient préalablement conservées de manière décentralisée, au sein de tous les postes.

En dépit de ces avancées majeures, des **progrès sont encore à accomplir pour parfaire les dispositifs de centralisation**. Plusieurs techniques, en particulier le recueil de données de connexion par *IMSI catcher*[1] ainsi que le recueil et la captation de données informatiques[2], se caractérisent encore en effet par **une collecte et une conservation disparate**. A cet égard, la CNCTR relève que certains services continuent, faute de réseau informatique suffisamment sécurisé capable d'acheminer des données sensibles, à conserver les données collectées de manière décentralisée, au sein de leurs antennes territoriales.

L'achèvement de ce processus de centralisation ne pourra, compte tenu de l'ampleur des investissements techniques à conduire et des contraintes d'hébergement physiques rencontrées actuellement par le GIC, **que s'inscrire dans la durée**.

Il a d'ores et déjà été indiqué à la délégation que le dispositif de centralisation mis en place pour la centralisation des paroles et des images pourrait être utilisé, à terme, pour centraliser les données informatiques

[1] *Art. L. 851-6 du code de la sécurité intérieure.*
[2] *Art. L. 853-2 du code de la sécurité intérieure.*

captées ou recueillies conformément à l'article L. 853-2 du code de la sécurité intérieure. Le besoin opérationnel demeure toutefois peu établi, dès lors que ces techniques sont pour l'heure principalement utilisées par la DGSI et la DGSE, qui disposent de leurs propres dispositifs de centralisation.

Dans la continuité de ce qui a été opéré jusqu'à présent, elle invite les services, en collaboration avec le GIC, à **engager une réflexion sur une possible prise en compte, dans ce même dispositif, des données de connexion recueillies *via* des dispositifs de proximité de type *IMSI-catcher***, bien que le recours à cette technique demeure, en volume, plus résiduel.

*b) Une traçabilité de l'exploitation des données encore perfectible*

L'article L. 822-1 du code de la sécurité intérieure impose aux services de renseignement d'établir un « *relevé de chaque mise en œuvre d'une technique de recueil de renseignement* », mentionnant « *les dates de début et de fin de cette mise en œuvre ainsi que la nature des renseignements collectés* ».

La CNCTR a eu l'occasion de faire état, dans le cadre de ses derniers rapports d'activité, des progrès accomplis, bien que de manière encore hétérogène, par les services de renseignement, dans la rédaction de ces relevés, communément appelés « fiches de suivi et de traçabilité ».

La principale marge de progression paraît aujourd'hui résider dans le **développement encore très inégal, selon les services, de dispositifs de traçabilité des consultations, des transcriptions et des extractions des données**, qui pèse, indéniablement, sur la capacité de la CNCTR à conduire un contrôle complet et efficace. Comme elle le relevait dans son rapport d'activité pour l'année 2018, « *le contrôle de l'existence même des transcriptions et extractions et, partant, celui de leur bien-fondé et de leurs conformité aux finalités légales peuvent s'en trouver fragilisés* ».

Avant même d'affecter le contrôle de légalité externe, l'absence de traçabilité complète du processus de traitement du renseignement technique soulève des **questions sérieuses quant à la capacité des services à exercer un contrôle interne** pertinent sur la mise en œuvre des techniques de renseignement. Déjà en 2015[1], la délégation rappelait la nécessité, pour les services de renseignement du premier comme du second cercle, d'organiser des mécanismes de contrôle interne renforcés, à toutes les étapes de la collecte de renseignement et de leur transmission, observant à cet égard : « *les nouvelles techniques sont mises en œuvre à partir de l'enquêteur, qui collecte les données et les exploite lui-même, directement. Ce n'est donc que dans un second temps qu'il les transmet à l'organe de contrôle. Se pose donc la question nouvelle de la non-altération du renseignement transféré aux organismes de contrôle* ».

---

[1] *Rapport n° 423 (Sénat, 2015-2016) et n° 3524 (Assemblée nationale, XIV^e législature), fait par M. Jean-Pierre Raffarin au nom de la délégation parlementaire au renseignement.*

A la lumière des témoignages recueillis par la délégation, il semblerait que les difficultés dont a fait état la CNCTR ne soient **pas uniquement liées aux difficultés des services de taille plus modeste** à achever, faute de ressources humaines, financières et techniques suffisantes, la mise en œuvre de ces dispositifs, mais **également, dans certains cas, à des carences de certains services dans l'organisation de cette traçabilité et dans la production des « fiches de traçabilité ».**

La délégation **regrette, en dépit de ses sollicitations, n'avoir pu obtenir d'informations plus précises sur les insuffisances effectivement observées de même que sur les services concernés**.

Faute de pouvoir formuler, en conséquence, de recommandation précise, elle estime nécessaire que le Premier ministre, auquel la loi confie la responsabilité d'assurer la traçabilité des techniques de renseignement, **diligente une mission de l'inspection des services de renseignement pour dresser un état des lieux de la mise en œuvre, par les services de renseignement, de cette exigence légale** essentielle à l'exercice d'un contrôle adéquat, et, plus globalement, des dispositifs de contrôle interne instaurés pour sécuriser les procédures de demande et de traitement des techniques de renseignement.

**Elle demande à ce que les résultats de cette inspection puissent lui être communiqués.**

**Recommandation n° 3 : Confier à l'inspection des services de renseignement une mission de contrôle de la mise en œuvre, par les services du premier cercle ainsi que les services listés par décret en application de l'article L. 811-4 du code de la sécurité intérieure, de l'exigence de traçabilité définie par le législateur et, plus globalement, des dispositifs de contrôle interne instaurés pour sécuriser les procédures de demande et de traitement des techniques de renseignement.**

**Communiquer à la délégation parlementaire au renseignement les résultats de cette inspection.**

Pour les services les plus petits, en particulier ceux relevant du second cercle, pour lesquels l'investissement dans un système de traçabilité peut se révéler complexe, il conviendrait de **favoriser autant que possible les mutualisations et partages d'expérience avec les services ayant déjà procédé au développement de dispositifs renforcés de traçabilité**.

La délégation a noté, à cet égard, que la DGSI avait développé et mis en production, dès la fin de l'année 2015, son propre outil interne de traitement des techniques de renseignement, qui permet de suivre son évolution du stade de la demande initiale formulée par l'enquêteur jusqu'à l'exploitation des données collectées. Ainsi qu'elle l'a indiqué à la délégation, la DGSI est aujourd'hui en capacité de procéder à l'industrialisation de ce dispositif et pourrait, le cas échéant, le déployer au sein d'autres services.

**Recommandation n° 4 : Favoriser les mutualisations et les partages d'expérience sur la mise en œuvre de dispositifs de traçabilité. Etudier la possibilité de déployer le dispositif informatique de traitement des techniques de renseignement de la DGSI au sein des services du second cercle.**

### *B. LES POSSIBILITÉS DE SURVEILLANCE OFFERTES PAR LA LOI RENSEIGNEMENT SONT AUJOURD'HUI PLEINEMENT EXPLOITÉES PAR LES SERVICES, BIEN QUE DE MANIÈRE ENCORE DISPARATE*

#### 1. Une utilisation des techniques de renseignement en hausse constante depuis l'entrée en vigueur de la loi

##### *a) Un nombre de demandes qui n'a cessé de croître, bien que de manière contrastée selon les techniques*

Conséquent dès l'entrée en vigueur de la loi, le nombre de demandes de techniques de recueil de renseignement mises en œuvre sur le territoire national connaît, depuis, une **hausse constante d'environ 3 % par an.**

Au total, il a **augmenté d'environ 8,5 % en quatre ans**, passant de 69 083 demandes en 2016 à 75 082 demandes en 2019, toutes techniques confondues[1].

On constate une évolution similaire du nombre de personnes surveillées par le biais de techniques de renseignement. Selon les données communiquées à la délégation par la CNCTR, 22 210 cibles ont fait l'objet d'au moins une technique de renseignement (hors accès aux données de connexion en temps différé) en 2019, contre 20 360 en 2019, soit une augmentation de 9 % en quatre ans.

L'augmentation des demandes de techniques de renseignement est, du moins pour partie, la **conséquence des progrès faits par les services dans l'appréhension du nouveau cadre légal et des procédures**, qui conduisent les agents à davantage anticiper le recours au renseignement technique. Elle résulte également, pour certains services, de **la hausse du nombre d'agents de renseignement** et de l'augmentation conséquente de leur activité. Tel est notamment le cas pour la DGSI, dont le volume de demandes de mises en œuvre de techniques de renseignement a augmenté d'environ 30 % par an depuis 2016, soit un rythme de progression dix fois supérieure à la moyenne des services. Enfin, certains services, comme la DGSE et la DNRED, ont fait état d'un besoin croissant de recourir au renseignement technique au regard de l'évolution des menaces et de l'actualité internationale, ainsi que de la **technicité croissante des méthodes employées par les cibles** visées.

[1] *Ces chiffres n'incluent pas les techniques de surveillance internationale.*

Cette tendance à la hausse reflète toutefois des **réalités contrastées**.

Il est d'usage, à cet égard, de distinguer deux catégories de techniques : les accès aux données de connexion en temps différé et les autres techniques, qui se caractérisent par leur plus fort degré d'intrusivité.

Les accès aux données de connexion en temps différé représentent, en volume, la **part la plus importante des demandes de techniques** de renseignement. En 2019, 39 726 demandes ont ainsi été formulées par les services de renseignement, soit près de 53 % du total. Le recours à ces techniques connait toutefois une baisse progressive et s'est réduit, entre 2016 et 2019, de 18 %, sans que les raisons de cette évolution n'aient pu, à ce jour, être clarifiées, ni par la CNCTR, ni par les services eux-mêmes.

A l'inverse, le **recours aux techniques de renseignement plus intrusives** tend à s'accentuer depuis l'entrée en vigueur de la loi.

**Evolution du nombre de demandes de certaines techniques de renseignement soumises à autorisation sur le territoire national[1]**

| Technique | Référence | 2016 | 2019 | Evolution 2016/2019 |
|---|---|---|---|---|
| **Interceptions de sécurité** | L. 852-1 | ***** | ***** | ***** |
| **Géolocalisation en temps réel** | L. 851-4 | ***** | ***** | ***** |
| **Données de connexion en temps réel** | L. 851-2 | ***** | ***** | ***** |
| **Balisage** | L.851-5 | ***** | ***** | ***** |
| **Recueil de données de connexion par *IMSI-catchers*** | L. 851-6 | ***** | ***** | ***** |
| **Enregistrements de parole** | L. 853-1 | ***** | ***** | ***** |
| **Enregistrements d'images** | L. 853-1 | ***** | ***** | ***** |
| **Recueil de données informatiques** | L. 853-2 | ***** | ***** | ***** |
| **Captation de données informatiques** | L. 853-2 | ***** | ***** | ***** |
| **Introduction dans un lieu privé** | L. 853-3 | ***** | ***** | ***** |

Les besoins forts liés à l'usage des interceptions de sécurité a d'ailleurs nécessité, à deux reprises, une augmentation du contingentement

[1] *Ces chiffres sont issus des statistiques fournies annuellement par la CNRLT dans le cadre du rapport annuel d'activité des services de renseignement.*

prévu par le législateur et arrêté par le Premier ministre : fixé à 2 700 autorisations simultanément en vigueur lors de l'entrée en vigueur de la loi, il a été augmenté à 3 040 en 2017, puis à 3 600 en 2018.

**Les techniques de renseignement soumises à contingentement**

Quatre techniques de renseignement sont soumises, par la loi, à un contingentement, qui implique que le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par arrêté du Premier ministre après avis de la CNCTR :

- les interceptions de sécurité prévues à l'article L. 852-1 du code de la sécurité intérieure ;

- le recueil des données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure ;

- le recueil de données de connexion par *IMSI catcher* prévu par l'article L. 851-6 du même code ;

- l'exploitation des données collectées dans le cadre d'une surveillance internationale à des fins de surveillance d'identifiants rattachables au territoire national, prévu par le V de l'article L. 854-2 du code de la sécurité intérieure.

Ainsi que le rappelle la CNCTR dans son rapport d'activité de 2018, le principe du contingentement « *est conçu comme une incitation pour les services de renseignement à mettre un terme aux autorisations devenues inutiles avant de pouvoir en obtenir de nouvelles et, de manière générale, à ne recourir à la technique concernée* "que dans les seuls cas de nécessité d'intérêt public prévus par la loi" ».

Le Conseil constitutionnel a élevé ce principe parmi les garanties essentielles permettant d'opérer une conciliation équilibrée entre la prévention des atteintes à l'ordre public et le respect au droit de la vie privée. Il a ainsi jugé contraire à la Constitution l'extension à l'entourage de la personne concernée par une autorisation de la technique du recueil de données de connexion en temps réel, faute, pour le législateur, d'avoir fixé un nombre maximal d'autorisations (décision n° 2017-648 QPC du 4 août 2017, *La Quadrature du net et autres*).

Le contrôle du respect du contingentement est, en pratique, effectué par le GIC, qui centralise l'ensemble des demandes de techniques de renseignement.

*****

**Seules deux techniques soumises à autorisation sur le territoire nationale demeurent, en définitive, peu utilisées**, et ce de manière constante depuis l'entrée en vigueur de la loi :

— d'une part, la **captation de données informatiques**, *****. L'absence de recours à cette technique serait liée d'une part, à la difficulté à différencier d'un point de vue opérationnel cette technique de celle du recueil de stock de données informatique et, d'autre part, à la difficulté opérationnelle pour les services à la mettre en œuvre dans certains cas.

Dans les faits, le recueil de données informatiques, qui permet un accès au stock de données contenues dans des équipements informatiques, a donc été systématiquement privilégié par les services, en accord avec la CNCTR. Par soucis de simplification, il conviendrait dès lors de simplifier l'article L. 853-2 du code de la sécurité intérieure pour ne prévoir qu'une seule et même définition de l'accès aux données informatiques.

Les durées d'autorisation des deux techniques étant actuellement différentes – 60 jours pour la captation de données en temps réel et 30 jours pour le recueil de données stockées -, il est proposé d'aligner le régime sur la durée la plus longue, par ailleurs appliquée pour d'autres techniques tout aussi intrusives, comme la captation de paroles et d'images dans un lieu privé par exemple ;

— d'autre part, *****. Selon les informations communiquées à la délégation, les conditions strictes prévues par la loi, en particulier les finalités limitées de la technique et la durée courte de conservation, de 48 heures, n'auraient trouvé à être réunies que dans un nombre réduit de cas. Pour la DGSI cependant, le maintien de cette technique dans la loi est essentiel et pourrait notamment se révéler utile en cas d'imminence d'un attentat terroriste.

**Recommandation n° 5 : Modifier l'article L. 853-2 du code de la sécurité intérieure afin de prévoir une modalité unique de collecte de données informatiques, plus conforme aux besoins opérationnels des services.**

*b) Des nouvelles capacités de surveillance internationale rapidement prises en main par les services*

La délégation n'a pu obtenir de chiffres consolidés sur la mise en œuvre, depuis 2015, des techniques de surveillance des communications internationales, dans la mesure où celles-ci n'étaient pas légalement soumises, jusqu'en 2018, à un contrôle *a priori* par la CNCTR et ne faisaient dès lors l'objet d'aucune comptabilisation officielle[1].

Selon les données communiquées individuellement par les services ayant répondu à la sollicitation de la délégation, il peut toutefois être observé, à l'instar des techniques domestiques, une **hausse constante, depuis 2015, des demandes d'autorisations d'exploitation de données collectées dans le cadre d'une surveillance internationale**[2].

[1] *Pour rappel, jusqu'en 2018, les autorisations d'exploitation de données collectées dans le cadre d'une surveillance internationale était délivrée par le Premier ministre, sans avis préalable de la CNCTR.*

[2] *Jusqu'en 2018, deux types d'autorisations d'exploitation des données collectées dans le cadre d'une surveillance internationale existaient : d'une part, l'autorisation d'exploitation non individualisée, d'une durée d'un an ; d'autre part, l'autorisation d'exploitation individualisée des données de*

*****

Depuis l'entrée en vigueur de la loi de programmation militaire pour les années 2019 à 2025 et l'élargissement des possibilités d'exploitation des données collectées dans le cadre de la surveillance internationale, **3 104 demandes d'autorisations d'exploitation de communications internationales interceptées** ont été formulées au total par les services auprès de la CNCTR, dont **971 au cours des derniers mois de l'année 2018 et 2 133 en 2019**[1].

Il a été indiqué à la délégation que les **nouvelles capacités d'exploitation** des données collectées dans le cadre d'une surveillance internationale à des fins soit de levée de doute, soit de surveillance d'une personne située sur le territoire national **avaient été rapidement et pleinement utilisées par les services de renseignement**. Elles ont en effet conduit à élargir le recours à la surveillance internationale à des services qui y recourraient peu jusque-là, en particulier les services de sécurité intérieure, principalement amenés à traiter des cibles situées sur le territoire national.

*****

Sur le plan qualitatif, l'introduction des nouvelles mesures par le législateur semble avoir été à la hauteur des résultats escomptés et aurait **permis de combler un vide laissé par la loi du 24 juillet 2015**.

*****

Les évolutions du régime de la surveillance internationale offrent par ailleurs des **possibilités de surveillance nouvelles**. *****

*****

*c) Des techniques principalement mises en œuvre aux fins de prévention du terrorisme et de la criminalité organisée*

Deux finalités représentent, en volume, les deux tiers environ des techniques de renseignement demandées[2] :

- d'une part, la **prévention du terrorisme**, qui a justifié à elle seule 38,2 % des demandes en 2019[3], soit 29 288 demandes au total, mais dont la part tend à se réduire (44,6 % des demandes en 2018) ;

- d'autre part, la **prévention de la délinquance et de la criminalité organisées**, dont la part est restée stable au cours des deux dernières années (invoquée respectivement dans 17,3 % et 18,4 % des demandes en 2018 et 2019).

---

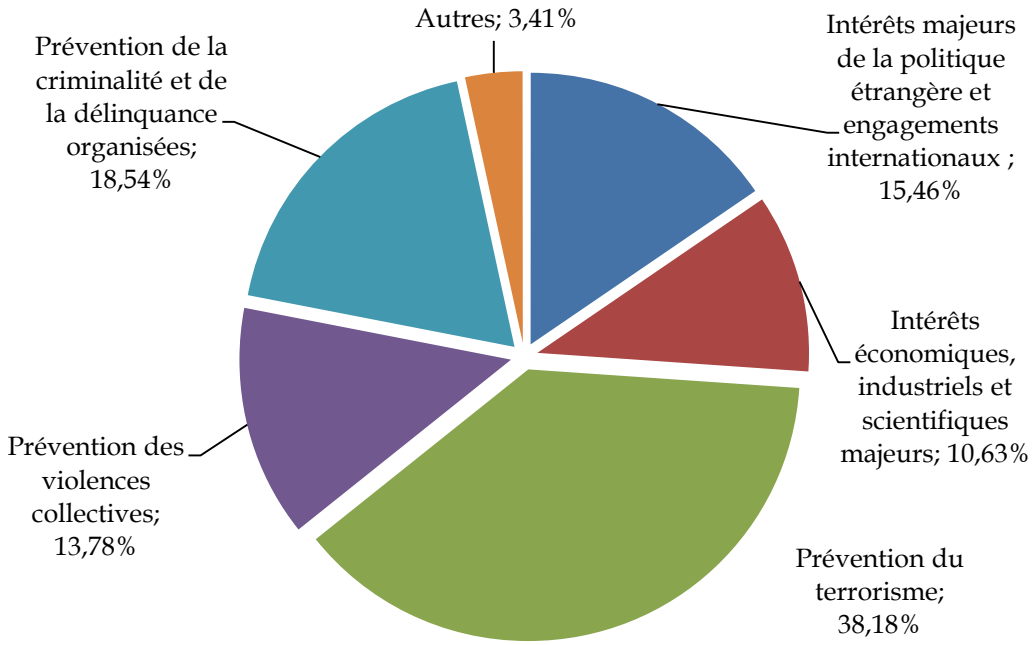
*connexion ou des communications. Les chiffres communiqués à la délégation ne distinguent pas ces deux types d'autorisation.*

*[1] Ces statistiques comprennent l'ensemble des exploitations soumises à un avis préalable de la CNCTR, qu'elles concernent ou non des identifiants rattachables au territoire national.*

*[2] Ces statistiques découlent des données chiffrées communiquées à la délégation par la CNCTR.*

*[3] Une même technique peut être invoquée pour plusieurs finalités.*

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




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

Viennent ensuite :

• la **protection des intérêts majeurs de la politique étrangère et des engagements internationaux**, invoquée dans environ 15 % des demandes de techniques en 2018 comme en 2019 ;

• la **prévention des violences collectives**, qui a connu une hausse sensible, étant passé de 9,5 % des demandes en 2018 à 13,8 % des demandes en 2019, notamment sous l'effet de la mobilisation des services de sécurité intérieure dans le cadre du mouvement des « gilets jaunes » ;

• la **protection des intérêts économiques, industriels et scientifiques majeurs de la nation,** qui, en 2018 comme en 2019, a été invoqué dans environ 15 % des demandes de techniques.

Les autres finalités, bien qu'essentielles, ne mobilisent que faiblement le renseignement technique.

**La part de chacune de ces finalités varie, bien évidemment, selon les services et leurs missions**. Ainsi, pour ne citer que les services les plus demandeurs en techniques de renseignement, l'essentiel du renseignement technique de la DGSI se concentre sur trois finalités : la lutte contre le terrorisme d'une part, à hauteur de près de 60 %, la protection des intérêts majeurs de politique étrangère, à hauteur de 22 % et la prévention des

violences collectives, à hauteur de 13 %[1]. Quant à la DGSE, elle recourt aux techniques de renseignement pour deux principales finalités : la protection des intérêts économiques, industriels et scientifiques majeurs de la nation, dans 60 % des cas, et la protection des intérêts majeurs de politique étrangère, dans environ 25 % des cas.

### 2. L'algorithme : des résultats en deçà des attentes

Eu égard à son caractère novateur et aux craintes qu'il a pu susciter lors des débats parlementaires, **la technique dite de l'algorithme a reçu une application temporaire.**

Initialement fixée au 31 décembre 2018, l'échéance a été repoussée de deux ans par la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, soit jusqu'au 31 décembre 2020, au regard de la mise en œuvre tardive des premiers algorithmes.

Le renouvellement de la technique ou sa pérennisation nécessitant une approbation du législateur, la délégation s'est penchée, dans le cadre de ses travaux, sur l'application de cette technique, dans l'objectif d'éclairer le parlement sur la nécessité de la proroger ou non.

*a) Une technique strictement encadrée par le législateur*

Définie à l'article L. 851-3 du code de la sécurité intérieure, la technique de l'algorithme consiste, **pour la seule finalité liée à la prévention du terrorisme**, à imposer aux opérateurs ou fournisseurs de communications électroniques de mettre en œuvre sur leurs réseaux des traitements automatisés afin de détecter des connexions susceptibles de révéler une menace terroriste.

L'algorithme n'est donc rien d'autre qu'un programme informatique destiné à analyser les flux de données transitant par les équipements des opérateurs de communications électroniques en vue de détecter, en fonction de paramètres définis à l'avance, la menace que pourrait représenter une personne.

**Le degré d'ingérence potentielle d'une telle technique dans la vie privée a justifié qu'elle soit entourée d'importantes garanties**.

Outre la limitation de son champ d'application à la finalité de prévention du terrorisme, la procédure d'autorisation de la mise en œuvre de l'algorithme a été strictement encadrée : il ne peut ainsi être mis en œuvre que pour une durée initiale de deux mois renouvelée par période de quatre mois, après avis préalable de la CNCTR sur le dispositif technique envisagé et les paramètres retenus.

---

[1] *Ces statistiques portent sur l'année 2019.*

S'agissant du fonctionnement de la technique en elle-même, il a été **prévu que ne puissent être analysées que les données de connexion**, le traitement des données de contenu des communications étant exclu. En outre, il a été précisé que le traitement automatisé **ne doit en aucun cas permettre d'identifier les personnes** auxquelles les données de connexion analysées se rapportent. Ce n'est que dans un second temps qu'un service, en cas de révélation d'une menace terroriste, peut demander l'autorisation au Premier ministre de « lever l'anonymat », après avis de la CNCTR, sur les données de connexion en question et de les conserver.

*b) Une utilisation tardive et à l'efficacité encore perfectible*

Compte tenu de la complexité technique du dispositif et des demandes d'ajustement formulées par la CNCTR[1] sur les premiers dispositifs qui avaient été envisagés par le Gouvernement, la mise en œuvre effective du premier algorithme est intervenue tardivement, en 2017[2], soit près de deux ans après son autorisation par le législateur. Deux nouveaux algorithmes ont depuis été autorisés et mis en place au cours de l'année 2018.

Sur les **trois algorithmes actuellement actifs**, deux sont gérés par la DGSI et un par la DGSE. Leur mise en œuvre a toutefois été confiée au GIC, selon la recommandation formulée par la CNCTR, et leur usage limité, pour l'heure, à la **lutte contre le terrorisme islamiste**.

Sur le plan technique, la CNCTR s'est dite satisfaite des conditions de fonctionnement des algorithmes et affirme n'avoir, à ce jour, pas détecté d'irrégularité majeure dans leur utilisation.

En ce qui concerne l'efficacité et l'utilité de la technique, il ressort des auditions et déplacements conduits par la délégation qu'en dépit de premiers résultats encourageants, ce dispositif technique n'a pas encore donné tous les résultats escomptés.

Conformément à l'article 25 de la loi du 24 juillet 2015, le Gouvernement a remis au parlement un rapport sur l'application de l'article L. 851-3 du code de la sécurité intérieure, le 30 juin 2020, soit après l'adoption du présent rapport. Une annexe classifiée a été remise à la même date à la délégation parlementaire au renseignement.

Ces deux rapports confortent l'existence de premiers résultats encourageants, mais également l'existence de marges d'amélioration de la technique, évoquant la nécessité d'étendre le champ des données traitées aux URL.

[1] *Saisie d'une première demande d'autorisation d'un algorithme le 18 juillet 2017, la CNCTR a émis un premier avis défavorable à la mise en œuvre du traitement,* « après avoir relevé que l'architecture générale prévue pour sa mise en œuvre ne respectait pas toutes les garanties préconisées ». *Ce n'est donc que le 25 septembre 2017 que la CNCTR, saisie d'une demande rectificative, a donné un avis favorable au déploiement du premier algorithme.*

[2] *L'architecture des algorithmes et les conditions de leur mise en œuvre ont été définies dans une décision classifiée du Premier ministre du 27 avril 2017.*

Outre le manque de recul et d'expérience sur l'application de la technique, la communauté du renseignement invoque, pour expliquer ces résultats encore décevants, le **champ trop restreint des données susceptibles d'être analysées** par les traitements automatisés mis en œuvre, qui n'inclut pas, à ce jour, l'ensemble des éléments des *URL*.

Dans sa décision portant sur la loi du 24 juillet 2015, le Conseil constitutionnel a validé la conformité à la Constitution de la technique de l'algorithme tout en relevant que les techniques d'accès administratifs aux données de connexion, dont elle fait partie, « *ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des* ***informations consultées****, sous quelque forme que ce soit, dans le cadre des communications* ».

Se fondant sur cette jurisprudence de même que sur les standards techniques internationaux[1], tant la Commission nationale informatique et libertés (CNIL) que la CNCTR ont **exclu** la possibilité que la technique de l'algorithme **puisse permettre un accès complet aux *URL*.** Dans leurs avis respectifs rendus au Premier ministre sur le projet de décret relatif aux techniques de renseignement, les deux autorités précisent en effet que **les *URL* constituent des données mixtes**, comprenant à la fois des données de connexion, c'est-à-dire des éléments relatifs à l'acheminement de la communication internet, et des données de communication, c'est-à-dire des éléments fournissant des précisions sur l'objet ou le contenu du site internet consulté.

Au vu de ces éléments, l'élargissement de la technique de l'algorithme souhaité par les services à l'analyse de la totalité des informations contenues dans les *URL* reviendrait, de fait, à autoriser un traitement automatisé de données révélant, pour partie, le contenu de communications.

Bien qu'elle en comprenne l'intérêt opérationnel, la délégation observe qu'une telle évolution induirait une modification significative **de la technique autorisée par le parlement en 2015, sur lequel il est possible de s'interroger d'un point de vue constitutionnel**. En effet, si le Conseil constitutionnel n'interdit pas, par principe, que des services de renseignement puissent accéder, sous réserve de garanties sérieuses, au contenu des communications, **il n'a reconnu, jusqu'à présent, la conformité à la Constitution que d'une collecte individualisée**, c'est-à-dire visant nominativement une personne susceptible de présenter une menace. Il n'est pas certain, en revanche, que les mêmes conclusions seraient tirées s'agissant d'une technique induisant un traitement en masse de données de communications.

---

[1] *Dans son avis rendu sur le projet de décret, la CNCTR se fonde notamment sur la définition technique d'une URL donnée par le modèle de référence de l'Union internationale des communications.*

Au regard de ces risques, la **délégation demeure donc prudente sur les souhaits d'extension du dispositif, qui pourrait compromettre sa conformité à la Constitution**.

Elle estime qu'une telle extension **ne saurait, en tout état de cause, être admise qu'à titre expérimental**, aux seules fins de prévention des actes de terrorisme, pour une période limitée dans le temps et sous le contrôle étroit de la CNCTR. La délégation juge également indispensable qu'une telle évolution, si elle venait à être mise en œuvre, soit **assortie de garanties renforcées**. Outre l'anonymisation des données, elle propose notamment que la durée de conservation des données collectées, lorsqu'elle concernerait des données de contenu, soit **limitée à 30 jours**.

Enfin, la délégation considère nécessaire **qu'une évaluation régulière de cette technique** puisse être réalisée par le parlement et qu'un rapport lui soit remis annuellement, pendant la durée de l'expérimentation, sur l'évaluation de l'efficacité des algorithmes mis en œuvre.

**Recommandation n° 6 : Proroger, à titre expérimental, la technique dite de l'algorithme prévue par l'article L. 851-3 du code de la sécurité intérieure. N'envisager son extension aux données de navigation sur internet, et en particulier aux *URL*, que sous réserve d'un renforcement conséquent des garanties entourant la mesure et de la mise en place d'un contrôle parlementaire renforcé.**

La délégation a pris acte de la volonté du Gouvernement de reporter d'une année supplémentaire la durée de l'expérimentation, sans modification du cadre légal, et du dépôt prochain d'un projet de loi en ce sens.

Bien qu'il ne soit pas motivé, contrairement à sa recommandation, par l'insuffisance des résultats obtenus, mais par l'incertitude que l'épidémie de Covid-19 fait peser sur le calendrier parlementaire, la délégation estime que ce nouveau délai devrait permettre de disposer d'un recul plus important sur l'efficacité de la technique de l'algorithme et d'alimenter utilement le débat parlementaire.

Les réserves qu'elle formule quant à l'extension du champ des algorithmes demeureront, en tout état de cause, valables à l'issue de ce délai.

### 3. Des services encore freinés dans leur recours aux techniques de renseignement

*a) Une concentration des techniques au sein des services du premier cercle*

Sans surprise, le recours aux techniques de renseignement se révèle très hétérogène selon les services.

Les services du premier cercle ont mis en œuvre, en 2018 comme en 2019, **75 % environ des demandes de techniques de renseignement formulées**, hors demandes d'accès aux données de connexion.

Au sein même des services du premier cercle, **trois services concentrent l'essentiel de ces demandes**, à savoir la DGSI, la DGSE et, dans une moindre mesure, la DNRED.

La **DRSD** ne recourt que de manière plus marginale aux techniques de renseignement les plus intrusives, et connaît même une baisse de ses demandes. En revanche, il peut être noté un usage croissant, depuis 2015, des demandes d'accès aux données de connexion *****, qu'elle explique par un élargissement des accords du GIC avec de nouveaux opérateurs et l'amélioration de ses outils pour effectuer les enquêtes.

La **DRM** exerçant ses activités quasi exclusivement à l'international, elle recourt, dans les faits, principalement à des mesures de surveillance internationale et uniquement de manière très marginale aux techniques domestiques.

Quant à **Tracfin**, son recours aux techniques de renseignement a été très réduit depuis l'entrée en vigueur de la loi, le service travaillant principalement en sources ouvertes et sur la base des déclarations de soupçons qui lui sont transmises. *****

**Demandes de techniques de renseignement soumises à autorisation sur le territoire national par service**

***Tableau*** *****

*b) Des services qui pâtissent encore de l'insuffisance de leurs moyens techniques*

A l'exception de la sous-direction de l'anticipation opérationnelle de la gendarmerie nationale, les demandes de techniques de renseignement des services du second cercle, bien que moins nombreuses en volume, ont connu une forte croissance depuis l'entrée en vigueur de la loi.

*****

De même, les demandes de techniques de la **direction du renseignement de la préfecture de police de Paris**, qui ont peu augmenté entre 2016 et 2018, ont connu une forte hausse de 20 % en 2019, *****.

Enfin, le service national du renseignement pénitentiaire (SNRP), dernier service à avoir intégré la communauté du renseignement et, ce

faisant, à avoir eu accès aux techniques de renseignement, a augmenté sensiblement le nombre de ses demandes, *****[1].

Cette montée en puissance des services du second cercle a été facilitée, pour certains d'entre eux, par la **mise en place de mutualisations qui ont permis de combler partiellement l'insuffisance de moyens matériels et de capacités techniques.**

La DGSI apporte ainsi son assistance technique à plusieurs services du second cercle dans la mise en œuvre de techniques de renseignement. Elle a conclu deux protocoles avec la DRPP et le SNRP pour assurer à leur profit, en tant que simple opérateur, la réalisation d'opérations d'*IMSI-catching* et réalise, pour le compte de plusieurs services, des opérations de recueil de données informatiques.

De manière encore plus intégrée, a été mise en place en avril 2019 une unité spécialisée dans la mise en œuvre des techniques d'interceptions de paroles et d'images en milieu pénitentiaire, commune au SNRP et à la DGSI, le **groupe technique des opérations pénitentiaires (GTOP)**, composé de cinq agents techniques, dont deux de la DGSI et trois du SNRP[2].

Ces coopérations n'ont toutefois pas permis de doter tous les services de capacités techniques suffisantes.

**A cet égard, le SCRT est le service qui a fait état, devant la délégation, des freins techniques les plus importants**. *****

Aussi la délégation estime-t-elle souhaitable que les **coopérations opérationnelles puissent-être approfondies à l'avenir, en particulier au profit de ce service**. Si elles ne sauraient se substituer totalement à l'acquisition d'équipements dont la mobilisation peut nécessiter une réactivité particulière, ces mutualisations permettent d'assurer une montée en puissance technique des services du second cercle et d'éviter des investissements coûteux et peu rentables.

Compte tenu tant de son expérience que de son rôle de chef de file en matière de lutte contre la radicalisation violente et le terrorisme, la **DGSI semble le service le mieux placer pour piloter cette mutualisation**.

Sans aller nécessairement jusqu'à la mise en place, pour l'heure, d'une structure technique commune, la **négociation d'un protocole entre la DGSI et le SCRT,** sur le modèle de ce qui se fait déjà avec d'autres services, mériterait sans aucun doute d'être rapidement engagée, *a minima* pour la mise en œuvre des techniques les plus complexes dont le renseignement territorial n'a actuellement pas la maîtrise, faute de moyens suffisants[3]. Au

---

[1] *Chiffre au 4 décembre 2019.*

[2] *Des développements plus importants concernant cette structure de mutualisation figurent dans la partie du présent rapport relative au renseignement pénitentiaire.*

[3] *La DGSI et le SCRT ont récemment entamé des travaux afin d'identifier les champs de coopération possible en matière de mutualisation d'outils informatiques ou d'appui technique. Une coopération a débuté en septembre 2019 dans le domaine de la recherche sur les sources ouvertes. Pour l'heure,*

regard de l'organisation de ces deux services, ce protocole mériterait de trouver une déclinaison territoriale, au niveau de chaque direction zonale de la sécurité intérieure.

A plus long terme, la délégation estime par ailleurs souhaitable que puisse être engagée une réflexion interservices en vue de la mise en place de protocoles ou de structures de mutualisation des capacités techniques et humaines de déploiement des techniques de renseignement.

**Recommandation n° 7 : Engager des négociations en vue de la conclusion d'un protocole d'assistance entre la DGSI et le SCRT dans la mise en œuvre de certaines techniques de renseignement. Envisager, à terme, la mise en place d'une unité de mutualisation commune à plusieurs services.**

Grâce à la mise en place d'une unité technique commune avec la DGSI, le SNRP fait désormais état de difficultés plus importantes pour ses opérations d'exploitation des données collectées que pour le déploiement des techniques en elles-mêmes. Il relève notamment des besoins en matière de traduction, faute de capacités propres en la matière, *****.

*****

**Recommandation n° 8 :** *****

Tant que la montée en puissance des services du second cercle ne sera pas achevée, **la délégation suggère enfin que le périmètre des techniques qui leur sont autorisées ne soit, en dépit des demandes formulées, pas modifié**.

### *C. EN DÉPIT DE L'ÉQUILIBRE ATTEINT, DES ÉVOLUTIONS A LA MARGE DU CADRE LÉGAL APPARAISSENT SOUHAITABLES*

#### 1. La nécessité de préserver l'équilibre atteint

Près de cinq ans après l'entrée en vigueur de la loi du 24 juillet 2015, il semble que **l'objectif poursuivi par le législateur d'offrir un encadrement légal à l'activité des services sans contraindre excessivement leur action ait été atteint.**

De fait, les définitions données par la loi aux différentes techniques ou catégories de techniques, nécessaires pour donner un cadre suffisamment précis aux actions de recueil de renseignement, conformément d'ailleurs aux exigences posées par la jurisprudence de la CEDH, se sont révélées

*rien n'a en revanche été engagé concernant la coopération technique pour la mise en œuvre des techniques de renseignement.*

**suffisamment larges pour absorber les évolutions technologiques** sans qu'il ait été nécessaire de revenir systématiquement devant le parlement.

A cet égard, l'on ne peut d'ailleurs que se féliciter que la CNCTR, dans le cadre de l'exercice de son contrôle *a posteriori*, ait **fait preuve de souplesse et développé une jurisprudence relativement englobante**. *****.Dans ce contexte, les acteurs de la **communauté du renseignement appellent, à l'unanimité, à faire preuve de prudence dans la révision de la loi** et à ne pas fragiliser l'équilibre atteint entre efficacité des services et protection des droits individuels. Ils revendiquent, en particulier, de ne pas remettre en cause la philosophie adoptée par le législateur en 2015.

**C'est également la position de la délégation, qui a toujours revendiqué l'adoption d'un cadre suffisamment large pour ne pas risquer d'être rendu obsolète par une évolution technologique par essence plus rapide que l'action du législateur.**

### 2. Des ajustements ponctuels de certaines techniques pour répondre à des besoins opérationnels

Ceci étant, tout en s'opposant à une rénovation profonde du cadre légal instauré en 2015, les services de renseignement ont fait état devant la délégation, outre des assouplissements procéduraux précédemment développés (voir partie II, I), de **plusieurs souhaits d'évolution de certaines techniques, destinés à renforcer l'efficacité de leur action**.

Il ne fait aucun doute que tous répondent à un besoin opérationnel avéré. Comme elle a eu l'occasion de le rappeler, la délégation estime néanmoins indispensable d'appréhender ces demandes d'ajustement avec le souci permanent de garantir la protection du respect de la vie privée et du secret des correspondances, au risque, à défaut, de déstabiliser l'équilibre constitutionnel auquel le législateur est parvenu.

La délégation a fait le choix de l'exhaustivité et présente donc toutes les propositions qui lui ont été remontées. Elle n'a toutefois pas choisi de reprendre à son compte l'ensemble d'entre elles, dont certaines lui paraissent porter une atteinte non proportionnée aux droits individuels.

*a) Un élargissement des techniques ouvertes pour la finalité économique*

Plusieurs services ont exprimé le souhait d'élargir le champ des techniques susceptibles d'être mise en œuvre dans le cadre de la finalité de préservation et de promotion des intérêts économiques, industriels et scientifiques majeurs de la Nation.

Ils revendiquent notamment une **extension à cette finalité des autorisations d'exploitation, à des fins de surveillance de personnes situées sur le territoire national, des données collectées dans le cadre de la**

**surveillance internationale**[1]**,** qui ne peuvent actuellement être demandées que pour cinq des sept finalités du renseignement.

La délégation a déjà eu l'occasion, dans son rapport d'activité pour l'année 2017, de souligner toute l'importance de l'action des services de renseignement pour préserver le patrimoine économique de notre pays. Elle ne s'est, de même, jamais opposée à ce que les techniques de recueil de renseignement puissent être mises en œuvre non seulement à des fins défensives, mais également dans le cadre d'une action offensive. En 2014, avant même l'adoption de la loi relative au renseignement, elle affirmait ainsi : « *notre appareil de renseignement ne saurait revêtir une dimension purement défensive (…) ; il doit faire montre de capacités analytiques et prospectives afin de s'insérer pleinement dans le processus décisionnel politique* ».

Au regard du caractère par nature international des menaces pesant sur les intérêts économiques de la France, la délégation est donc **favorable à l'extension souhaitée**, dès lors d'une part, que des techniques très intrusives, en particulier les interceptions de sécurité et le recueil de données informatiques, peuvent déjà être mises en œuvre pour la finalité économique et, d'autre part, que l'exploitation de données collectées dans le cadre d'une surveillance internationale est entourée de garanties identiques à celles prévues pour la mise en œuvre de ces techniques sur le territoire national. La délégation observe notamment que les demandes d'exploitation seraient soumises à un avis préalable de la CNCTR, qui s'assurera du respect du cadre légal.

**Recommandation n° 9 : Etendre à la finalité de préservation et de promotion des intérêts économiques, industriels et scientifiques majeurs de la Nation le champ de l'autorisation d'exploitation de données collectées dans le cadre d'une surveillance internationale, à des fins de surveillance d'une personne située sur le territoire national.**

*b) Une rationalisation nécessaire des durées de conservation des données collectées*

Les durées de conservation des données collectées dans le cadre des techniques de renseignement ont été définies, en 2015, selon deux principaux critères : la nature des données collectées et leur durée d'intrusivité, d'une part ; le niveau de complexité et, par conséquent, la durée moyenne pour procéder à leur exploitation, d'autre part.

**Bien que pertinents, ces critères n'ont pas permis d'aboutir à un dispositif totalement satisfaisant.**

A l'instar de la CNCTR, la délégation reconnaît en effet qu'il existe une incohérence dans le dispositif adopté par le législateur en 2015 s'agissant de la conservation des images et des paroles collectées en application de

[1] *Article L. 854-2 du code de la sécurité intérieure, V.*

l'article L. 853-1 du code de la sécurité intérieure. Sur le plan opérationnel en effet, la fixation de durées de conservation distinctes pour ces deux catégories de données, 120 jours pour les images et 30 jours pour les paroles, bien qu'elle se justifie au regard de leur degré d'intrusivité, complexifie le travail d'exploitation lorsque les services ne disposent, au-delà de 30 jours, plus que des images sans la parole.

Par ailleurs, il semble, en particulier pour les services de taille plus modeste disposant de moins de personnels, que **la durée maximale de conservation des données de communication, actuellement fixée à 30 jours, se révèle parfois trop courte pour permettre leur exploitation dans de bonnes conditions**. Le SNRP a par exemple fait état de sa difficulté à procéder à l'exploitation des sonorisations réalisées par le biais de dispositifs déconnectés placés dans les cellules de détenus, dont la récupération peut se révéler complexe.

Afin de répondre à ces problématiques, **la délégation estime souhaitable de repenser l'échelle de ces durées de conservation**, sans toutefois remettre en cause son caractère gradué, sur lequel le Conseil constitutionnel s'est d'ailleurs appuyé pour reconnaître la conformité à la Constitution du dispositif de conservation[1].

Elle propose ainsi trois niveaux de durée[2] :

- une **durée maximale de 60 jours pour l'ensemble des données portant sur le contenu des communications**, c'est-à-dire les données collectées dans le cadre des interceptions de sécurité, réalisées par le biais d'un opérateur ou par un dispositif technique *IMSI-catcher* ainsi que les données recueillies dans le cadre d'interceptions de communications empruntant la voie hertzienne privative.

Seraient également alignés sur cette durée les enregistrements audio ainsi que les images captées. La délégation est consciente, sur ce point, qu'elle ne satisfait pas complètement les souhaits des services de renseignement, qui appelaient à un alignement à 120 jours de la durée maximale de conservation.

Elle rappelle toutefois qu'en 2015, le choix avait été fait d'assimiler la captation de paroles prononcées à titre privé ou confidentiel, technique jugée très intrusive, à une interception de sécurité et de leur appliquer, dès lors, des garanties identiques, notamment en termes de durée de conservation. L'augmentation de 30 à 120 jours de la durée de conservation des

---

[1] *Dans sa décision n° 2015-713 DC sur la loi relative au renseignement, le Conseil constitutionnel a estimé* « qu'en prévoyant de telles durées de conservation en fonction des caractéristiques des renseignements collectés ainsi qu'une durée maximale de conservation de six ans à compter du recueil des données chiffrées (…), le législateur n'a méconnu aucune exigence constitutionnelle ». *Il a, en conséquence, jugé que les dispositions de l'article L. 822-2 du code de la sécurité intérieure étaient conformes à la Constitution.*

[2] *Hors mesures de surveillance internationale, qui font l'objet de durées de conservation plus longues.*

enregistrements sonores, comme de celles des interceptions de sécurité, serait, de l'avis de la délégation, susceptible d'être jugée disproportionnée par le Conseil constitutionnel. C'est pourquoi il lui apparaît **plus raisonnable d'envisager une durée intermédiaire de 60 jours.**

De fait, cette réorganisation conduirait à abaisser la durée de conservation des images captées. L'exploitation de ces données n'apparaissant toutefois pas plus complexe que les enregistrements sonores, la délégation ne voit pas d'obstacle opérationnel à cette évolution, dès lors qu'elle permet d'assurer une plus grande cohérence du dispositif ;

- **une durée maximale de 120 jours** pour les données collectées dans le cadre d'un recueil ou d'une captation de données informatiques, le maintien d'une telle durée se justifiant par les difficultés d'exploitation spécifiques à ce type de données et à leur volume ;

- **enfin, une durée maximale maintenue 4 ans pour les données de connexion**.

**Evolution proposée de l'échelle des durées de conservation des données collectées dans le cadre des techniques de renseignement soumises à autorisation sur le territoire nationale**

| Technique | Référence législative | Durée de conservation actuelle | Durée de conservation proposée |
|---|---|---|---|
| **Accès aux données de connexion en temps différé** | L. 851-1 | 4 ans | 4 ans |
| **Donnée de connexion en temps réel** | L. 851-2 | 4 ans | 4 ans |
| **Géolocalisation en temps réel** | L. 851-4 | 4 ans | 4 ans |
| **Balisage** | L.851-5 | 4 ans | 4 ans |
| **Recueil de données de connexion par IMSI-catchers** | L. 851-6 | 4 ans | 4 ans |
| **Détection par algorithme** | L. 851-3 | 60 jours | 60 jours |
| **Interceptions de sécurité** | L. 852-1 | 30 jours | 60 jours |

| Technique | Référence législative | Durée de conservation actuelle | Durée de conservation proposée |
|---|---|---|---|
| **Interceptions de correspondance par IMSI-catchers** | L. 852-1 | 30 jours | 60 jours |
| **Interceptions de correspondance empruntant la voie hertzienne privative** | L. 852-2 | 30 jours | 60 jours |
| **Enregistrements de parole** | L. 853-1 | 30 jours | 60 jours |
| **Enregistrements d'images** | L. 853-1 | 120 jours | 60 jours |
| **Recueil de données informatiques** | L. 853-2 | 120 jours | 120 jours |
| **Captation de données informatiques** | L. 853-2 | 120 jours | 120 jours |

**Recommandation n° 10 : Réviser l'échelle des durées de conservation des données collectées dans le cadre des techniques de renseignement afin de tenir compte des contraintes opérationnelles liées à l'exploitation des données, sans toutefois remettre en cause le principe de graduation prévu par le législateur en 2015.**

*c) L'élargissement du champ d'application de certaines techniques à l'entourage*

En l'état du droit, seules deux techniques de renseignement peuvent être mises en œuvre à l'encontre de l'entourage des cibles surveillées, à savoir les interceptions de sécurité et, depuis 2016[1], le recueil en temps réel des données de connexion.

Plusieurs services ont émis le **souhait d'étendre plusieurs autres techniques de renseignement à l'entourage** des personnes susceptibles d'être en lien avec une menace, en particulier la **technique de géolocalisation en temps réel, le balisage, la captation d'images ou de paroles ou encore le recueil de données informatiques**. Selon les indications fournies à la délégation, cette évolution présenterait un avantage sur le plan

[1] *Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.*

opérationnel, en permettant aux services de localiser plus facilement la personne surveillée, d'anticiper ses déplacements ou encore de recueillir des informations à son encontre.

**La délégation ne voit pas d'obstacle de principe à ce qu'il soit procédé à l'extension à l'entourage de la géolocalisation en temps réel**, l'ingérence dans la vie privée permise par cette technique n'étant pas plus importante que dans le cadre d'un accès en temps réel aux données de connexion.

Au regard de l'atteinte portée à la vie privée des personnes concernées, **une telle évolution nécessiterait toutefois, pour être constitutionnelle, d'être encadrée par l'instauration d'un contingentement**. Dans sa décision n° 2017-648 QPC du 4 août 2017, le Conseil constitutionnel, se prononçant sur l'extension à l'entourage de la technique de recueil de données de connexion en temps réel, a en effet estimé que *« faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité, le législateur n'a pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le respect de la vie privée »*.

S'agissant en revanche des autres techniques précédemment mentionnées, la délégation estime que **leur extension à l'entourage pourrait se révéler plus fragile sur le plan constitutionnel.** Dès lors qu'elles impliquent le recueil de données de correspondance, et non plus seulement de connexion et qu'elles peuvent au demeurant justifier, pour leur déploiement, l'introduction dans un lieu privé, ces techniques impliquent en effet un degré d'ingérence plus fort dans la vie privée, qui pourrait être jugé disproportionné pour des individus qui ne présentent pas, comme le Conseil constitutionnel a déjà eu l'occasion de le rappeler, de lien nécessairement étroit avec la menace[1].

**Recommandation n° 11 : Etendre la technique de géolocalisation en temps réel, définie à l'article L. 851-4 du code de la sécurité intérieure, à l'entourage des personnes surveillées, sous réserve de l'application d'un contingent maximal d'autorisations délivrées simultanément.**

*d) Un ajustement de la technique de géolocalisation en temps réel à étudier*

Le GIC a fait part à la délégation d'une suggestion d'**ajustement du cadre légal applicable à la technique de géolocalisation en temps réel**.

En l'état du droit, il est prévu que cette technique soit mise en œuvre sur « *sollicitation du réseau* »[2] de l'opérateur. En pratique, cela consiste, pour l'opérateur, à adresser des messages « invisibles » au terminal mobile placé sous surveillance afin que celui-ci se manifeste et indique l'antenne du

[1] *Décision n° 2017-648 QPC du 4 août 2017 précitée.*
[2] *Art. L. 851-4 du code de la sécurité intérieure.*

réseau mobile à laquelle il est rattaché à un instant « t ». La localisation de l'antenne est transmise au GIC et permet de connaître, de manière approximative, la localisation du terminal surveillé.

*****

**Recommandation n° 12 :** *****

*e) L'extension de la technique accessoire d'introduction dans un lieu privé : une évolution à envisager avec prudence*

En vertu de l'article L. 853-3 du code de la sécurité intérieure, l'introduction dans un lieu privé et, *a fortiori*, dans un lieu d'habitation, ne peut être autorisée que dans le cadre du déploiement de trois techniques de renseignement : le balisage, la captation de paroles ou d'images et le recueil ou la captation de données informatiques.

Certains services estiment que, pour des raisons opérationnelles, la technique de l'accès aux données de connexion par le biais d'un dispositif technique de type *Imsi-catcher* mériterait également de pouvoir être déployée au sein d'un lieu privé. Il a en effet été indiqué à la délégation qu'en raison de la portée limitée des dispositifs techniques, les services de renseignement étaient susceptibles de rencontrer des difficultés pour intercepter les données, par exemple lorsque la cible est située en étage élevé.

La délégation a pu constater, lors de ses travaux, que **l'intérêt opérationnel de l'extension proposée par certains services n'était pas partagé par l'ensemble des services de renseignement.**

Or, il doit être rappelé qu'en 2015, le législateur a prévu un principe de subsidiarité et expressément limité l'application de l'introduction dans un lieu privé aux seuls cas où aucun autre moyen légalement autorisé ne permet d'aboutir au même résultat.

Aussi la délégation, soucieuse d'assurer la proportionnalité des moyens accordés aux services de renseignement, n'a-t-elle pas souhaité, en l'absence d'éléments complémentaires justifiant d'un besoin opérationnel impérieux, reprendre à son compte ce souhait d'évolution.

### 3. Des oublis à corriger

*a) L'introduction d'un régime de tests*

Le GIC comme les services de renseignement procèdent, sur une base régulière, à la conduite de tests sur les équipements techniques utilisés pour collecter du renseignement. Outre le fait qu'elle est utilisée dans le cadre des processus de formation des agents, la conduite de tests est également essentielle pour vérifier le bon fonctionnement des capacités techniques déployées ainsi que pour expérimenter de nouvelles méthodes de recueil en vue d'assurer leur adaptation permanente aux évolutions

technologiques. Les équipements de collecte de renseignement peuvent, en outre, être utilisés par les services à des fins de formation et d'entraînement des agents.

Comme l'a indiqué le GIC à la délégation, la réalisation de ces tests peut induire la collecte de données privées ou l'interception de correspondance, voire, dans certains cas, donner lieu à des réquisitions auprès des opérateurs de communications électroniques. Dans le cas de l'utilisation d'un *IMSI-catcher*, elle peut également conduire à perturber ponctuellement le fonctionnement d'un réseau mobile.

Or, **en 2015, aucun régime juridique n'a été prévu pour encadrer la réalisation des tests et entraînements**, apporter des garanties suffisantes aux atteintes à la vie privée et au secret des correspondances susceptibles d'être réalisées dans ces circonstances et, le cas échéant, sécuriser l'action des services.

Le **législateur est partiellement revenu sur cet oubli en 2017**, en introduisant dans le code de la défense une disposition nouvelle autorisant la direction générale de l'armement et certaines unités des armées à réaliser des campagnes de test sur des matériels de renseignement[1]. Initialement limité aux équipements utilisés pour l'interception des communications empruntant la voie hertzienne, ce régime a été étendu à un spectre plus large de matériels par la dernière loi de programmation militaire[2].

Il apparaît **souhaitable de dupliquer ce régime de tests, au sein du code de la sécurité intérieure, pour les autres services de renseignement ainsi que pour le GIC.** En effet, l'usage de matériels de renseignement en dehors des cas prévus par le code de la sécurité intérieure demeure particulièrement fragile sur le plan juridique et susceptible de recours en cas d'atteinte portée à la vie privée et au secret des correspondances. Il apparaît, au demeurant, souhaitable de donner un statut aux données collectées dans le cadre de campagnes de tests afin notamment de s'assurer de leur destruction.

Des garanties identiques à celles prévues pour les armées devraient donc être introduites, à savoir :

- la déclaration préalable obligatoire à la CNCTR de tout essai conduit sur un matériel de renseignement ;

- la limitation des personnes autorisées à réaliser des tests aux seuls individus désignés et habilités à cet effet ;

---

[1] *Art. L. 2371-2 du code de la défense, créé par la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.*

[2] *Peuvent désormais être testés sur ce fondement les matériels IMSI-catcher, les équipements utilisés pour procéder à des interceptions de sécurité, pour intercepter des communications empruntant la voie hertzienne ainsi que pour des surveillances internationales.*

• la destruction immédiate des données collectées une fois les tests achevés.

Au regard des difficultés techniques encore rencontrées par plusieurs services du second cercle, la délégation considère que le régime de tests pourrait, du moins dans un premier temps, n'être ouvert qu'aux services spécialisés de renseignement et au GIC, qui se trouve en première ligne pour l'expérimentation de nombreux matériels.

L'ensemble des matériels utilisés pour la mise en œuvre pourraient être concernés, qu'il s'agisse des techniques reposant sur un recueil de données auprès des opérateurs comme des techniques consistant en une collecte directe de données par les services.

**Recommandation n° 13 : Encadrer législativement la conduite de tests par le GIC et les services de renseignement du premier cercle sur les matériels de collecte de renseignement, à l'instar du régime prévu par l'article L. 2371-2 du code de la défense.**

*b) La création d'une technique autorisant l'ouverture des lettres et des paquets*

Se focalisant sur l'encadrement des techniques de renseignement faisant appel aux outils technologiques les plus avancées, le législateur a, en 2015, **omis de créer un régime spécifique encadrant la méthode plus traditionnelle d'ouverture des lettres et des paquets physiques**. L'atteinte portée à la vie privée et au secret des correspondances de cette méthode est pourtant assimilable à celle d'autres techniques de renseignement, dès lors qu'elle permet à un service de renseignement d'accéder au contenu d'une correspondance.

La délégation suggère donc que la technique de l'interception de sécurité puisse être étendue et adaptée pour couvrir également les interceptions de communications physiques, avec des garanties identiques, notamment en termes de durée d'autorisation (4 mois) et de durée de conservation des données collectées (30 jours).

L'accès auxdites lettres et courriers peut nécessiter, de la part des services, l'introduction dans un lieu privé, qui devrait, dès lors, être autorisée pour cette nouvelle technique.

**Recommandation n° 14 : Créer une nouvelle interception de sécurité pour couvrir la surveillance des correspondances physiques (lettres, paquets, *etc.*), susceptible, selon les besoins opérationnels, d'être associée à une introduction dans un lieu privé.**

*c) La nécessité de prévoir un encadrement réglementaire précis des conditions d'échanges de renseignements entre services*

L'article L. 863-2 du code de la sécurité intérieure prévoit que les services spécialisés du renseignement et les services relevant du second cercle « *peuvent partager toutes les informations utiles à l'accomplissement de leurs missions* ».

Les modalités et les conditions dans lesquelles ces échanges peuvent s'effectuer sont renvoyées, par la loi, à un décret en Conseil d'État. Il a été indiqué à la délégation que ce décret n'avait pas été pris à ce jour, faute, pour le législateur, d'avoir prévu qu'il ne serait pas publié.

Ceci étant, il ressort des travaux conduits par la délégation que l'absence de cadre réglementaire **n'a pas empêché les services de procéder à des partages réguliers** non seulement de renseignements exploités, c'est-à-dire d'extractions et de transcriptions, mais également de renseignements collectés, c'est-à-dire de données brutes recueillies dans le cadre d'une technique de renseignement.

La délégation a ainsi été informée de l'existence d'une **procédure dite d'extension**, qui permet la communication de transcriptions effectuées au sein du GIC[1] à un service autre que celui qui a fait la demande initiale de technique de renseignement. En pratique, la communication est effectuée par le GIC, à la demande du service qui a demandé la technique et réalisé la transcription initiale, et donne lieu à une information de la CNCTR. Le service bénéficiaire ne peut se voir transmettre que les renseignements en lien avec une des finalités qui lui sont autorisées par la loi.

**La délégation regrette de n'avoir pu obtenir, en revanche, d'informations plus précises sur les conditions juridiques et opérationnelles dans lesquelles il est procédé à des partages de données brutes**. Bien qu'il lui ait été assuré que ceux-ci étaient réalisés dans le respect des principes posés par la loi de 2015, elle n'a pas été en mesure de constater, par elle-même, les conditions dans lesquelles les règles relatives à la conservation des données brutes collectées et à l'utilisation de ces mêmes données étaient assurées.

**Elle estime en tout état de cause urgent qu'un encadrement précis de ces échanges soit réalisé**, afin de définir les conditions dans lesquelles les renseignements collectés par le biais d'une technique de renseignement peuvent être partagés et exploités par d'autres services. Il s'agit d'une exigence non seulement en termes de protection du droit au respect de la vie privée, mais également pour sécuriser l'action des services.

---

[1] *Cette procédure ne concerne que les transcriptions réalisées au sein du GIC, c'est-à-dire celles qui portent sur des interceptions de sécurité, des exploitations de données collectées dans le cadre de la surveillance internationale et concernant des communications mixtes ou rattachables au territoire national et les captations de paroles, lorsqu'elles sont centralisée par le GIC.*

A cet égard, le renvoi simple à un décret pourrait se révéler insuffisant et placer le législateur en situation d'incompétence négative. La délégation juge en conséquence souhaitable que soient précisées dans la loi certaines garanties minimales, parmi lesquelles les catégories de données susceptibles d'être échangées, les conditions d'utilisation de ces données par les services, en particulier s'agissant des finalités d'utilisation, ainsi que les règles de conservation et de destruction de ces mêmes données.

Les conditions d'application de ces dispositions pourraient être, quant à elles, renvoyées à un décret non publié, qui pourrait être **pris après avis de la CNCTR.**

**Recommandation n° 15 : Donner un cadre légal aux conditions dans lesquelles les renseignements collectés par le biais de techniques de renseignement peuvent être partagés entre services de renseignement. Modifier, en conséquence, l'article L. 863-2 du code de la sécurité intérieure.**

*d) Une demande de conservation des données collectées à des fins de recherche et développement qui nécessite d'être approfondie*

Face au volume important de données collectées dans le cadre des techniques de renseignement se pose, pour les services de renseignement, un défi croissant d'exploitation, qui nécessite le développement de dispositifs techniques de recueil, d'extraction et de transcription de ces données.

Pour ce faire, plusieurs services **revendiquent que puisse être autorisée la conservation, à des fins de recherche et développement, des données collectées dans le cadre d'une technique de renseignement**, au-delà des durées actuellement prévues par la loi.

Il s'agit de pouvoir disposer d'un volume important de données sur lesquels conduire des études, tests et expérimentations, qui, pour donner des résultats satisfaisants, doivent avoir été recueillies dans des conditions identiques à celles de l'exploitation. A titre d'exemple, il a été indiqué à la délégation que pour développer un outil de discrimination capable d'isoler les images d'une plaque d'immatriculation dans un enregistrement vidéo de plusieurs heures, il était nécessaire d'alimenter l'outil à partir d'images recueillies avec le même outil que celui qui aura été utilisé pour collecter les données destinées à être *in fine* analysées.

**La délégation entend l'intérêt opérationnel de cette demande, à laquelle elle n'est pas, par principe, opposée.** Elle estime cependant qu'une telle évolution législative **nécessite d'être strictement encadrée et ne saurait, en tout état de cause, concerner de manière systématique l'ensemble des données collectées.**

Il lui est, en l'état de l'information dont elle dispose sur les besoins techniques des services, complexe de définir avec précision les garanties minimales qu'il serait nécessaire d'apporter à un tel dispositif.

Il lui apparaît a minima nécessaire qu'une attention particulière soit apportée aux possibilités d'anonymisation des données conservées et qu'une procédure de contrôle renforcé soit instaurée, afin de garantir que les données ainsi conservées ne puissent être utilisées à d'autres fins.

Il mériterait également d'être réfléchi aux conditions dans lesquelles la conservation de données à des fins de recherche et développement pourrait être soumise à une procédure d'autorisation préalable, afin de s'assurer que la conservation des données soit dûment justifiée et soit réalisée de manière ciblée.

### 4. L'enjeu du passage à la « 5G » : des besoins d'ajustement encore difficiles à appréhender

L'arrivée de la cinquième génération des communications électroniques mobiles, dite « 5G », en raison de l'évolution des réseaux de communication classique qu'elle induit, devrait avoir un impact important sur les conditions de mise en œuvre de certaines techniques de renseignement.

Il est en particulier probable qu'elle complexifie, voire rende obsolète, la technique de recueil de proximité de données de connexion par les dispositifs de type *Imsi-catcher*. En effet, dans un réseau classique, les antennes-relais ne servent qu'à retransmettre les flux de données entre les terminaux mobiles des utilisateurs et les cœurs de réseaux des opérateurs. Dans ce modèle, les *Imsi-catcher* sont donc utilisés comme des antennes factices, qui se substituent, dans un périmètre donné, aux antennes-relais aux fins de collecte de deux catégories de données de connexion :

- d'une part, les données relatives à l'identification d'un équipement terminal ou d'un numéro d'abonnement, c'est-à-dire le numéro identificateur d'usager mobile (IMSI, soit *International Mobile Subscriber Identity*), numéro unique figurant dans la carte SIM, et le numéro international de l'équipement mobile (IMEI, soit *International Mobile Equipment Identity*), numéro unique du terminal ;

- d'autre part, les données relatives à la localisation technique des terminaux utilisés.

Avec la « 5G », les identifiants électroniques des terminaux qui seront échangés avec les antennes-relais ne seront plus uniques, comme actuellement, mais éphémères. Dans ce système, les terminaux mobiles disposeront toujours de numéros IMSI et IMEI, mais seul l'opérateur disposera des informations permettant de faire le lien entre ces identifiants uniques et les identifiants éphémères échangés sur le réseau.

Au regard de l'enjeu de cette évolution technologique, la délégation a été informée de la **création d'un groupe de travail interservices, chargé**

**d'étudier les conséquences du passage à la « 5G » pour le renseignement et les ajustements nécessaires.**

La définition des normes techniques du réseau « 5G » n'étant pas complètement aboutie, les conséquences exactes de cette évolution technologique majeure et, partant, les éventuelles évolutions législatives qui pourraient se révéler nécessaires, demeurent encore difficiles à appréhender.

Pour l'heure, il apparaît que si une évolution des modes opératoires des services et du GIC pourrait se révéler nécessaire, la nature des techniques encadrées par la loi pourrait ne pas être modifiée.

### 5. L'accès aux données de connexion : des techniques qui pourraient être fragilisées par la jurisprudence européenne

Au-delà de la nécessaire adaptation du droit aux évolutions technologiques, le cadre juridique actuel pourrait se voir fortement fragilisé par l'évolution de la jurisprudence de la Cour de justice de l'Union européenne (CJUE).

Par un arrêt *Tele2 Sverige* du 21 décembre 2016, la Cour de justice de l'Union européenne (CJUE), se prononçant sur le cas de la Suède, a en effet **jugé contraire au droit de l'Union[1] le principe d'une conservation généralisée et indifférenciée, à des fins préventives, des données de connexion** par les opérateurs de communications électroniques et les fournisseurs de services publics en ligne.

Dans les faits, cette décision **remet en cause l'existence même des techniques d'accès aux données de connexion en temps différé**, non seulement en matière pénale, mais également dans le champ du renseignement, dont la mise en œuvre repose sur l'obligation légale imposée aux opérateurs de communications électroniques ainsi qu'aux fournisseurs d'accès à internet de conserver, pendant une durée d'une année, l'ensemble des données de connexion transitant par leurs réseaux[2].

Cette jurisprudence, dont les conséquences seraient assurément désastreuses tant pour l'efficacité des enquêtes pénales que de l'activité des services de renseignement, pourrait pourtant se voir prochainement confirmée dans le cadre de son application au droit français.

Saisi de plusieurs contentieux portant sur des actes réglementaires applicables aux activités de renseignement, le Conseil d'État a en effet renvoyé à la CJUE, le 26 juillet 2018, trois questions préjudicielles relatives à la conformité au droit de l'Union des dispositions du code de la sécurité intérieure relatives à la conservation des données de connexion.

---

[1] *Directive européenne 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.*

[2] *Le III de l'article 34-1 du code des postes et des communications électroniques prévoit en effet que*

Au regard du contexte « *marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste* », la juridiction française relève qu' « *une telle conservation présente une utilité sans équivalent par rapport au recueil de ces mêmes données à partir du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'État* » et interroge les juges européens sur la possibilité qu'une telle obligation imposée aux opérateurs soit regardée, « *notamment eu égard aux garanties et contrôles dont sont assortis (...) le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres* ».

L'affaire n'a, pour l'heure, **pas été définitivement jugée par la CJUE, qui ne devrait rendre son arrêt qu'à l'été 2020**. Au regard toutefois des conclusions rendues par l'avocat général au début du mois de janvier 2020[1], il existe un **risque sérieux que l'arrêt *Tele2 Sverige* soit confirmé**. En matière de renseignement, une telle décision aurait pour conséquence de priver de fondement les techniques d'accès aux données de connexion en temps différé de l'article L. 851-1 du code de la sécurité intérieure.

**Les conclusions de l'avocat général**
**sur les renvois préjudiciels du Conseil d'État (15 janvier 2020)**

Les renvois formés par le Conseil d'État devant la CJUE soulevait, en droit, **deux questions distinctes**.

La première concerne le **champ d'application de la directive relative à la vie et privée et aux communications électroniques en cause et, en particulier, son applicabilité aux activités relevant de la sécurité nationale**. La France, comme plusieurs autres états membres de l'Union ayant déposé des mémoires en défense, estimait que l'article 15 de la directive excluait du champ d'application de la directive les activités menées par les pouvoirs publics en vue de préserver la sécurité nationale et estimait, dès lors, que la CJUE n'était pas légitime à se prononcer sur la conformité au droit de l'Union des dispositions du code de la sécurité intérieure.

Dans ses conclusions, l'avocat général auprès de la CJUE rejette ces arguments, estimant quant à lui que si la directive exclut bien de son champ d'application les activités menées, en vue de préserver la sécurité nationale, par les pouvoirs publics pour leur propre compte, tel n'est en revanche pas le cas lorsque le concours d'autres acteurs et, en l'espèce, des opérateurs de communications électroniques, est requis.

La seconde question soulevée par les renvois porte sur **la portée de l'autorisation faite par la directive aux États membres d'apporter, à des fins de**

[1] Conclusions de l'avocat général Campos Sanchez-Bordona dans l'affaire C-623/17 Privacy International, dans les affaires jointes C-511/18 La Quadratude du Net e.a. et C-512/18 French Data Network e.a. ainsi que dans l'affaire C-52D/18 Ordre des barreaux francophones et germanophone e.a.

**sécurité nationale, des limitations à l'obligation faite aux opérateurs de garantir la confidentialité des communications**.

Sur ce point également, l'avocat général propose de confirmer la jurisprudence *Tele2* quant au caractère disproportionné d'une législation ou réglementation imposant aux opérateurs une conservation généralisée et indifférenciée de l'ensemble des données de connexion.

Reconnaissant toutefois l'utilité d'une obligation de conservation des données pour préserver la sécurité nationale et lutter contre la criminalité, il estime en revanche possible d'envisager une conservation limitée et différenciée, soit la conservation, pour une période déterminée, de certaines catégories de données qui seraient considérées comme absolument indispensables pour la prévention de la criminalité et la préservation de la sécurité nationale.

Au vu de ces éléments, l'avocat général conclut à la non-conformité au droit de l'Union européenne des dispositions relatives à l'obligation de conservation généralisée imposée, par la législation et la réglementation françaises, aux opérateurs de communications électroniques, sur laquelle repose l'accès aux données de connexion en temps différé.

En revanche, il estime que la directive ne s'oppose pas à la possibilité d'un recueil en temps réel, par les autorités publiques, des données relatives au trafic et aux données de localisation de certaines personnes ce qui, dès lors, semble préserver les techniques de géolocalisation et d'accès aux données de connexion en temps réel.

Plusieurs services et autorités ministériels ont fait état, devant la délégation, de leurs fortes préoccupations quant aux suites à donner à la décision de la CJUE, si les conclusions de l'avocat général venaient à être suivies.

Pour la France, les possibilités de réaction seraient en effet étroites.

A ce stade, les pouvoirs publics paraissent exclure de suivre la voie choisie par la Suède, qui a consisté à renoncer à toute capacité d'investigation rétroactive, au regard des conséquences qu'elle pourrait avoir sur l'efficacité de l'action des services de renseignement comme de l'action judiciaire.

La révision de la directive susmentionnée ayant été mise sur la table au niveau européen, il est envisagé, à ce stade, de pousser les négociations pour modifier les textes européens dans un sens qui permettrait de neutraliser les conséquences de la jurisprudence de la CJUE.

Compte tenu des délais d'adoption des textes législatifs au niveau européen, la **délégation estime possible et souhaitable, dans l'attente, qu'une conservation généralisée des données soit maintenue en matière de renseignement**. L'avocat général n'a en effet pas exclu la possibilité que soient conservées temporairement les législations nationales incompatibles avec le droit de l'Union, dès lors que ce maintien serait justifié par des considérations impérieuses de sécurité publique.

En tout état de cause, la délégation demeure fermement attentive à l'évolution de cette jurisprudence et aux évolutions législatives qu'elle pourrait rendre nécessaire.

### 6. L'encadrement des échanges de renseignement avec des États étrangers : une réflexion à engager

*a) Une absence d'encadrement des échanges de renseignement étranger qui interroge et pourrait constituer une source de fragilité juridique*

Les échanges de renseignements avec des services étrangers n'ont pas été inclus dans le cadre fixé par le législateur en 2015. La loi du 24 juillet 2015 a d'ailleurs expressément exclu la possibilité pour la CNCTR de connaître des données communiquées par des services étrangers.

Dans le cadre de son rapport d'activité pour l'année 2018, la CNCTR a toutefois rouvert le débat et invité les autorités publiques comme le législateur à engager une réflexion sur un possible encadrement légal de ces échanges, dès lors qu'ils « *incluent des données sur des citoyens français ou sur toute personne résidant en France* ».

La délégation a estimé souhaitable de se saisir de ce sujet qui, en creux, **soulève la question de l'effectivité du cadre légal instauré par le législateur en 2015**.

Il n'est, bien entendu, pas question pour elle de mettre en doute l'intégrité des services de renseignement. Ceci étant, elle observe, à l'instar de la CNCTR, que **l'exclusion des échanges avec des services étrangers de tout encadrement légal soulève deux interrogations** en termes de respect des droits et libertés constitutionnellement garantis :

- d'une part, **celle de l'effectivité de la protection des droits des citoyens français et des individus résidants sur le territoire français** dans l'hypothèse où des renseignements issus d'une technique de renseignement seraient communiqués par un service français à un de ses partenaires étrangers **(« flux sortants »**). Rien, en l'état du droit, ne garantit en effet que les règles posées par le législateur quant aux règles de conservation des données collectées dans le cadre d'une technique ainsi que des transcriptions et extractions réalisées sont respectées lorsque les données sont communiquées à un service étranger ;

- d'autre part, **celle du cadre applicable aux données concernant des citoyens français ou des individus résidant sur le territoire national communiquées**, par un service étranger, à un service français (« **flux entrants** »). A titre d'exemple, aucune règle n'encadre actuellement l'utilisation et la conservation de données de communication collectées par un service étranger sur le territoire français et transmises à un service de renseignement français.

Cette absence complète d'encadrement légal des échanges de renseignements pourrait par ailleurs soulever des **difficultés de conformité avec la convention européenne de sauvegarde des droits de l'homme**. Dans un arrêt *Big Brother Watch c/ Royaume Uni* du 13 septembre 2018, la CEDH s'est en effet prononcée, pour la première fois, sur le principe de ces échanges.

Bien qu'il ne soit pas encore définitif, ayant été renvoyé en grande chambre, cet arrêt, qui ne portait que sur le traitement des renseignements entrants, pose un certain nombre de règles. Observant que « *si les États contractants jouissaient d'une latitude illimitée pour demander à des États non contractants d'intercepter des communications ou de leur remettre des communications interceptées, ils pourraient aisément contourner les obligations que leur impose la Convention* », la Cour indique que « *le droit interne doit donc, afin d'éviter les abus de pouvoir, énoncer aussi les circonstances dans lesquelles il est possible de demander à des services de renseignement étrangers des éléments interceptés* ».

La CEDH n'exige pas, dans cette hypothèse, que des conditions identiques au droit interne soient prévues, mais impose que le droit interne prévoit des garanties à quatre niveaux : « *les circonstances dans lesquelles il est possible de demander des éléments interceptés ; la procédure à suivre pour l'examen, l'utilisation et la conservation des éléments obtenus ; les précautions à prendre pour la communication de ces éléments à d'autres parties ; et les circonstances dans lesquelles ces éléments doivent être effacés* ».

*b) Un engagement du Gouvernement à mieux formaliser les protocoles d'échanges qui va dans le bon sens*

**Les services de renseignement s'opposent, majoritairement, à toute forme d'encadrement légal de leurs échanges avec des partenaires étrangers.** De leur point de vue, cette coopération relève de la souveraineté de l'État et de son action diplomatique et doit, à ce titre, être couverte par un secret absolu. Ils revendiquent, au demeurant, un risque d'atteinte à la règle du tiers service, en vertu de laquelle un service de renseignement est tenu à la confidentialité absolue sur tout renseignement qui lui serait transmis par un partenaire étranger.

**Pour répondre aux préoccupations formulées tant par la CNCTR que par la CEDH, le Gouvernement envisage néanmoins de donner un cadre réglementaire plus formalisé à ces échanges, pour améliorer les conditions dans lesquelles les liaisons avec des partenaires étrangers sont établies**.

Pour l'heure, l'échange de renseignements avec les partenaires étrangers relève en effet, dans la majorité des cas, d'accords bilatéraux négociés directement par les chefs de services, dans certains cas formalisés par la signature de protocoles. Selon les informations communiquées à la délégation, des réflexions sont en cours pour évaluer l'opportunité de

prévoir que **toute ouverture d'une liaison avec un service étranger soit validée au niveau politique, par le ministre de tutelle du service concerné.**

Il est également envisagé la **rédaction d'une charte**, actuellement en cours de préparation par la CNRLT, fixant, à l'égard services de renseignement, un ensemble de principes à respecter dans la « protocolisation de la liaison ». Il a été indiqué à la délégation que pourraient par exemple être prévu qu'une coopération ne puisse être engagée que lorsque les moyens de collecte du renseignement par le partenaire concerné sont conformes à des principes démocratiques.

**La délégation ne peut que soutenir le Gouvernement dans cette démarche.** Il lui apparaît que ces réformes, bien que ne se traduisant par aucune évolution législative, **seraient de nature à apporter une première forme d'encadrement aux échanges de renseignement.**

*c) Un débat légitime sur le statut des renseignements techniques collectés ou exploités grâce à l'assistance d'un service étranger*

En ce qui concerne la question de l'encadrement légal soulevée par la CNCTR, la délégation estime pour l'heure qu'il serait peu opportun, au regard des enjeux diplomatiques en cause et des impératifs opérationnels, de fixer dans la loi des règles plus précises encadrant l'ensemble des échanges de renseignement (qui consisteraient par exemple à imposer que ne puissent être transmis des informations qu'à des partenaires disposant de standards de collecte ou d'exploitation du renseignement similaires à ceux de la loi du 24 juillet 2015).

Une telle évolution risquerait en effet de se traduire par une limitation conséquente des possibilités d'échanges avec certains États, pourtant essentiels dans certains dossiers stratégiques, qu'il s'agisse par exemple de prévention du terrorisme ou d'intérêts militaires.

Ceci étant, elle relève qu'une réflexion mériterait d'être engagée sur le statut des renseignements techniques obtenus grâce à l'assistance d'un partenaire étranger et qui concernent des citoyens français ou des individus résidant sur le territoire national.

Il ne s'agit en aucun cas, pour la délégation, de soulever un risque de contournement volontaire du cadre légal par les services, par exemple pour la mise en œuvre d'une technique malgré un refus du Premier ministre.

Néanmoins, il lui a été indiqué que, faute de capacités techniques suffisantes, les services de renseignement français pouvaient parfois être amenés à recueillir l'assistance de leurs partenaires étrangers pour la collecte ou l'exploitation de renseignement technique. Cela peut par exemple être le cas *****

Il est donc légitime, de l'avis de la délégation, de s'interroger sur le niveau de protection qui entoure ces pratiques, notamment s'agissant des règles d'autorisation et des conditions de centralisation, de traçabilité et de

conservation des données recueillies ou exploitées grâce à l'assistance d'un service étranger. Cette question devra être débattue dans le cadre de l'examen du prochain projet de loi de réforme de la loi renseignement annoncé par le Gouvernement.

**Recommandation n° 16 : Engager une réflexion sur le statut des renseignements techniques recueillis ou exploités grâce à l'assistance d'un service de renseignement étranger et sur le niveau de protection qui les entoure.**

## III. UN CONTRÔLE SUR L'ACTIVITÉ DES SERVICES FORTEMENT RENFORCÉ, AU BÉNÉFICE DE LA PROTECTION DES DROITS DES CITOYENS

### *A. LA CNCTR A SU MONTER EN PUISSANCE POUR ASSUMER PLEINEMENT SA FONCTION DE CONTRÔLE, QUI DEMEURE TOUTEFOIS IMPARFAITE*

Pilier de la réforme de 2015, le renforcement du contrôle de l'usage des techniques de renseignement, tant *a priori* qu'*a posteriori,* a trouvé une traduction pratique assez rapide, grâce à la montée en puissance de la CNCTR.

Cinq ans après son installation, force est toutefois de constater que le champ du contrôle exercé par cette autorité indépendante demeure limité et ne permet de s'assurer qu'imparfaitement de l'effectivité du cadre prévu par le législateur.

#### 1. La mise en place de la CNCTR : une montée en charge progressive

La CNCTR a été mise en place à compter du 1er octobre 2015, date de nomination de ses membres[1], et s'est substituée à la CNCIS, qui assurait, depuis 1991, le contrôle de la mise en œuvre des interceptions de sécurité, et, par la suite, des autres techniques de renseignement autorisées par le législateur.

Au cours des premiers mois qui ont suivi sa création, la CNCTR a dû s'appuyer sur les seuls moyens dont disposaient la CNCIS, qui étaient, par nature, insuffisants au regard de l'élargissement important du champ des missions de l'autorité nouvellement créée.

---

[1] *Décret du Président de la République du 1er octobre 2015 relatif à la composition de la Commission nationale de contrôle des techniques de renseignement.*

Dans cette phase de transition, elle a donc concentré son activité sur la mise en œuvre du dispositif de contrôle *a priori* (*cf. infra*), qui était prioritaire au regard de la nécessité, pour elle, d'être rapidement en mesure de faire face aux demandes adressées par les services, dans les délais fixés par le législateur.

La CNCTR a, par la suite, bénéficié rapidement de renforts en effectifs, qui lui ont permis de monter en puissance sur sa mission de contrôle *a posteriori*, au fur et à mesure des recrutements.

Outre les trois membres du collège exerçant leurs fonctions à temps plein, elle s'appuie sur une **équipe composée de 17 personnes, chargés de mission, juristes et informaticiens**. 11 d'entre elles sont plus particulièrement chargés d'instruire les demandes adressées par les services dans le cadre du contrôle a priori et d'assurer l'organisation et la conduite des contrôles *a posteriori*.

**En l'état de ses missions, la CNCTR estime ces moyens suffisants.**

### 2. Un contrôle *a priori* fonctionnel

#### *a) Le contrôle a priori, un contrôle de légalité des techniques de renseignement sollicitées*

Dans l'exercice de son contrôle *a priori*, la CNCTR examine les demandes de techniques de renseignement qui lui sont transmises sous trois angles.

Elle s'assure, en premier lieu, de la **légalité formelle** de la demande. A ce titre, il est notamment vérifié que le service demandeur est bien compétent pour recourir à la technique sollicitée et que la demande comporte bien l'ensemble des éléments formels exigés par la loi : motifs de la demande, personnes, lieux ou véhicules visés, *etc*.

En second lieu, la CNCTR examine le **bien-fondé de la demande**. Il s'agit notamment, pour elle, de vérifier que sont apportés suffisamment d'éléments permettant d'établir une menace potentielle pour les intérêts fondamentaux de la Nation, justifiant qu'il soit recouru à une technique de renseignement.

Enfin, en troisième et dernier lieu, le contrôle *a priori* comporte un **contrôle de proportionnalité**. Autrement dit, la CNCTR s'assure que l'atteinte à la vie privée et, le cas échéant, au secret des correspondances, engendrée par la technique demandée est proportionnée à la menace décrite, aux enjeux concernés et aux informations recherchées. Pour les techniques les plus intrusives, elle vérifie également le respect du principe de subsidiarité posé par le législateur, c'est-à-dire qu'elle contrôle qu'aucun autre moyen moins intrusif ne permettrait de recueillir les informations recherchées.

*b) Une action de contrôle pleinement respectée, qui se nourrit des échanges avec les services*

Cinq ans après l'entrée en vigueur de la loi, le rôle de « filtre » confié à la CNCTR apparaît pleinement assumé et respecté, tant par les autorités publiques que par les services utilisateurs de techniques de renseignement.

Depuis 2015, le **Premier ministre n'est ainsi jamais passé outre les avis défavorables rendus par la commission**. Dans certains cas, il s'est même opposé à la mise en œuvre d'une technique de renseignement, en dépit d'un avis favorable de la commission.

La CNCTR a su, par ailleurs, inscrire l'exercice de son contrôle dans un **rapport de confiance et un dialogue nourri avec les services** de renseignement demandeurs. Il est ainsi régulier, pour la CNCTR, de solliciter des informations complémentaires à l'appui d'une demande, lorsqu'elle estime ne pas disposer des éléments suffisants.

Ces échanges se révèlent fructueux à deux niveaux. Comme indiqué précédemment, ils ont tout d'abord permis aux services de renseignement de s'adapter progressivement aux exigences de la commission et de perfectionner la formulation et la motivation de leurs demandes. Il a déjà été rappelé, à cet égard, la diminution importante du taux d'avis défavorables rendus par la CNCTR.

A l'inverse, il apparaît que ce dialogue nourri a **également permis à la CNCTR de mieux comprendre les besoins des services, voire, dans certains cas, d'adapter sa doctrine à leurs exigences opérationnelles**.

Tel a par exemple été le cas de l'appréciation de la finalité portant sur la préservation et la promotion des intérêts économiques, industriels et scientifiques majeures de la Nation. En 2017, la délégation s'était étonnée de l'approche adoptée par la commission pour apprécier le bien-fondé des demandes qui lui étaient adressées sur cette finalité. Elle avait en particulier regretté que « *la CNCTR fonde son appréciation non pas sur ce que l'État aurait défini, notamment dans le cadre de la liste des entités économiques à protéger en priorité, comme présentant un intérêt majeur, mais sur une appréciation " propre " de ce qu'elle estime comme tel* »[1].

Il semble que la CNCTR, tenant compte des orientations politiques souhaitées par le Gouvernement en matière de protection des intérêts économiques de la France, ait fait évoluer sa doctrine, ce dont la délégation se félicite. En témoigne la réduction du taux de refus pour cette finalité passé, selon les données communiquées par la CNRLT, de plus de 13 % en

[1] *Rapport n° 424 (Sénat, 2017-2018) et n° 875 (Assemblée nationale, XV^e législature) fait par M. Philippe Bas au nom de la délégation parlementaire au renseignement, déposé le 12 avril 2018.*

2017 à environ 8 % en 2018[1], alors même que le nombre de techniques sollicitées pour la finalité économique a augmenté sur la même période *****.

La CNCTR a également indiqué à la délégation avoir développé une interprétation souple pour la technique de balisage. Elle admet ainsi, pour certaines finalités, la pose d'une balise visant à la fois une personne dont l'identité n'est pas connue et un véhicule non identifié.

Enfin, **il est apparu à la délégation que l'efficacité du contrôle *a priori* était largement reconnue par la communauté du renseignement**. Grâce à l'organisation d'un système de permanences, la CNCTR ne s'est, ainsi, jamais trouvée dans la situation où son avis a été réputé rendu faute d'avoir été émis dans le délai légal. Elle semble également faire preuve d'une grande réactivité dans le rendu de ses avis, allant au-delà des contraintes de délais fixés dans la loi. Ainsi, elle a instauré avec les services de renseignement une procédure informelle permettant, en cas de demandes signalées comme prioritaires et spécialement motivées à cet effet, de rendre des avis en moins d'une heure.

Dans les faits d'ailleurs, la procédure d'urgence absolue prévue par l'article L. 821-5 du code de la sécurité intérieure, qui permet au Premier ministre, dans une situation d'urgence, d'autoriser la mise en œuvre d'une technique sans requérir l'avis préalable de la CNCTR, n'a été mise en œuvre qu'une fois, en décembre 2015, à l'occasion d'une suspicion d'attentat terroriste au cours de la nuit de Noël. Aucun service n'estime par ailleurs souhaitable de restaurer la procédure d'urgence opérationnelle, censurée par le Conseil constitutionnel (voir I), au regard de la fluidité des échanges avec la commission.

### 3. Un contrôle a *posteriori* en cours de consolidation

#### *a) Une mission à inventer, qui, au regard des investissements nécessaires, a connu une montée en charge progressive*

Rôle déjà assumé par l'ancienne CNCIS, le contrôle *a posteriori* a, après la loi du 24 juillet 2015, changé de dimension au regard tant du volume de techniques que du nombre de services concernés. La CNCTR a donc dû, rapidement après l'entrée en vigueur de la loi, s'organiser et se forger une doctrine pour exercer du mieux possible cette mission.

Selon les informations communiquées à la délégation, la commission conduit ses contrôles selon **deux méthodes** différentes, en fonction de la nature des techniques concernées.

Lorsque les données sont collectées et centralisées par le GIC, à savoir l'accès aux données de connexion en temps différé, la géolocalisation

[1] *Ces taux sont calculés sur les avis donnés par la CNCTR sur les techniques de renseignement autres que les accès aux données de connexion, en temps réel et en temps différé,* via *les opérateurs.*

en temps réel, le balisage et les interceptions de sécurité réalisées auprès des opérateurs, la CNCTR exerce un **contrôle quotidien, à distance**, depuis ses propres locaux, *via* les applications informatiques sécurisées mises en place par le GIC.

Parallèlement, elle réalise des **contrôles sur pièces et sur place au sein de l'ensemble des services de renseignement ainsi qu'au sein des centres territoriaux du GIC**. L'organisation de ces contrôles a connu une montée en charge progressive depuis l'entrée en vigueur de la loi, au gré de l'augmentation de ses effectifs. Ainsi, alors que 60 déplacements avaient pu être organisés en 2016, le renforcement du secrétariat général à compter de 2017 a permis de réaliser 130 déplacements en 2017, 120 en 2018 et 105 en 2019.

**La fréquence des contrôles réalisés varie selon les services.** Elle dépend, en pratique, de l'importance et de la sensibilité des dossiers traités par le service, ainsi que du nombre et de la nature des techniques mises en œuvre. C'est ainsi que la DGSE et la DGSI, qui sont les principaux consommateurs de techniques de renseignement, font l'objet d'au moins un à deux contrôles sur pièces et sur place par mois. 33 contrôles ont par exemple été menés en 2019 au sein de la DGSE.

A l'inverse, les services qui y recourent de manière ponctuelle ne font l'objet que de quelques contrôles par an. A titre d'exemple :

- un contrôle par mois est effectué au sein des locaux de la DNRED ;

- 9 contrôles par an ont été conduits, en 2018 et en 2019, au sein de la DRSD ;

- le SCRT est en moyenne contrôlé 7 fois par an en centrale, en complément d'autres contrôles organisés de manière plus aléatoires dans les antennes territoriales ;

- 9 contrôles ont été conduits depuis septembre 2018 au sein de la DRPP.

Compte tenu de l'impossibilité évidente de contrôler l'intégralité des techniques mises en œuvre, des données collectées et des extractions et transcriptions réalisées, **la CNCTR fonctionne principalement par ciblage**. La plupart de ses contrôles sont réalisés sur des dossiers identifiés dès le stade du contrôle *a priori*, par exemple en raison du caractère particulièrement intrusif d'une technique demandée. S'agissant du contrôle des techniques de surveillance internationale, elle fonctionne en revanche selon une méthode d'échantillonnage.

La centralisation toujours plus approfondie des données collectées, si elle permet de faciliter les contrôles, n'a **pas vocation à se substituer aux contrôles sur pièces et sur place** qui, de l'avis de la CNCTR, offrent le plus d'enseignements sur la manière dont le cadre légal est mis en œuvre et lui permettent, par ailleurs, de **diffuser sa doctrine au sein des services** et de

répondre aux interrogations des agents de terrain. A cet égard, la CNCTR affirme ne pas s'inscrire dans une logique de contrôles-sanctions, mais bien d'interaction permanente avec les services en vue d'améliorer l'appréhension du cadre légal par l'ensemble des acteurs. Comme elle le relève dans son rapport d'activité pour l'année 2017, « *la réussite d'un contrôle dépend de la coopération constructive entre le service concerné et la commission* ». Cet état d'esprit explique d'ailleurs pourquoi la CNCTR n'a jamais, pour l'heure, recouru à la possibilité d'effectuer des contrôles inopinés, comme le prévoit la loi.

Entendu par la délégation, le président de la commission fait état d'une **parfaite collaboration des services de renseignement à l'occasion des contrôles**. Afin de fluidifier les échanges, la plupart d'entre eux ont identifié des interlocuteurs privilégiés de la commission, chargés de préparer l'organisation des contrôles. La délégation se félicite, en particulier, que la CNCTR ne rencontre aucune difficulté dans l'accès aux données brutes collectées comme aux extractions et transcriptions réalisées par les services.

Au-delà de ces aspects méthodologiques, la CNCTR indique avoir **progressivement approfondi son contrôle** depuis l'entrée en vigueur de la loi du 24 juillet 2015. Alors qu'elle s'était principalement consacrée, jusqu'en 2017, sur le contrôle des modalités de recueil et de conservation des données collectées, elle a, à compter de 2018, également fait porter son attention sur les phases d'exploitation et de transcription. La tâche de la commission consiste, en ce domaine, à s'assurer que les extractions et transcriptions réalisées par les services de renseignement ne sont pas utilisées pour d'autres finalités que celles prévues par l'autorisation concernée[1].

*b) Des irrégularités très rarement constatées, qui n'ont donné lieu qu'à des recommandations peu nombreuses*

Depuis l'entrée en vigueur de la loi, peu d'irrégularités ont été mises à jour par la CNCTR à l'occasion des contrôles qu'elle a pu mener, soit sur les infrastructures du GIC, soit au sein des services de renseignement.

Entendu par la délégation, son président n'a ainsi fait état de la découverte que de **trois irrégularités sérieuses**.

La première, dont la CNCTR a fait état dans son rapport d'activité pour l'année 2018, a été découverte à l'occasion d'un contrôle sur pièces et sur place. Elle se traduisait par la surveillance d'une personne qui n'était pas visée dans l'autorisation initiale du Premier ministre. Bien que la technique ait déjà pris fin lors du contrôle ayant permis de révéler l'irrégularité, les données collectées étaient conservées par le service, conduisant la CNCTR à

[11] *En vertu de l'article L. 822-3 du code de la sécurité intérieure, les extractions et transcriptions réalisées par les services sur la base des données collectées dans le cadre d'une technique de renseignement*

faire usage de son pouvoir de recommandation en vue de la destruction des renseignements collectés illégalement.

La délégation a été informée par la CNCTR de deux nouvelles irrégularités significatives en 2019, pour lesquelles elle n'a pu obtenir d'informations complémentaires.

À l'exception de ces trois cas, **des anomalies de plus faibles gravité ont été détectées**. Celles-ci ont pu porter sur une conservation des données brutes collectées au-delà de la durée légale, ou encore sur la poursuite d'une technique de renseignement alors que des poursuites judiciaires avaient été engagées à l'encontre de la même personne. Selon les informations communiquées par la CNCTR à la délégation, ces anomalies ont toutefois donné lieu à une régularisation immédiate par les services de renseignement concernés et n'ont dès lors pas rendu nécessaire pour la CNCTR de faire usage de son pouvoir de recommandation au Premier ministre.

*c) Un contrôle par nature limité*

Pour lui permettre d'exercer pleinement son contrôle, le législateur a prévu que la CNCTR puisse bénéficier d'un accès permanent, complet et direct aux renseignements recueillis ainsi qu'aux extractions et transcriptions réalisées à partir de ces renseignements[1].

Bien que d'importants progrès aient été conduits en matière de centralisation et de traçabilité pour faciliter cet accès (voir partie II, I), la CNCTR ne dispose, à l'heure actuelle, d'**aucun accès aux fichiers de souveraineté** des services de renseignement, ces derniers s'y étant jusqu'à présent opposés.

Entendue par la délégation, **la CNCTR y voit une limite à l'exercice de son contrôle**. En effet, dès lors que ces fichiers sont susceptibles de contenir des informations recueillies dans le cadre d'une technique de renseignement, elle considère que le fait de ne pouvoir y accéder ne lui permet pas de s'assurer qu'aucune donnée n'a été recueillie, transcrite ou extraite en méconnaissance du cadre légal, voire en l'absence d'une autorisation accordée par le Premier ministre.

Cet obstacle au contrôle de la CNCTR joue non seulement dans le cadre des contrôles *a posteriori*, mais également lorsque la CNCTR est saisie, préalablement à l'engagement d'un recours devant le Conseil d'État, d'une réclamation par une personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard.

Dans cette dernière hypothèse, la délégation considère pourtant essentiel, au regard du droit au recours effectif, que la CNCTR soit en mesure d'exercer pleinement la mission de contrôle que la loi lui confère et dispose de tous les moyens lui permettant d'éclairer le Conseil d'État,

[1] *Art. L. 833-2 du code de la sécurité intérieure.*

lorsqu'elle est sollicitée pour fournir un avis dans le cadre d'une procédure de recours.

À cet égard, il peut être observé que la CNIL, dans le cadre du droit d'accès indirect des citoyens aux données figurant dans un fichier de souveraineté, dispose d'un droit d'accès auxdits fichiers[1].

La délégation considère donc qu'il serait également **opportun de réfléchir à ouvrir un droit d'accès à ces mêmes fichiers à la CNCTR, sur le seul fondement des réclamations dont elle est saisie**. Un tel accès demeurerait, en tout état de cause, ponctuel, au regard du nombre de cas concernés, évalués à moins d'une cinquantaine par la CNCTR à moins d'une cinquantaine par an. La conduite de cette réflexion pourrait être confiée à la CNRLT.

**Recommandation n° 17 : Engager une réflexion en vue d'ouvrir un droit d'accès ponctuel aux fichiers de souveraineté à la CNCTR, lorsqu'elle est saisie de réclamations sur le fondement de l'article L. 833-4 du code de la sécurité intérieure, à l'instar des droits actuellement reconnus à la CNIL.**

### *B. LE DROIT AU RECOURS, ESSENTIEL À LA PROTECTION DES DROITS DES CITOYENS, DEMEURE PEU MIS EN ŒUVRE À CE JOUR*

#### 1. L'ouverture d'un droit au recours spécifique : une innovation de la loi de 2015

*a) Les conditions d'exercice du droit au recours*

L'absence de voies de recours effectives à l'encontre des techniques de renseignement constituait l'une des principales insuffisances du cadre légal qui prévalait avant 2015. La contestation des techniques de renseignement, qui ne pouvait être faite que dans les conditions de droit commun, se heurtait en effet au secret de la défense nationale qui, sauf déclassification, était régulièrement opposé au juge.

Afin de renforcer le droit au recours effectif, le législateur a estimé souhaitable d'ouvrir un accès au juge pour tous les citoyens, aujourd'hui consacré à l'article L. 841-1 du code de la sécurité intérieure. Le contentieux spécifique des techniques de renseignement a été confié à **une formation spécialisée du Conseil d'État, qui statue en premier et dernier ressort.**

**Deux voies de recours ont été instaurées.**

---

[1] *L'article 118 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que, dans le cadre des fichiers relatifs à la sûreté de l'État, le droit d'accès, de rectification ou d'effacement reconnus aux citoyens est exercé de manière indirecte. Les demandes doivent être adressées à la CNIL, qui procède aux vérifications nécessaires. Le demandeur est simplement informé que les vérifications ont été accomplies et de son droit de former un recours juridictionnel.*

Un recours juridictionnel est tout d'abord **ouvert à tous les particuliers qui souhaitent vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à leur égard**.

La recevabilité des requêtes est toutefois **conditionnée à la formation d'un recours administratif préalable obligatoire devant la CNCTR**. Lorsqu'elle est saisie par un particulier, celle-ci est chargée, comme dans le cadre d'un contrôle *a posteriori*, de vérifier l'existence ou non d'une technique et, le cas échéant, de s'assurer de sa régularité. Une fois ses vérifications terminées, elle se borne toutefois à informer l'intéressé de la fin de ses opérations de contrôle.

Le Conseil d'État **peut également être saisi directement par le président de la CNCTR ou par au moins trois de ses membres** lorsque le Premier ministre ne donne pas suite aux avis ou recommandations qu'elle a formulées ou que les suites qui y sont données sont jugées insuffisantes.

De manière à assurer la protection du secret de la défense nationale, **des possibilités d'aménagement de la procédure contradictoire ont été instaurées**. Le Conseil d'État peut ainsi décider de siéger à huis clos, d'entendre les parties séparément ou d'occulter, dans le dossier communiqué au requérant et à sa défense, certains passages.

En cas d'illégalité constatée, le Conseil d'État peut annuler les autorisations correspondantes et ordonner la destruction immédiate des données collectées de manière irrégulière.

*b) La question de l'extension du recours aux techniques de surveillance internationale*

En l'état du droit, les particuliers ne disposent d'aucune voie de recours directe devant le juge administratif pour contester la régularité de techniques de renseignement mises en œuvre par les services au titre de la surveillance internationale. En vertu de l'article L. 854-9 du code de la sécurité intérieure, ils ne peuvent en effet qu'adresser une réclamation à la CNCTR, celle-ci étant la seule compétente pour saisir, en cas d'irrégularité constatée, le juge administratif.

Un bémol a été apporté à ce principe du recours indirect par la loi de programmation militaire pour les années 2019 à 2025. Celle-ci ayant ouvert la possibilité d'exploiter les données collectées dans le cadre d'une technique de surveillance internationale à des fins de surveillance d'une personne située sur le territoire national, elle a logiquement prévu, pour ces personnes, un droit de recours direct devant le juge administratif. Il s'agissait, en effet, d'assurer aux personnes résidant sur le territoire national des possibilités de recours identiques, quel que soit le fondement de leur surveillance.

Dans son rapport d'activité sur l'année 2018, **la CNCTR recommande d'aller plus loin en conférant un droit d'accès direct au juge**

**pour l'ensemble des techniques de surveillance internationale**, à l'instar des techniques mises en œuvre sur le territoire national. Elle « *doute, s'agissant du droit au recours, de la pertinence d'une distinction fondée sur le rattachement au territoire national des identifiants techniques concernés. Aussi recommande-t-elle de permettre à toute personne de saisir le juge administratif de toute mesure susceptible de concerner ses communications électroniques internationales, sous la seule réserve de justifier avoir préalablement saisi la commission d'une réclamation* ».

**La délégation n'estime pas, à ce jour, nécessaire de procéder à cette modification**. Elle considère en effet qu'il n'est pas illégitime qu'une différence soit faite entre les activités conduites par les services de renseignement sur le territoire national, et qui se doivent d'être soumises au respect de l'État de droit, et les activités conduites à l'international. Le Conseil constitutionnel, amené à se prononcer sur le contentieux des techniques de surveillance internationale, a d'ailleurs validé la conformité à la Constitution du dispositif de recours indirect. Il a en effet constaté que bien que « *la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure* », le législateur, « *en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale […] a assuré une conciliation qui n'est manifestement pas disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale* »[1].

### 2. Un contentieux qui demeure faible au regard du nombre de technique

*a) Un droit au recours peu exercé à ce jour*

Dans la pratique, le contentieux des techniques de renseignement a été très faible depuis l'entrée en vigueur de la loi.

Entre début 2016 et fin mai 2020, la formation spécialisée du Conseil d'État a été saisie de **39 requêtes**, toutes formées par des particuliers, après saisine préalable de la CNCTR.

Aucun recours n'a en revanche été porté devant le juge administratif par la CNCTR, ses quelques recommandations au Premier ministre ayant, toutes, été suivies d'effets.

[1] *Décision n° 2015-722 DC du 26 novembre 2015, loi relative aux mesures de surveillance des communications électroniques internationales.*

**Nombre de requêtes présentées (hors référés)**
**sur le fondement de l'article L. 841-1 du code de la sécurité intérieure**
*(au 31 mai 2020)*

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| **Requêtes présentées au titre de l'article L. 841-1 (hors référés)** | 9 | 4 | 11 | 10 | 5 |
| *dont requête de la CNCTR* | *0* | *0* | *0* | *0* | *0* |

*Source : Conseil d'État.*

Dans les faits, il semble que le dispositif de recours administratif préalable devant la CNCTR permette d'assurer un premier filtre et d'éviter un nombre de recours trop important devant le juge. L'on constate, en effet, un écart important entre le nombre de réclamations adressées à la commission et le nombre de recours formés par la suite devant le Conseil d'État.

**Nombre de réclamations reçues par la CNCTR**

| | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|
| **Nombre de réclamations** | 49 | 54 | 30 | 47 |

*Source : CNCTR.*

*b) Des suites judiciaires qui n'ont révélé aucune irrégularité majeure*

A l'exception d'un cas, l'ensemble des recours traités à ce jour par la formation spécialisée du Conseil d'État concernait des personnes ayant de simples soupçons de surveillance mais n'en faisant pas l'objet.

Dans un cas seulement, une technique de renseignement avait effectivement été mises en œuvre.

Sur les 25 décisions rendues au 31 mai 2020**, aucune n'a donné lieu au constat d'une illégalité dans le cadre de la mise en œuvre d'une technique de renseignement.**

### 3. Un contentieux spécifique, dont l'effectivité pourrait être renforcée

*a) Un contentieux asymétrique*

Créée par la loi du 24 juillet 2015, la formation spécialisée du Conseil d'État est composée de **5 membres**, assistés d'un greffe composé de trois

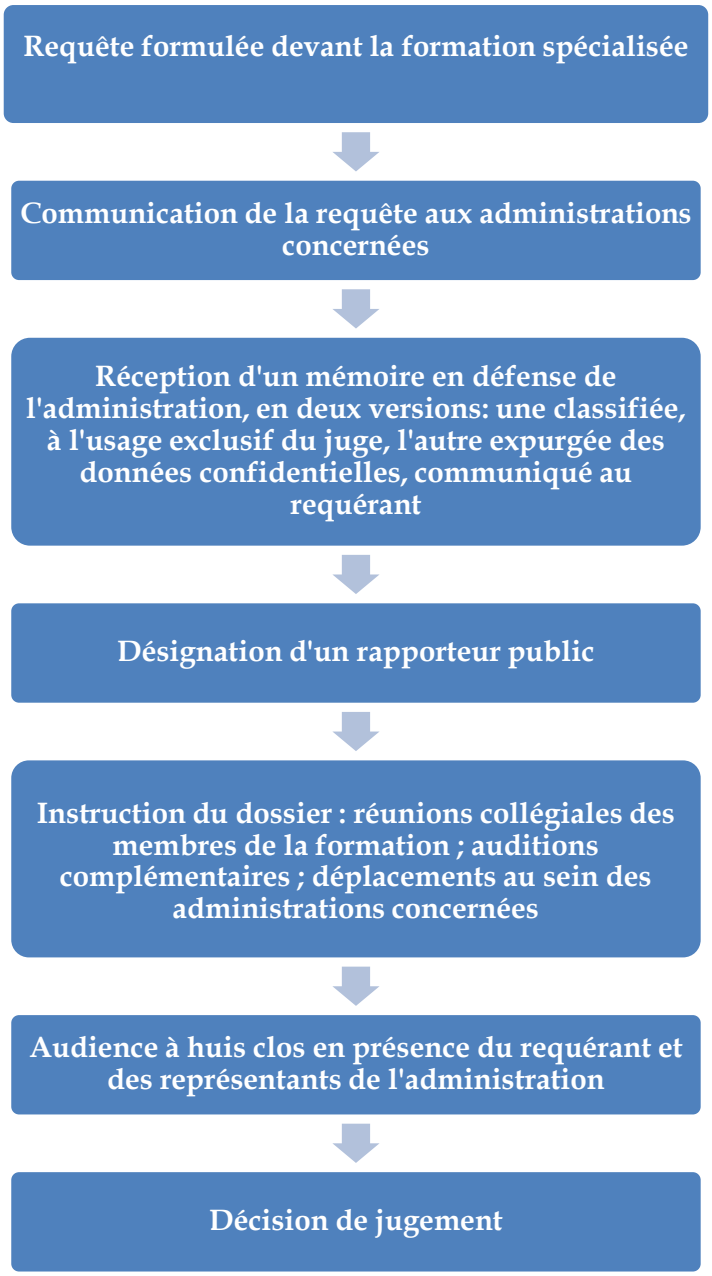
personnes, tous habilités *es qualité* au secret de la défense nationale. **Deux rapporteurs publics** sont chargés de l'instruction des requêtes.

Entendu par la délégation, le président de la formation a insisté sur son **fonctionnement très collégial.** En effet, bien qu'un rapporteur soit, pour chaque affaire, désigné pour instruire le dossier, plusieurs réunions de l'ensemble des membres de la formation de jugement sont généralement organisées avant l'audience.

Ce fonctionnement résulte, de fait, de la **particularité du contentieux asymétrique** prévu par le législateur. Les requérants n'étant pas autorisés à accéder aux données classifiées contenues dans le dossier, il appartient dans la pratique au juge de s'y substituer pour apprécier la fiabilité des données, le respect du cadre légal et, plus globalement, des principes fondamentaux. Il peut également, pour les mêmes raisons, relever d'office tout moyen.

Pour ce faire, la formation est destinataire d'un mémoire en défense classifié de l'administration concernée par le recours. Elle peut également procéder à toutes les auditions qu'elle juge utile, prérogative à laquelle il a été recouru surtout dans le cas des dossiers complexes, pour entendre soit le requérant, soit des représentants de l'administration. Enfin, l'avis de la CNCTR peut être sollicité, ce qui a été systématiquement le cas dans les recours formés à ce jour.

**Procédure applicable au contentieux des techniques de renseignement**




*Source : Délégation parlementaire au renseignement*

*b) Une expertise technique limitée*

Le président de la formation spécialisée a fait état, devant la délégation, de **l'insuffisance des moyens d'expertise technique** à sa disposition pour assurer une instruction efficace des contentieux qui lui sont confiés, qu'il s'agisse du contentieux des techniques de renseignement comme de celui des fichiers relevant de la sûreté de l'État[1].

[1] *En application de l'article L. 841-2 du code de la sécurité intérieure, la formation spécialisée du Conseil d'État est également compétente pour connaître des recours formés par des particuliers pour*

Bien que cette fragilité ne semble pas avoir soulevé de difficultés majeures à ce jour, la formation spécialisée apparaît par exemple dans l'incapacité de s'assurer, si cela venait à être soulevé dans le cadre d'un contentieux, que les techniques de renseignement utilisées ne conduisent pas à collecter des données autres que celles pour lesquelles elles ont été autorisées ou que les fichiers relevant de la sûreté de l'État sont bien conformes, dans leur fonctionnement comme dans leur contenu, au cadre légal et respectent les libertés fondamentales.

Il apparaît dès lors souhaitable à la délégation qu'elle puisse **s'adjoindre, à l'avenir, le concours de personnels techniques.**

Il pourrait, pour ce faire, être envisagé que la formation spécialisée intègre de nouvelles compétences à son équipe, soit par la voie d'un recrutement, soit par la voie de vacations. Une telle solution nécessiterait toutefois que des crédits complémentaires soient alloués au Conseil d'État à cette fin, ce qui, au vu du volume des contentieux traités, demeure une piste incertaine.

A défaut, la délégation estime que pourrait être donnée la possibilité aux magistrats de la formation spécialisée de **requérir, dans le cadre d'un contentieux, l'appui technique, selon les cas, des équipes de la CNCTR ou de la CNIL**. Ces autorités ayant d'ailleurs, lorsqu'un recours est formé par un particulier, été systématiquement saisies en amont par la personne concernée, leurs équipes ont normalement procédé à de premières vérifications techniques ce qui devrait, en pratique, limiter la charge de travail complémentaire induite.

**Recommandation n° 18 : Conférer à la formation spécialisée du Conseil d'État la possibilité de s'adjoindre le concours de personnels techniques, soit par la voie d'un recrutement, soit par la voie d'un appui technique des équipes, selon les cas, de la CNCTR ou de la CNIL, dans le cadre de l'instruction des recours dont elle est saisie.**

*c) Une absence de procédure pour assurer l'effectivité des décisions à combler*

Lors de son audition par la délégation, le président de la formation spécialisée du Conseil d'État a également observé que le législateur n'avait prévu aucune disposition spécifique pour garantir l'exécution, par les services de renseignement, des décisions rendues sur les techniques de renseignement.

Pour l'ensemble du contentieux administratif, sont normalement applicables des procédures dites d'exécution, qui permettent à la personne intéressée par une décision d'engager des démarches auprès de la juridiction

*faire valoir leur droit d'accès, de rectification et d'effacement portant sur des fichiers relevant de la sûreté de l'État.*

administrative l'ayant prononcée, en cas d'inexécution de cette décision par l'administration.

**Les procédures d'exécution des décisions du Conseil d'État**

En application de l'article L. 911-5 du code de justice administrative, le **Conseil d'État est compétent pour assurer l'exécution des décisions qu'il rend en premier et dernier ressort**, dans les conditions fixées par le code de justice administratif.

Sur le plan organisationnel, cette tâche est assurée par la délégation de l'exécution des décisions de justice, qui est rattachée à la **section du rapport et des études.**

La demande d'exécution doit être **formulée par la personne intéressée**, qui pâtit de l'inexécution de la décision rendue par le Conseil d'État. La demande doit être formulée trois mois minimum après la date de la décision, sauf dans deux cas : d'une part, lorsque la décision juridictionnelle a ordonné une mesure d'urgence ; d'autre part, lorsque cette même décision a fixé à l'administration un délai.

Depuis un décret du 6 avril 2017, le Conseil d'État **peut également s'autosaisir** et demander, de sa propre initiative, à l'administration concernée de justifier de l'exécution des décisions qu'il a prononcées.

La procédure d'exécution se déroule en **deux phases** :

- une **phase administrative**, au cours de laquelle la délégation de l'exécution peut accomplir toutes les démarches qu'elle juge utile pour assurer l'exécution de la décision ;

- une **phase juridictionnelle**, qui consiste, pour le président de la section du rapport et des études, à saisir la section du contentieux en vue, le cas échéant,

**Ces procédures se révèlent, en pratique, difficilement applicables au contentieux des techniques de renseignement**.

Si rien n'exclut, en droit, que la personne intéressée puisse saisir le Conseil d'État en vue de vérifier si la décision le concernant a ou non été exécutée, l'exercice de ce droit apparaît, en pratique, plus difficile, dès lors que le requérant ne connait pas le contenu de la décision et est dans l'incapacité d'en constater lui-même l'inexécution.

Surtout, la section du rapport et des études du Conseil d'État normalement chargée de l'exécution des décisions ne dispose pas de personnels habilités et ne peut, dès lors, pas procéder à l'instruction des recours, ainsi que le prévoit le droit en vigueur.

De manière à garantir l'effectivité des décisions rendues par la formation spécialisée du Conseil d'État il serait donc utile, de l'avis de la délégation, que des **dérogations à la procédure habituelle d'exécution**

**soient prévues pour les décisions rendues par la formation spécialisée** et couvertes par le secret de la défense nationale.

Il s'agirait, en premier lieu, de confier à la formation spécialisée, plutôt qu'à la section du rapport et des études, le soin d'instruire les demandes tendant à assurer l'exécution des décisions qu'elle rend et, le cas échéant, de se saisir d'office.

De manière complémentaire, il pourrait également être envisagé de **confier**, selon les contentieux concernés, **à la CNCTR ou à la CNIL, le soin de se substituer au requérant aux fins d'en assurer l'exécution.** Pour ce faire, il pourrait lui être ouvert la possibilité, en cas d'inexécution constatée ou en cas de doute sur l'exécution d'une décision, de saisir, par le biais de son président, la formation spécialisée du Conseil d'État en vue d'engager une procédure d'exécution, qui pourrait comprendre une injonction assortie, le cas échéant, d'une astreinte.

**Recommandation n° 19 : Adapter, pour les décisions rendues par la formation spécialisée, la procédure d'exécution de droit commun :**

**- en confiant à la formation spécialisée le soin d'instruire les requêtes tendant à assurer l'exécution des décisions qu'elle rend et en lui autorisant à se saisir d'office ;**

**- en permettant à la CNCTR ou à la CNIL, en cas d'inexécution constatée d'une décision du Conseil d'État, de saisir la formation spécialisée en vue d'engager une procédure d'exécution.**

# CHAPITRE II :
# LE RENSEIGNEMENT PÉNITENTIAIRE, L'AFFIRMATION D'UN SERVICE EN PREMIÈRE LIGNE DANS LA LUTTE CONTRE LE TERRORISME

Évasion spectaculaire de Redouane Faïd du centre pénitentiaire de Réau, attaque au couteau de deux surveillants à Condé sur Sarthe, hausse de la radicalisation en détention : la question pénitentiaire anime le débat politique et médiatique et interpelle une opinion publique très préoccupée par ce qu'elle sait ou ne sait pas de ce qui se passe dans les prisons françaises.

Dans ce contexte, la prison ne pouvait rester plus longtemps un angle mort du renseignement. La surveillance en milieu carcéral est devenue en quelques années un enjeu central dans le dispositif de lutte contre le terrorisme, conférant au renseignement pénitentiaire une place de plus en plus signifiante.

La montée en puissance du renseignement pénitentiaire, à travers la création d'un service à compétence nationale doté de réels moyens et de prérogatives renforcées, vise à relever le défi de cette menace terroriste devenue endogène, à un moment où s'accélère le rythme des sorties de prison de détenus condamnés pour terrorisme.

## I. LA MONTEE EN PUISSANCE DU RENSEIGNEMENT PENITENTIAIRE

En quelques années, le renseignement pénitentiaire a connu un développement considérable, se hissant au rang des priorités de l'agenda politique et administratif. Dernier né des services de renseignement, le service national du renseignement pénitentiaire dessine progressivement sa place au sein de la communauté du second cercle.

### *A. D'UN BUREAU CENTRAL À UN SERVICE À COMPÉTENCE NATIONALE*

L'organisation d'une véritable structure de renseignement au sein de l'administration pénitentiaire est récente. Elle est consécutive à l'apparition d'une menace terroriste endogène à laquelle il a fallu répondre dans l'urgence – même si ses missions sont plus larges – en s'appuyant sur une culture ancienne du renseignement pénitentiaire dans notre pays.

### 1. Le renseignement pénitentiaire : une pratique ancienne

Le renseignement pénitentiaire existe depuis longtemps dans notre administration, mais il se pratiquait, depuis les années 80, « à la bonne franquette » selon l'expression employée par M. Sébastien Nicolas, secrétaire général du Syndicat national pénitentiaire Force Ouvrière, lors de son audition à l'Assemblée nationale le 21 mars 2019 par la commission d'enquête parlementaire sur « *la situation, les missions et les moyens des forces de sécurité* ». Une quinzaine de personnes seulement étaient jusqu'alors chargées de traiter les informations transmises par les établissements pénitentiaires.

Il faut remonter à un arrêté du 7 janvier 2003 sur l'organisation de la direction de l'administration pénitentiaire pour trouver trace de la création formelle d'un « bureau du renseignement pénitentiaire » au sein de la sous-direction de l'état-major de sécurité. L'article 4 dudit arrêté définit ainsi les missions de ce bureau : « *chargé de recueillir et d'analyser l'ensemble des informations utiles à la sécurité des établissements et des services pénitentiaires, il organise la collecte de ces renseignements auprès des services déconcentrés et procède à leur exploitation à des fins opérationnelles. Il assure la liaison avec les services centraux de la police et de la gendarmerie* ».

Quelques semaines à peine après la publication de cet arrêté, deux évasions spectaculaires à l'arme lourde défrayaient la chronique dans les prisons de Borgo (Corse) et de Fresnes (Val-de-Marne) qui devaient conduire le Gouvernement de l'époque à prendre des mesures de renforcement de la sécurité dans les prisons.

Dans ce contexte, le Bureau du renseignement pénitentiaire a d'abord eu pour objectif d'assurer une surveillance des détenus dits difficiles, avant de voir sa mission étendue, après les attentats de Londres et de Madrid en 2005, aux phénomènes de radicalisation. Néanmoins, le renseignement pénitentiaire n'a disposé, jusqu'à une période récente, que de moyens matériels et humains très limités.

Avec les attentats commis par Mohamed Merah en 2012 puis ceux de janvier et novembre 2015, le renforcement du renseignement pénitentiaire a fait l'objet de nombreuses discussions et de controverses politiques, tant la question de la radicalisation en prison a été au cœur du débat public et demeure un sujet de préoccupation majeur aussi bien pour les autorités politiques que pour l'opinion publique.

### 2. La création du BCRP en 2017…

Le Bureau du renseignement pénitentiaire, dans sa forme et son fonctionnement datant de 2003, a été réorganisé en 2015. Depuis 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, l'action du renseignement pénitentiaire est désormais inscrite dans le cadre légal du renseignement. En avril 2017, un nouveau bureau Central du Renseignement Pénitentiaire (BCRP) a été créé et formellement intégré au second cercle de la communauté du renseignement.

Ce nouveau BCRP reprend les attributions de l'ancien, en y ajoutant la lutte contre le terrorisme et contre la criminalité organisée. Son effectif se trouve alors plus que doublé, passant à une quarantaine d'agents s'appuyant sur un réseau de renseignement pénitentiaire sur l'ensemble du territoire.

Aux termes du livre VIII du code de la sécurité intérieure (CSI), le renseignement pénitentiaire a pour mission d'objectiver et de prévenir les risques d'atteinte aux intérêts fondamentaux de la Nation, ainsi que les risques d'atteinte à la sécurité des personnels pénitentiaires et des personnes détenues.

Le renseignement pénitentiaire poursuivait alors trois finalités :

- la prévention du terrorisme, qui a pris une importance prépondérante ces dernières années ;

- la prévention de la criminalité et de la délinquance organisées ;

- la prévention des évasions et le maintien du bon ordre et de la sécurité dans les établissements.

Les agents du BCRP sont désormais habilités à utiliser des techniques jusque-là réservées à ceux du ministère de l'Intérieur, sous le contrôle de la CNCTR et sur autorisation du Premier ministre.

### 3. …et sa transformation en service national du renseignement pénitentiaire en 2019

Deux ans à peine après sa création, ce « Bureau » s'est mué par arrêté du 29 mai 2019 en « service à compétence nationale ».

La création de services à compétence nationale a été rendue possible par un décret du 9 mai 1997. Ces services se situent à mi-chemin entre les administrations centrales et les administrations déconcentrées. En effet, il s'agit de services dont les attributions ont un caractère national – à la différence des services déconcentrés –, et dont l'exécution ne peut être déléguée à un échelon territorial. Mais ils se distinguent également des services centraux, car leurs missions ont un caractère opérationnel et bénéficient d'une certaine autonomie.

Ce changement de statut fut notamment guidé par la volonté de mettre un terme aux interférences – pour ne pas dire aux contradictions – qui ont pu être relevées entre d'un côté les orientations données aux agents du renseignement pénitentiaire par le BRCP ou les CIRP (cellules interrégionales du renseignement pénitentiaire) et de l'autre, celles qui leur

étaient délivrées, sur le terrain, par leurs supérieurs hiérarchiques du fait de contingences liées à la gestion de la détention. Les agents locaux étaient en effet placés jusqu'alors sous deux autorités : hiérarchique d'une part (celle de leur chef d'établissement) et fonctionnelle d'autre part (celle de la CIRP) Désormais, les cellules interrégionales et les délégations locales sont placées sous l'autorité exclusive de l'échelon central du service national du renseignement pénitentiaire. Concrètement, ce nouveau statut de « service national » permet ainsi au renseignement pénitentiaire de s'émanciper des pesanteurs d'une double tutelle hiérarchique et fonctionnelle.

Le réseau du renseignement pénitentiaire se structure ainsi autour de trois niveaux tels que définis à l'article 4 de l'arrêté du 29 mai 2019 :

- *au niveau local*, chaque établissement pénitentiaire se voit affecter un ou plusieurs délégués locaux au renseignement pénitentiaire (DLRP) qui ne sont plus soumis à l'autorité hiérarchique du chef d'établissement. Le DLRP est le premier opérateur de collecte du renseignement pénitentiaire en milieu carcéral, essentiellement d'origine humaine. *****. Par ailleurs, au sein de chacun des 103 services de probation et d'insertion pénitentiaire (SPIP), un cadre du service est désigné comme référent pour le renseignement pénitentiaire et communique aux CIRP les informations collectées en milieu ouvert en lien avec les objectifs du réseau ;

- *au niveau interrégional*, dix cellules interrégionales sont composées de personnels de l'administration pénitentiaire spécialisés sur la mission de renseignement et d'agents formés à l'investigation numérique et à la recherche en sources ouvertes. Ces derniers œuvrent au recueil et à l'exploitation de la donnée et orientent les capteurs dans les établissements de leur ressort géographique, en lien, le cas échéant, avec les unités déconcentrées des services de renseignement partenaires ;

- *au niveau national*, l'échelon central anime l'ensemble du réseau et entretient les relations institutionnelles avec les partenaires de la communauté du renseignement. L'échelon central est composé de trois bureaux : un bureau de l'administration, un bureau des opérations et un bureau des investigations et de l'analyse.

Enfin, signe de la montée en puissance du renseignement pénitentiaire et de sa pleine intégration au sein de la communauté du renseignement, *****.

### *B. LA SINGULARITÉ DU RENSEIGNEMENT EN MILIEU FERMÉ*

Dans ses murs, le renseignement pénitentiaire se concentre sur quatre menaces principales : les détenus ayant des velléités de passage à l'acte à l'intérieur de la détention, ceux qui préparent de l'intérieur des attentats à l'extérieur, ceux qui travaillent à une évasion et, de plus en plus souvent, ceux repérés comme profils sensibles mais au comportement

exemplaire et qui sont susceptibles de passer à l'acte alors que rien ne laisse le supposer.

Les spécificités de la scène carcérale, liées notamment à la gestion de l'espace et du temps, permettent de se forger une idée plus précise des contraintes qui pèsent sur le cycle du renseignement en milieu fermé, et qui en font la singularité.

À première vue, s'il est un milieu qui se prête facilement au recueil d'informations, c'est bien celui, fermé, des établissements pénitentiaires. En prison, tout se sait et tout se voit ; les lieux sont clos et les individus sont contraints. En application de l'article 727-1 du code de procédure pénale, les détenus savent que leurs communications téléphoniques autorisées peuvent être légalement écoutées – hormis celles avec leur avocat – sous le contrôle du procureur de la République territorialement compétent.

Pourtant, même si cela peut sembler paradoxal, faire du renseignement en milieu carcéral se révèle être une mission bien plus complexe et souvent plus risquée qu'en milieu ouvert. La parfaite connaissance des lieux que permet le milieu carcéral est à la fois un atout et un inconvénient. En effet, toutes les personnes qui interviennent en milieu fermé, à un titre ou à un autre, sont connues et leurs missions sont identifiées et tracées. La totalité des espaces sont cartographiés ainsi que les flux de circulation d'un endroit à un autre, selon des horaires préétablis ce qui permet une prévisibilité complète des déplacements et des usages en milieu fermé. *****. Dès lors, tout ce qui sort des schémas préétablis devient suspect, d'autant que rares sont les personnels qui ont à en connaître.

### 1. La primauté du renseignement d'origine humaine

L'essentiel du renseignement pénitentiaire est d'origine humaine. En prison, l'information est principalement recueillie par l'intermédiaire des agents pénitentiaires, qui sont la source de renseignement la plus importante parce qu'en contact permanent avec les détenus. Ce sont les premiers témoins de ce qui peut attirer l'attention. La particularité du renseignement pénitentiaire réside également dans le fait que le SNRP est chargé du traitement de signalements pour tous les types d'intervenants en détention (personnels pénitentiaires, aumôniers, intervenants socio-culturels, personnels privés partenaires, etc.)..

Ce facteur humain est essentiel pour comprendre les rouages du renseignement pénitentiaire. En effet, ce qui peut sembler anodin en milieu ouvert est susceptible de devenir un levier pour obtenir des informations : un changement de cellule, un transfert d'établissement, le droit de travailler, *etc*.

*****

### 2. Un environnement peu propice aux techniques de renseignement

À travers l'écoute de la téléphonie légale (art. L. 727-1 du code de procédure pénale), le renseignement pénitentiaire peut exploiter des informations obtenues à partir des échanges téléphoniques autorisés des détenus. La saisie des téléphones portables illégalement introduits en milieu carcéral peut également être une source de renseignement très utile.

Mais depuis que la loi du 3 juin 2016[1] l'y autorise, le renseignement pénitentiaire peut également avoir recours à la plupart des techniques de renseignement de la loi de 2015, au titre des finalités suivantes :

- la prévention du terrorisme (art. L. 811-3, 4° du CSI) ;

- la prévention de la criminalité et de la délinquance organisées (art. L 811-3, 6° du CSI) ;

- la sécurité au sein des établissements pénitentiaires (art. L-855-1 du CSI) ;

- une quatrième finalité a été octroyée au SNRP par le décret n° 2019-1503 du 30 décembre 2019 qui élargit la possibilité de mettre en œuvre certaines techniques de renseignement à la contre-subversion et aux mouvances extrêmes violentes (a, b et c de la finalité 5° de l'article L. 811-3 du CSI).

*****

**Demandes de techniques de renseignement mises en œuvre par le BCRP puis le SNRP par finalités**

*Tableau* *****

*****. Le groupement technique des opérations pénitentiaires (GTOP) est l'illustration remarquable d'une coopération intégrée entre services de renseignement, l'un du premier cercle et l'autre du second cercle. Plutôt que de partir de zéro, le SNRP s'appuie sur l'expertise technique de la DGSI, à laquelle il apporte sa connaissance fine du milieu carcéral.

La création du GTOP repose sur :

- une mutualisation de moyens matériels et de ressources humaines, un partage des infrastructures et des coûts ;

---

[1] *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.*

- un partage d'expériences entre d'un côté l'expertise technique de la DGSI et de l'autre la connaissance du milieu pénitentiaire par le SNRP ;

- une compétence nationale avec une capacité de déploiement sur l'ensemble du territoire.

*****

### *C. LES DÉFIS DU RENSEIGNEMENT PÉNITENTIAIRE*

La montée en puissance du renseignement pénitentiaire est le reflet d'une progression très importante, en peu de temps, de l'activité de renseignement. Celle-ci se mesure à travers plusieurs indicateurs comme le nombre d'objectifs suivis et le volume des techniques de renseignement mises en œuvre

#### 1. Le défi de l'exponentiel : l'augmentation du nombre des personnes suivies

La création du BCRP en 2017 est allée de pair avec une hausse très forte du nombre d'objectifs à suivre, jusqu'à 3 000 détenus, sur une population carcérale d'environ 70 000 personnes. Cette augmentation exponentielle est bien sûr liée au contexte de lutte contre le terrorisme qui a suivi la vague d'attentats de 2015 et 2016. Le renseignement pénitentiaire se trouve en première ligne dans le cadre de la mise en œuvre du plan national du Gouvernement pour la prévention de la radicalisation « Prévenir pour protéger », de février 2018.

Parmi les objectifs suivis par le renseignement pénitentiaire, il faut distinguer les détenus pour terrorisme (525 TIS au 6 janvier 2020) des détenus de droit commun suivis du fait de leur radicalisation avérée (585 RAV au 28 mai 2020). À cela s'ajoute le suivi de près d'un millier de détenus particulièrement surveillés pour risque d'évasion, de mise à mal de la sécurité pénitentiaire ou de criminalité organisée au sein des murs. Aux cibles identifiées en milieu fermé s'ajoutent également 728 individus suivis en milieu ouvert, répartis entre 454 RAV et 274 TIS.

Ramené aux effectifs du service, le nombre d'objectifs suivis par agent du renseignement pénitentiaire se révèle particulièrement élevé, si on le compare à d'autres services de renseignement ; et ce malgré les nombreux recrutements réalisés ces dernières années au sein du SNRP. *****. L'augmentation progressive du nombre des DLRP dans les établissements pénitentiaires, et leur professionnalisation ont également accru la quantité d'informations recueillies et en conséquence le travail d'analyse de renseignement.

À l'échelon des circonscriptions interrégionales comme au niveau central, chaque analyste est ainsi chargé d'un suivi pouvant aller de 70 à 120

objectifs contre une quarantaine habituellement dans les autres services de renseignement ; au-delà de ces suivis individuels, les informations à traiter augmentent continûment, l'intégration du renseignement pénitentiaire au sein de la communauté nationale du renseignement ayant démultiplié les transmissions en provenance des partenaires et l'exploitation des techniques de recueil de renseignement, désormais accessibles au SNRP, mobilise les analystes.

Cette augmentation du nombre des personnes suivies n'est pas un phénomène ponctuel mais correspond à une évolution structurelle de la menace qui doit conduire à mieux organiser et à professionnaliser le renseignement pénitentiaire.

*****. La Délégation parlementaire au renseignement a saisi la Garde des Sceaux le 20 septembre 2019 pour demander la communication du rapport de l'Inspection générale de la justice sur cette agression. Outre le fait que le rapport ne lui a pas été communiqué, la Délégation s'étonne que la chancellerie n'ait même jamais répondu à son courrier et aux nombreuses relances. Aussi, la DPR préconise une évolution législative à l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958, en soumettant le Gouvernement d'une part, au respect d'un délai maximum – un mois – pour répondre à une demande de transmission d'un document par la DPR et d'autre part, en le contraignant à motiver sa décision en cas de refus.

**Recommandation n° 20 : Inscrire à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 l'obligation pour le Gouvernement de respecter le délai maximum d'un mois pour répondre à une demande de transmission d'un document par la DPR et de motiver sa décision en cas de refus.**

### 2. Le défi des ressources humaines

La création du BCRP puis sa transformation en service à compétence nationale se sont accompagnées d'un plan massif de recrutements puisqu'en cinq ans, les effectifs du renseignement auront été multipliés par plus de dix. Il faut toutefois rappeler qu'avant même la création du « nouveau BCRP » en 2017, le plan de lutte contre le terrorisme du 21 janvier 2015 avait considérablement accru le nombre d'agents du réseau de renseignement pénitentiaire, aux niveaux central, interrégional et local. Ses effectifs ont à cette époque été renforcés de plus d'une centaine de nouveaux emplois.

L'évolution des effectifs réels se révèle être conforme aux prévisions de la loi de programmation de la justice pour la période 2018-2022, avec un effectif du SNRP qui devrait atteindre 329 postes d'ici à la fin de l'année 2020. 109 postes auront ainsi été créés entre 2018 et 2020.

**Effectifs du renseignement pénitentiaire**
***(en ETPT réels/théoriques)***

| | 2014 | 2015 | 2016 | Fin 2017 | Fin 2018 | Fin 2019 |
|---|---|---|---|---|---|---|
| Echelon central | 13/13 | 11/15 | 13/17 | 39/39 | 42/42 | 75/80 |
| CIRP | 14/14 | 34/42 | 37/42 | 128/128 | 128/128 | 134/137 |
| DLRP temps plein | - | 7/30 | 37/44 | 40/49 | 77/84 | 79/84 |
| **TOTAL** | **27/27** | **52/87** | **87/103** | **207/216** | **247/254** | **288/301** |

*Source : Direction de l'administration pénitentiaire.*

Les créations de postes ont majoritairement bénéficié aux CIRP, afin de renforcer les fonctions support mais aussi la capacité d'analyse, notamment à travers la prise en charge à l'échelon interrégional du traitement des sources humaines. Le nombre de postes de DLRP, au sein des établissements pénitentiaires, est également en forte progression.

Selon l'échelon territorial auquel on se trouve, il existe des différences quant au profil et au statut des personnes recrutées. La politique de recrutement associe trois cultures professionnelles distinctes : celle de l'administration pénitentiaire, celle des services partenaires et aussi une culture extérieure pour certains métiers spécifiques : informaticiens, traducteurs, spécialistes de la veille sur internet…

Plus on est proche du terrain, plus les agents de renseignement sont des fonctionnaires de l'administration pénitentiaire. Au niveau des cellules interrégionales, les profils sont plus variés avec des analystes, des traducteurs et donc une proportion plus importante de personnels contractuels et/ou de fonctionnaires détachés. *****, le service ayant besoin de compétences disposant déjà d'une expertise en renseignement, ce qui nécessite, pour une structure jeune, d'aller chercher cette ressource à l'extérieur. C'est par exemple le cas actuellement avec le détachement d'un personnel de la DGSE.

La montée en puissance du renseignement pénitentiaire suppose la mise en place d'une véritable filière RH du renseignement pénitentiaire, avec l'émergence de nouveaux besoins en termes de formation, un volet indispensable à la montée en compétence des agents. Un département dédié au renseignement pénitentiaire se structure au sein de l'Ecole nationale de l'administration pénitentiaire (ENAP) et les liens sont renforcés avec l'Académie du renseignement, signe de la pleine intégration du renseignement pénitentiaire au sein de la communauté du renseignement.

Se pose aussi la question de l'attractivité du métier d'agent du renseignement pénitentiaire. Une réflexion est en cours sur la pertinence, ou non, qu'il y aurait à instaurer un régime indemnitaire dédié à la filière du renseignement. Faut-il attribuer un logement de fonction aux DLRP ? Comment fixer un régime indemnitaire dédié au renseignement pénitentiaire sans prendre le risque de réduire la mobilité entre les services ? Faut-il et comment privilégier une approche interministérielle qui permettrait de donner du sens à certaines mutualisations au sein de la communauté du renseignement ?

Ces questions restent pour beaucoup sans réponse à ce stade mais le changement d'échelle du renseignement pénitentiaire appelle à des décisions rapides sur ces sujets.

La délégation préconise d'aller plus en avant dans cette démarche en expertisant les voies et modalités de création d'un régime indemnitaire dédié aux métiers du renseignement pénitentiaire.

**Recommandation n° 21 : Expertiser la possibilité de créer un régime indemnitaire dédié aux métiers du renseignement pénitentiaire.**

### 3. Le défi des moyens budgétaires

Le budget alloué au BCRP, puis au SNRP, est passé de 20 millions d'euros en 2017 (montant exécuté) à près de 23 millions d'euros en 2020 (dotation). Cette hausse significative s'explique par l'augmentation des effectifs du service qui ont augmenté d'environ 80 ETP depuis 2017. Hors masse salariale, le renseignement pénitentiaire dispose en 2020 d'un budget de 2,63 millions d'euros.

**Budget du BCRP puis du SNRP**

*(en millions d'euros)*

| | Exécuté 2017 | Exécuté 2018 | Exécuté 2019 | Dotation 2020 |
|---|---|---|---|---|
| Titre 2 – Dépenses de personnel | 16,70 | 15,79 | 18,56 | 20,35 |
| Titre 3 – Dépenses de fonctionnement | 2,19 | 0,97 | 2,05 | 2,44 |
| Titre 5 – Dépenses d'investissement | 1,18 | 0,93 | 0,78 | 0,00 |
| Titre 6 – Dépenses d'intervention | | | 0,19 | 0,19 |
| Total hors T2 (masse salariale) | 3,37 | 1,90 | 3,03 | 2,63 |
| **Total** | **20,07** | **17,68** | **21,58** | **22,98** |

*Source : Direction de l'administration pénitentiaire.*

Les investissements réalisés par le SNRP concernent l'acquisition d'équipements (*****) et le déploiement du système d'information classifié nécessaire à la structuration du service.

*****

**Recommandation n° 22 : *****

### 4. Le défi du droit

Il ressort des auditions effectuées par la Délégation parlementaire au renseignement que des évolutions pourraient être apportées aux règles juridiques qui encadrent le renseignement pénitentiaire afin de parachever sa professionnalisation.

Une première évolution pourrait consister à élargir aux agents du renseignement pénitentiaire la possibilité de recourir à une identité d'emprunt ou à une fausse qualité, comme c'est autorisé pour les agents des services du premier cercle. *****.

**Recommandation n° 23 : Élargir aux agents du renseignement pénitentiaire la possibilité de recourir à une identité d'emprunt dans l'exercice de leurs missions.**

Une deuxième évolution pourrait concerner l'allongement de la durée de conservation des enregistrements de téléphonie légale, actuellement fixée à 3 mois par l'article 727-1 du code de procédure pénale[1]. En pratique, cette durée de conservation se révèle très courte au vu de la masse de données liées à la téléphonie passée légalement. L'écoute et la retranscription en temps différé des conversations passées nécessite d'importants moyens humains et beaucoup de temps. Dans ces conditions, la durée de conservation de trois mois peut avoir pour effet de rendre inopérante l'exploitation des données enregistrées. A cet allongement de la durée de conservation, il conviendrait également de développer les outils de traduction et de transcription automatique de la parole avec captation de mots clés.

**Recommandation n° 24 : Allonger la durée de conservation des enregistrements de téléphonie légale (article 727-1 du code de procédure pénale) et recourir à des outils de traduction et de transcription automatique de la parole pour améliorer l'exploitation des données conservées.**

Une troisième évolution pourrait concerner l'extension du nombre des techniques de renseignement auxquelles le SNRP à accès. Actuellement, les seules techniques qui lui sont interdites sont d'une part, la surveillance en temps réel des connexions électroniques d'un individu aux fins de détection du terrorisme (prévue à l'article L. 851-2 du CSI) et d'autre part, le recours à l'algorithme censé pouvoir détecter dans le flux les communications numériques de potentielles connexions en lien avec une menace terroriste. C'est sur ce second point que porte la demande du SNRP. La technique de l'algorithme a été autorisée à titre expérimental par la loi du 24 juillet 2015 pour les services du premier cercle et il appartient au législateur, au plus tard le 31 décembre 2020, de décider de pérenniser cette technique, de la supprimer ou de modifier la liste des services autorisés à l'utiliser. Au vu du rôle confié au renseignement pénitentiaire dans la lutte contre le terrorisme, et dès lors que la technique de l'algorithme vise exclusivement cette finalité, il conviendrait d'expertiser la possibilité pour le SNRP d'y recourir, le moment venu.

**Recommandation n° 25 : Expertiser la possibilité pour le SNRP de recourir à la technique de l'algorithme si elle venait à être pérennisée par la loi.**

[1] *Cette durée de conservation maximale de 3 mois ne concerne que les seuls enregistrements qui ne sont suivis d'aucune transmission à l'autorité judiciaire en application de l'article 40.*

## II. LE RENSEIGNEMENT PENITENTIAIRE AU CŒUR DU DISPOSITIF DE LUTTE CONTRE LE TERRORISME

L'évolution de la menace terroriste, de plus en plus endogène, conduit à conférer au renseignement pénitentiaire un rôle central dans le dispositif de lutte contre le terrorisme. La radicalisation en prison présente des enjeux sécuritaires, autant à l'intérieur qu'à l'extérieur des prisons. En amont comme en aval, c'est toute la chaîne du renseignement qui s'en trouve impactée.

### *A. UNE SURVEILLANCE RENFORCÉE DE LA POPULATION CARCÉRALE*

L'institution pénitentiaire prend en charge environ 250 000 personnes placées sous main de justice, dont 70 651 étaient détenues au 1er janvier 2020, dans un contexte bien connu de sur-occupation carcérale.

#### 1. L'impératif de sécurité en milieu fermé

Les conditions de détention d'individus « radicalisés » ou en voie de radicalisation doivent permettre de les isoler des autres détenus pour éviter le prosélytisme et la propagation des processus de radicalisation.

*a) Le « profilage » des détenus*

L'administration pénitentiaire établit deux profils distincts de détenus liés à l'islam radical : d'une part, les détenus incarcérés pour des faits de terrorisme en lien avec l'islam radical (les « TIS ») et d'autre part, les détenus incarcérés pour des faits de droit commun mais signalés pour radicalisation (les « DCSR »). Cela représente un total d'environ 1 500 détenus qui nécessitent une attention particulière.

- *Les TIS*

En janvier 2020, on dénombrait 525 détenus – dont 72 femmes – considérés comme terroristes islamistes, en raison du motif de leur condamnation judiciaire. Les TIS sont automatiquement inscrits au Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT).

Après avoir triplé entre 2015 et 2017, le nombre de TIS est désormais stabilisé autour de 500. La France est néanmoins le pays d'Europe qui recense le nombre de détenus terroristes le plus important – près de la moitié du nombre total de TIS à l'échelle européenne –, loin devant le Royaume-Uni (autour de 250 TIS) puis la Belgique.

**Évolution du nombre de détenus TIS**

| Au 02/01/2017 | Au 26/12/2017 | Au 05/02/2019 | Au 06/01/2020 |
|---|---|---|---|
| **390** | **507** | **499** | **525** |

*Source : Direction de l'administration pénitentiaire.*

• *Les détenus de droit commun suivis pour radicalisation avérée (RAV)*

Aux TIS s'ajoutent les détenus incarcérés pour des faits de droit commun mais signalés pour radicalisation. Cette qualification et leur dangerosité sont donc liées soit à leur comportement à l'extérieur, repéré par les services de renseignement partenaires, soit à leur comportement en détention, repéré par l'administration pénitentiaire, ce qui implique une part de subjectivité en comparaison avec les TIS dont la qualification est liée au motif de leur condamnation.

L'administration pénitentiaire évalue le nombre de détenus de droit commun dont la radicalisation est avérée (RAV) à 585 personnes au 20 mai 2020, contre 627 au 1er janvier 2020, soit une diminution de 6,7 % en seulement quatre mois. A ces 585 détenus RAV, il faut ajouter 269 détenus considérés par le renseignement pénitentiaire, au 6 janvier 2020, comme « potentiellement radicalisés » (radicalisé en évaluation – RAE) et faisant à ce titre l'objet d'une évaluation par le SNRP.

La décroissance régulière du nombre de RAV (en baisse de 16 % entre mai 2019 et mai 2020) s'explique notamment par l'amélioration des critères de repérage et d'évaluation de la radicalisation par les agents du SNRP positionnés tant au sein des établissements qu'aux échelons interrégional et central. Ce renforcement des méthodologies et du savoir-faire des agents permet de clore le suivi d'individus qu'il n'est plus pertinent de considérer comme présentant une menace du fait de leur radicalisation.

À la différence des TIS qui relèvent d'une population de stock, la catégorie des détenus radicalisés fait référence à une population de flux, avec un taux de renouvellement élevé, proche de 50 %. La population pénale présente en effet des fragilités psychiques et sociales et qui viennent renforcer la vulnérabilité au phénomène de radicalisation.

Il est d'ailleurs remarquable, selon des données transmises à la délégation par l'administration pénitentiaire, que 25,9 % des personnes inscrites au FSPRT : au sein de la population hébergée en établissement pénitentiaire ont été détectées par l'administration pénitentiaire.

**Nombre de détenus TIS et RAV par établissement pénitentiaire**

*(au 6 janvier 2020)*

*Tableau ******

*b) Des conditions d'incarcération adaptées*

La stratégie pénitentiaire de repérage, d'évaluation et de prise en charge des détenus radicalisés est une composante majeure de la politique de prévention du terrorisme. En milieu fermé, elle repose sur une adaptation des conditions d'incarcération aux profils des détenus. La loi du 21 juillet 2016[1] a ainsi durci le régime d'exécution des peines en excluant les terroristes des réductions de peine automatique et en les privant de certains aménagements de peines (semi-liberté, suspension et fractionnement de peines, par exemple).

• *L'évaluation de la radicalisation*

Tous les détenus condamnés pour des faits de terrorisme ainsi que les détenus condamnés pour des faits de droit commun identifiés comme radicalisés ont vocation à passer par des quartiers de prise en charge de la radicalisation spécialisés dans l'évaluation (QPRE). Au renseignement pénitentiaire revient toutefois la tâche de prioriser les détenus radicaux dont la dangerosité et le prosélytisme doivent être évalués en urgence. 94 détenus ont ainsi été évalués au sein de 4 QER en 2018 et 151 l'ont été en 2019 au sein de 6 QER.

La création des QER fin 2016, a mis fin aux unités de prévention de la radication (UPRA) constituées au sein d'établissements situés exclusivement en Ile-de-France pour regrouper des détenus radicalisés, mais qui furent considérées comme un échec en favorisant un climat de violence ayant conduit à l'agression de deux surveillants à la prison d'Osny (Val-d'Oise) en septembre 2016.

L'administration pénitentiaire en a tiré les enseignements en concluant qu'avant de prendre en charge les détenus considérés comme radicalisés, il était d'abord nécessaire de les évaluer. C'est la vocation des QER, dont le premier a ouvert en février 2017 à la prison d'Osny ; il en existe désormais sept. Ces unités visent non seulement à détecter et évaluer les personnes détenues radicalisées, mais aussi à protéger les personnels pénitentiaires par un renforcement des dispositifs de formation, une sécurisation accrue et un régime de détention plus sévère que pour les autres détenus : fouilles régulières, davantage de caméras, moins d'activités collectives et presque un surveillant pour chaque détenu. Ceux-ci passent énormément de temps en cellule et certains barreaux ont même été remplacés par des vitres, pour éviter tout contact avec l'extérieur.

---

[1] *Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.*

Les QER accueillent les détenus pendant une durée de dix-sept semaines au cours desquelles ils sont évalués par des éducateurs, des psychologues, des référents religieux et des personnels de surveillance. Le but est d'évaluer le niveau d'honnêteté du détenu et sa potentielle capacité de dissimulation, la *taqiya* étant une pratique répandue chez les personnes radicalisées. Viennent ensuite l'évaluation du niveau de dangerosité, la probabilité de passage à un acte violent, puis le niveau de prosélytisme.

• *Des modalités de détention différenciées selon le niveau de dangerosité*

Il s'agit pour l'administration pénitentiaire, à l'issue de cette période d'évaluation, d'être en mesure de décider en connaissance de cause des modalités de la prise en charge future des détenus. Trois options sont alors possibles :

- la grande majorité des détenus passés par un QER, environ 75 %, sont placés en détention dite ordinaire car leur imprégnation idéologique est considérée comme faible. Ils font l'objet d'un suivi spécifique par le renseignement pénitentiaire et sont mis à l'écart du reste de la population carcérale, dans des « quartiers étanches » dans l'un des 78 établissements (sur 188) qui ont mis en œuvre des programmes de prévention de la radicalisation violence (PPRV) ;

- le placement à l'isolement pour les détenus considérés comme les plus dangereux, qui représentent environ 10 % des prisonniers évalués. Ceux-ci entrent dans la catégorie des idéologues très violents, présentant un risque d'agression physique et jugés incompatibles avec une prise en charge collective en détention. Ils ne croisent que des personnels dédiés et spécialement formés et ne sont jamais en contact avec d'autres détenus ;

- les détenus ne relevant d'aucune des deux catégories précédentes, soit environ 15 % des prisonniers évalués, seront affectés dans un quartier de prise en charge de la radicalisation (QPR). Il existe à ce jour 4 QPR à Lille-Annœullin, Condé-sur-Sarthe, Aix-Luynes et à Paris au sein de la prison de la Santé. Sont placés en QPR les détenus évalués appartenant à la catégorie des idéologues prosélytes ou susceptibles d'être violents mais accessibles à une prise en charge collective. En d'autres termes, les détenus concernés doivent démontrer leur volonté de désengagement à l'égard de la violence et du prosélytisme. Les QPR sont considérés comme une voie médiane, une sorte de « sas » entre la détention ordinaire et le quartier d'isolement. Les promenades y sont organisées en effectif réduit dans une cour intérieure dédiée, à l'abri des regards des autres prisonniers. Les petits groupes sont régulièrement renouvelés de manière à éviter la routine qui, en détention, représente un danger pour la sécurité. L'affectation en QPR est transitoire ; il ne s'agit pas en effet d'y effectuer la totalité de sa détention. La durée de passage y varie de six à dix-huit mois, éventuellement renouvelable, avant de réintégrer un régime de détention classique.

Après l'échec des UPRA, la mise en place de nouvelles méthodes d'évaluation de la radicalisation s'est donc accompagnée d'une politique d'adaptation des conditions de détention au niveau de dangerosité des prisonniers. Ce nouveau dispositif reste en cours de déploiement avec de nouvelles ouvertures de QER et de QPR prévues au cours du second semestre 2020 et du premier trimestre 2021 avec un nouveau QER à Vendin-le-Vieil et deux nouveaux QPR à Nancy et à Bourg-en-Bresse.

La délégation recommande qu'au moins un QER et un QPR soient dédiés aux femmes détenues.

**Recommandation n° 26 : Ouvrir un quartier d'évaluation de la radicalisation (QER) et un quartier de prévention de la radicalisation (QPR) dédié aux femmes.**

### 2. De nouveaux dispositifs de suivi en milieu ouvert

L'assassinat en juillet 2016 d'un prêtre à Saint-Etienne-du-Rouvray par un individu radicalisé sous bracelet électronique a provoqué une prise de conscience quant à la nécessité urgente à « boucher les trous dans la raquette » entre la prison et l'extérieur. Face à la multiplication des profils d'individus susceptibles d'être sensibles aux thèses djihadistes en milieu ouvert, l'administration pénitentiaire a dû adapter son dispositif.

Sur les 160 000 personnes suivies en milieu ouvert, quelques 274 sont en effet impliqués dans une affaire de terrorisme islamiste (TIS) et 474 qui relèvent du droit commun sont considérés comme radicalisés avérés (RAV). La réalité des profils est celle d'un éventail extrêmement large : on identifie parmi ces personnes sous main de justice quelques « revenants » de Syrie ou velléitaires du jihad mais surtout des individus poursuivis pour « apologie du terrorisme » ou « consultation de sites djihadistes » et des délinquants suspectés de radicalisation.

En milieu ouvert, il s'agit d'accompagner ces profils dits de « bas du spectre », que la justice n'a pas estimé nécessaire d'incarcérer ou qui ont obtenu un aménagement de leur peine, vers le désengagement d'une idéologie violente et, au bout du compte, la réinsertion. Tous sont suivis par le service de probation et d'insertion pénitentiaire (SPIP) dont des cadres ont été formés comme référents pour la radicalisation.

Pour les profils les plus complexes, un dispositif sur mesure dénommé « PAIRS » a été mis en place. Il s'agit d'un « Programme d'accueil individualisé et de réaffiliation sociale », qui succède à l'expérimentation non concluante du centre de déradicalisation de Pontourny, ouvert en octobre 2016 et fermé dès février 2017.

En complément de la prise en charge par un service pénitentiaire d'insertion et de probation qui demeure titulaire du mandat judiciaire, le

programme permet un suivi renforcé et pluridisciplinaire de personnes faisant l'objet d'une procédure ou exécutant une peine en lien avec une infraction terroriste. Ce nouveau dispositif, d'abord expérimenté à Paris a été étendu à Marseille, à Lille et à Lyon, et propose désormais 110 places.

Des rencontres sont organisées avec des éducateurs, des psychologues et des conseillers pénitentiaires sous la forme de temps d'échanges pouvant aller de 10 à 20 heures hebdomadaires. L'accent est ainsi mis sur l'efficacité d'un accompagnement intensif dans le processus de désengagement de l'idéologie violente.

Au moindre incident, un rapport est adressé au juge et le renseignement est alerté. A ce jour, on ne dénombre aucun passage à l'acte violent d'un profil terroriste ou radicalisé suivi hors de prison.

### 3. Le défi d'un retour en nombre des djihadistes français pour nos prisons

Parmi les Français partis rejoindre Daech en Irak ou en Syrie, ceux revenus sur le territoire français ont fait l'objet d'une judiciarisation systématique à leur retour qui s'est accompagnée, pour certains d'entre eux, d'une incarcération.

**Djihadistes français ayant fait l'objet d'une incarcération à leur retour en France**

*Tableau* *****

Les services de renseignement estiment qu'environ 200 ressortissants français se trouveraient encore détenus par les forces kurdes dans le nord-est de la Syrie.

La question de leur possible retour en France représente un défi pour notre système carcéral. Ces combattants sont des personnes très aguerries qui ont vécu pendant une longue durée dans une zone de guerre ; elles présentent a priori un niveau de dangerosité bien plus élevé que les autres détenus et nécessitent un suivi spécifique par le renseignement pénitentiaire.

Le retour des djihadistes français pose trois défis à notre système pénitentiaire :

- le premier est d'ordre capacitaire ***** ;

- le deuxième concerne la prise en charge des femmes radicalisées, dont le nombre est en augmentation régulière ces dernières années, au point que davantage de femmes que d'hommes revenant du djihad ont été incarcérées en 2019 ; et cette tendance semble se poursuivre au premier trimestre 2020. Le profil de ces femmes est généralement moins connu des

services de renseignement que celui des hommes. Les établissements pénitentiaires pour femmes ne sont pas adaptés à la prise en charge de la radicalisation ; on n'y trouve à ce jour ni QER ni QPR. ;

- le troisième est relatif aux mineurs : ils seraient déjà près de 150 à être revenus des zones de combat avec leurs parents, dont une forte majorité est âgée de moins de dix ans. Une circulaire du Premier ministre du 23 février 2018 définit un dispositif de prise en charge spécifique qui s'appuie largement sur le droit commun tout en mettant en œuvre des dispositions innovantes telles que le recours à des mesures de protection de l'enfance et la mise en place systématique d'un bilan somatique et médico-psychologique.

### *B. LA PRISE EN CHARGE DES SORTANTS DE PRISON*

L'enjeu sécuritaire que représente l'élargissement des terroristes islamistes (TIS) et des détenus de droit commun susceptibles de radicalisation appelle une coopération étroite entre le renseignement pénitentiaire et les services qui sont chargés de leur suivi une fois libres.

#### 1. L'exigence d'anticipation

*a) Se préparer à l'augmentation importante du nombre de sortants de prison*

Flavien Moreau, le premier djihadiste jugé en France à son retour de Syrie, est sorti de prison en janvier 2020. Il avait été condamné en 2014 à sept ans de prison pour « association de malfaiteurs en vue de la préparation d'un acte de terrorisme ».

La libération des détenus condamnés pour terrorisme est une source de préoccupation tant pour les pouvoirs publics que pour l'opinion publique. Entre 2018 et 2022, on évalue en effet à 355 le nombre de détenus TIS libérés ou libérables.

**Libérations effectives ou prévues de détenus TIS**

| **Année** | 2018 | 2019 | 2020 *(prév.)* | 2021 *(prév.)* | 2022 *(prév.)* |
|---|---|---|---|---|---|
| **Sorties** | 100 | 72 | 70 | 63 | 50 |

*Source : Direction de l'administration pénitentiaire.*

Le nombre de libérations plus important en début de période s'explique par le fait que les premiers détenus pour terrorisme, jugés au début des années 2010 et arrivés en fin de peine, ont fait l'objet de condamnations moins lourdes – généralement de 5 à 10 ans de prison – que

par la suite dans les affaires de terrorisme. Cette population des sortants représente un enjeu de taille : le régime des peines ayant été durci, les « sorties sèches » se multiplient. Sans dispositif dédié, les sortants pourraient retrouver leur liberté sans aucune obligation, ni suivi des services pénitentiaires.

*****

**Libérations effectives ou prévues de détenus inscrits au FSPRT**

*Tableau ***** *

*****

*****. La crise sanitaire liée à l'épidémie de covid-19 a également conduit à la libération anticipée de 8 000 détenus pour endiguer la propagation de la covid-19 dans les prisons, sans que cela ne concerne les détenus condamnés pour des crimes, des faits de nature terroriste ou les auteurs de violences conjugales.

L'ordonnance du 25 mars 2020 a créé trois dispositifs spécifiques :

- la remise en liberté, sous assignation à domicile, des détenus condamnés à une peine inférieure ou égale à 5 ans et dont le reliquat de peine est inférieur à deux mois ;

- l'octroi de remises de peine spéciales d'un maximum de deux mois pour les détenus qui auront adopté un comportement exemplaire durant la période d'état d'urgence sanitaire ;

- l'aménagement des peines inférieures à 6 mois sous la forme du travail d'intérêt général.

Auditionné 15 avril 2020 par la Commission des Lois de l'Assemblée nationale, Stéphane Bredin, directeur de l'administration pénitentiaire, a apporté des précisions sur le travail d'identification des prévenus ou détenus de droit commun suivis au titre de la radicalisation et concernés par l'ordonnance du 25 mars 2020 : 130 personnes inscrites au FSPRT étaient concernées pour lesquelles un avis du SPIP et du chef d'établissement a été sollicité. Stéphane Bredin a indiqué qu'« *au 14 avril 2020, onze de ces détenus, dont certains ont été retirés du FSPRT au moment de leur sortie, ont été libérés : deux ont fait l'objet d'une assignation à domicile et neuf d'une réduction de peine supplémentaire. Tous avaient la perspective d'une sortie très prochaine, parfois dans quelques jours* ».

*****

*b) Renseigner au mieux le profil de chaque détenu libéré*

Il ne s'agit pas seulement d'anticiper la date de sortie d'un détenu, mais aussi de disposer d'informations circonstanciées sur le profil de la personne libérée, et son niveau de dangerosité. Les profils des sortants de prison se révèlent très divers, et la menace qu'ils représentent, elle aussi est variée.

Lorsqu'un individu inscrit au FSPRT est incarcéré, c'est le renseignement pénitentiaire qui devient chef de file pour son suivi. *****.

*****

**2. L'exigence d'une coordination renforcée**

Nécessité faisant loi, la mise en place de nouveaux mécanismes de coopération vient bousculer les pratiques des services de renseignement qui reposent habituellement sur le cloisonnement et la protection du secret. Or le partage de l'information et la fluidité des circuits de transmission sont des éléments clés pour lutter efficacement contre le développement d'une menace terroriste endogène qui se nourrit de ses réseaux en milieu carcéral.

*a) Le rôle pivot de l'UCLAT à l'échelon central*

Il revient à l'UCLAT d'assurer le suivi centralisé de la problématique des sortants de prison.

Depuis la mi-2018, l'UCLAT a mis en place une unité spécialisée comprenant un officier issu de l'administration pénitentiaire. Cette unité spécialisée, dont la nature est autant technique qu'administrative, n'est pas chargée du suivi opérationnel des sortants de prison ; sa mission consiste à s'assurer de l'attribution de chaque sortant de prison – TIS et RAD – à un service de renseignement.

À cette fin, une réunion mensuelle nationale se tient le quatrième mardi de chaque mois ; elle associe les services de police et de gendarmerie ainsi que ceux du ministère de la Justice. Cette réunion mensuelle organisée par l'UCLAT se tient en présence de la CNRLT. *****.

*****

*b) Le suivi territorial au sein des GED*

Une part importante de la coopération opérationnelle entre les différents services de l'État se joue en effet au niveau départemental sous la direction du préfet à qui revient la charge de présider les GED (groupes d'évaluation départementaux).

Les GED sont composés des services de renseignement (échelon local de la DGSI et SDRT, échelon départemental du SCRT), du procureur de la République, de la gendarmerie et de la police nationale et désormais aussi

du renseignement pénitentiaire qui s'y trouve pleinement intégré. Les GED se réunissent généralement une fois tous les quinze jours, voire sur un rythme hebdomadaire dans les départements concernés par un grand nombre de personnes à suivre.

Lorsque le détenu est libéré, l'UCLAT s'assure auprès de la Préfecture et des services concernés que l'individu a bien été pris en compte, qu'un service est chargé de son suivi et que les rubriques correspondantes du FSPRT ont bien été modifiées.

Si le sortant de prison radicalisé a été condamné à une peine de milieu ouvert, le directeur du SPIP territorialement compétent s'assure de la poursuite de la prise en charge du radicalisé sortant de prison et évoque la situation de l'intéressé lors des cellules pour la prévention de la radicalisation et l'accompagnement des familles.

En revanche, les procureurs de la République n'ont à ce jour toujours pas accès au FSPRT, alors qu'ils participent aux GED. La Délégation considère qu'ils devraient pouvoir, à l'instar des autres participants, consulter ce fichier.

**Recommandation n° 27 : Autoriser les procureurs de la République à accéder au FSPRT.**

**Une coordination des services maintenue pendant la période de confinement**

Les GED ont maintenu leur activité pendant la période de confinement. L'UCLAT a ainsi été destinataire de 231 relevés de décisions émanant des GED et a participé à 2 GED en audioconférence ou visioconférence avec les départements de la Loire-Atlantique (44) et de l'Essonne (91). Une visioconférence a également été organisée avec les référents radicalisation des 7 zones de défense, notamment pour s'assurer de la bonne tenue des GED.

S'agissant plus spécifiquement des sortants de prison, les réunions mensuelles de coordination présidées par l'UCLAT ont été maintenues malgré le confinement. Elles ont ainsi pu se tenir en mars et en avril.

### 3. La permanence du suivi

Une fois sortis de prison, il s'agit donc de pouvoir garantir la permanence du suivi des personnes dont les services de renseignement estiment qu'elles demeurent susceptibles de présenter une menace pour la sécurité nationale. Pour les TIS étrangers qui présentent une « menace grave à l'ordre public », des mesures d'éloignement peuvent être ordonnées ; cela a concerné 44 sortants de prison au 31 décembre 2019.

Pour eux, la permanence du suivi après leur passage en prison ne se pose plus. En revanche, pour les autres, ce volet aval du renseignement

pénitentiaire se révèle aujourd'hui être un point de faiblesse de notre dispositif de suivi.

*a) Les MICAS : un outil juridique utilisé faute de mieux pour les sortants de prison*

La loi du 30 octobre 2017, dite « loi SILT », a introduit dans le droit commun diverses mesures inspirées des dispositions de la loi du 3 avril 1955 relative à l'état d'urgence. Parmi elles, figurent les MICAS (mesures individuelles de contrôle administratif et de surveillance), qui succèdent aux assignations à résidence prises dans le cadre l'état d'urgence.

Entre le 1er novembre 2017 et le 31 décembre 2019, 205 personnes ont fait l'objet d'une mesure individuelle de contrôle administratif et de surveillance. Sur ces 205 MICAS, 82 ont concerné des sortants de prison, qu'il s'agisse de TIS ou de détenus de droit commun dont la radicalisation était connue avant ou est apparue pendant leur peine d'emprisonnement.

Les statistiques du ministère de l'intérieur montrent l'augmentation continue des sortants de prison dans le total des MICAS, passant de 31 % au cours de la première année d'application de la loi à 57 % l'année suivante. Ces chiffres sont cohérents dans la mesure où ils traduisent l'accélération du rythme des libérations de détenus TIS et qu'en pratique, 100 % des sortants TIS font l'objet d'une MICAS.

La MICAS n'est certes pas l'unique moyen de suivi des sortants de prison ; mais cette mesure de police administrative, qui peut être utilisée en complément d'une mesure de contrôle judiciaire, présente un intérêt majeur. D'une part, parce qu'elle restreint la latitude opérationnelle des personnes à qui elle s'applique ; d'autre part, parce que l'astreinte du pointage quotidien permet de faire remonter des informations sur leur environnement direct.

Néanmoins, le recours aux MICAS se heurte à une difficulté majeure liée à leur durée. En effet, au-delà de six mois, une MICAS ne peut être renouvelée qu'en cas d'éléments nouveaux ; et ce renouvellement ne peut excéder six mois. En outre, la durée totale d'une MICAS ne peut excéder 12 mois, le Conseil constitutionnel ayant explicitement indiqué dans sa décision du 16 février 2018[1] que « *compte tenu de sa rigueur, cette mesure ne saurait, sans méconnaître les exigences constitutionnelles excéder, de manière continue ou non, une durée totale cumulée de douze mois* ».

Si la durée totale d'une MICAS ne saurait dépasser douze mois, la question reste ouverte quant à la possibilité de soumettre consécutivement un même individu à plusieurs MICAS comprenant des obligations différentes, au-delà d'une durée de douze mois. A ce jour, la conformité à la Constitution d'une telle pratique n'a pas été examinée par le Conseil constitutionnel. Mais en en tout état de cause, cela souligne l'absence de dispositif juridique adapté au profil des condamnés pour terrorisme, pour

[1] *Décision n° 2017-691 QPC du 16 février 2018.*

ceux dont la dangerosité ne diminue pas à leur sortie de prison et pour lesquels les mesures de suivi post-sentencielles sont inadaptées.

*b) La nécessité d'un régime de sûreté ah doc pour les sortants de prison*

Aussi, pour répondre à une inquiétude légitime des Français, notre droit doit rapidement s'adapter afin de fixer un cadre juridique dédié au suivi des sortants de prison, pour ceux d'entre eux susceptibles de représenter une menace pour la sécurité nationale.

Ce régime *ad hoc*, qui n'aurait vocation à s'appliquer que lorsque les dispositifs existants s'avèrent insuffisants concernerait les personnes condamnées pour des faits de terrorisme et en passe d'être libérées. Il viendrait ainsi renforcer les outils dont notre pays dispose pour prévenir les risques de passage à l'acte. Pour pouvoir être d'application immédiate, il ne doit pas être qualifié ou même être qualifiable de peine : il doit s'agir de mesures de sûreté.

Il imposera de requérir l'avis préalable de la commission pluridisciplinaire des mesures de sûreté, qui aura accès pour se prononcer à l'ensemble des pièces des dossiers judiciaire et pénitentiaire, sur la dangerosité de la personne concernée.

Les sortants de prison concernés par ce régime se verraient soumis à diverses obligations, cumulatives ou non, telles que :

- répondre aux convocations du juge d'application des peines ;

- établir leur résidence en un lieu déterminé ;

- obtenir une autorisation avant tout changement d'emploi ou de résidence ainsi que pour tout déplacement à l'étranger ;

- régime de présentation périodique ;

- interdictions d'entrer en relation et de paraître dans certains lieux ;

- placement sous surveillance électronique mobile.

Il reviendrait au tribunal de l'application des peines – dont la formation collégiale est une garantie essentielle – de prononcer tout ou partie de ces mesures de sûreté.

Celles-ci seraient ordonnées pour une durée d'un an, renouvelable dans une limite de dix ans en matière correctionnelle et vingt ans en matière criminelle. Des sanctions – amende et peine d'emprisonnement – devront être prévues en cas de non- respect des mesures prononcées.

Le sortant de prison pourrait demander la modification ou la levée de ces mesures.

La délégation parlementaire au renseignement considère que cette possibilité nouvelle de suivi des personnes purgeant une peine de prison

pour des faits de terrorisme est aujourd'hui indispensable pour assurer dans de bonnes conditions la sécurité des Français.

**Recommandation n° 28 : Instaurer un régime de sûreté *ad hoc* pour les sortants de prison.**

*

* *

Quelques années auront finalement suffi au renseignement pénitentiaire pour conquérir sa légitimité au sein de la communauté du renseignement. Mais ce renseignement, singulier à plus d'un titre, doit encore poursuivre sa montée en puissance pour occuper toute sa place dans la chaîne du renseignement.

Et si l'impératif de la lutte contre le terrorisme a motivé le développement et la structuration du renseignement pénitentiaire, cette finalité pourrait le moment revenu revenir au second plan face à sa vocation première que représente la sûreté pénitentiaire.

# CHAPITRE III :
# LA MAÎTRISE DES RISQUES

*« Dire le secret des autres est une trahison, dire le sien est une sottise. »*
*Voltaire*

Ces dernières années, la presse s'est fait l'écho de plusieurs affaires impliquant des agents ou d'anciens agents des services de renseignement, qui ont mis en lumière des cas de compromission du secret de la défense nationale et des manquements déontologiques graves. À l'aune de ces informations, la délégation a décidé de consacrer une partie de ses travaux à l'audit des dispositifs de contrôle en vigueur dans les services, destinés à maîtriser les risques auxquels ils sont exposés.

À la suite de l'attaque au couteau perpétrée à la préfecture de police le 3 octobre 2019 par l'un de ses agents, la délégation a souhaité élargir le champ de ses travaux pour prendre en compte les risques qui se sont fait jour au regard du profil de l'assaillant[1]. Cela l'a conduite à s'intéresser à la procédure d'habilitation ainsi qu'à la sécurité et la sûreté[2] des services de renseignement.

## I. LA PROCÉDURE D'HABILITATION

En matière de protection du secret de la défense nationale, la procédure d'habilitation constitue la première phase – et probablement la plus importante – de la chaîne de maîtrise des risques.

### *A. L'ENQUÊTE D'HABILITATION*

Les enquêtes de sécurité visent à évaluer les vulnérabilités personnelles des candidats ou des membres du personnel déjà habilités, et leur compatibilité avec les fonctions exercées. L'objectif est de se prémunir de tout risque de compromission du secret de la défense nationale, c'est-à-dire d'éviter qu'une information ou un support classifié ne soit porté à la connaissance d'une personne non habilitée ou n'ayant pas le besoin d'en connaître.

---

[1] *L'assaillant était agent d'un service de renseignement, habilité au niveau « secret-défense », potentiellement radicalisé et affecté au sein d'un service informatique.*

[2] *La sécurité désigne l'ensemble des moyens (humains, techniques, organisationnels) de prévention et d'intervention utilisés contre les risques à caractère accidentel. La sûreté s'attache quant à elle à prévenir et entraver les actes malveillants.*

Suivant les fonctions occupées et les informations dont ils auront à connaître, les services ou les personnes pressenties pour y être affectées initient une demande d'habilitation à l'un des trois niveaux de classification définis aux articles R. 2311-2 et R. 2311-3 du code de la défense :

- le niveau « très secret-défense », réservé aux informations et supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense nationale ;

- le niveau « secret-défense », réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale ;

- le niveau « confidentiel-défense », réservé aux informations et supports dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié au niveau « secret-défense » voire « très secret-défense ».

### 1. Les services enquêteurs

Les enquêtes d'habilitation sont réalisées par quatre services enquêteurs :

- les trois services mentionnés à l'article 24 de l'instruction générale interministérielle n° 1300 (IGI 1300), à savoir la direction générale de la sécurité intérieure (DGSI), la direction du renseignement et de la sécurité de la défense (DRSD) et la direction générale de la sécurité extérieure (DGSE) ;

- et la direction du renseignement de la préfecture de police de Paris (DRPP) qui participe aux enquêtes administratives sur la base d'un protocole signé avec la DGSI.

Ainsi, la DRPP n'est pas consacrée par l'IGI 1300 comme un service enquêteur, ce qui peut constituer une fragilité sur le plan juridique en cas de recours concernant les avis de sécurité qu'elle émet. Sa participation aux enquêtes administratives est prévue par le décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la DGSI, et l'arrêté du 6 juin 2006 portant règlement général d'emploi de la police nationale, et s'effectue sur la base d'un protocole « confidentiel-défense »[1].

[1] *Ce protocole a été signé avec la DGSI le 21 février 2019.*

Les modes opératoires d'enquête de la DRPP sont néanmoins identiques à celles de la DGSI : les deux services s'échangent leurs « bonnes pratiques », et des formations sont régulièrement dispensées par la direction générale de la sécurité intérieure (méthodes d'entretien, sensibilisation sur les vulnérabilités liées aux réseaux sociaux, *etc.*). En outre, la DRPP lui adresse un tableau d'activités récapitulant l'ensemble des dossiers traités, ainsi qu'une copie de tous les dossiers défavorables ou restrictifs afin de permettre un suivi centralisé des dossiers d'une part, et un « contrôle qualité » d'autre part.

| | Structure interne chargée des enquêtes | Ressources humaines | Missions | Populations concernées | Statistiques |
|---|---|---|---|---|---|
| **DRSD** | Centre national des habilitations de défense (CNDH), rattaché à la sous-direction des centres nationaux d'expertises (SDCNE).<br><br>*NB : les enquêtes sur le personnel du service sont assurées par le « bureau enquêtes personnel service » (BEPS), qui relève du CNDH. Les enquêtes sur le personnel du BEPS sont réalisées par un autre bureau du CNDH.* | *Effectifs* : 135 personnes au CNDH, dont 6 au BEPS habilités « secret défense » (un officier, deux sous-officiers, 2 personnels civils de catégorie B et un militaire du rang).<br><br>*Ancienneté moyenne* : 4 ans à la DRSD, 2 ans au sein du BEPS. Les agents du BEPS sont choisis parmi les personnels affectés au CNHD. | Enquêtes administratives pour le renseignement et la sûreté (EARS) au profit de l'ensemble de la sphère défense. | - Ensemble de la sphère défense : forces armées, directions et services du ministère, base industrielle et technologique de défense, division des applications militaires du CEA (commissariat à l'énergie atomique et aux énergies alternatives) et entreprises contractant avec la DAM (direction des applications militaires ;<br><br>- personnel de la DRSD (y compris les stagiaires). | - *Nombre d'organismes étatiques ou industriels concernés par les EARS* : 6 800.<br><br>- *Nombre d'avis restrictifs* : 130 agents du service font l'objet d'un avis restrictif au niveau « secret défense ». |

| | Structure interne chargée des enquêtes | Ressources humaines | Missions | Populations concernées | Statistiques |
|---|---|---|---|---|---|
| **DGSI** | - Un service en charge des enquêtes ***** ;<br>- *****. | ***** | Enquêtes sur le personnel de la DGSI et contrôles après habilitation. | Personnel de la DGSI, y compris les enquêteurs. | - *Nombre d'enquêtes menées de janvier à novembre 2019* : 787, dont 564 pour des premières demandes (557 au niveau « secret défense » et 7 au niveau « très secret défense ») et 223 pour des renouvellements (222 au niveau « secret défense » et 1 au niveau « très secret défense »).<br>*NB : quelque 1 000 enquêtes sont menées chaque année.*<br>- *Résultat des enquêtes (de janvier à novembre 2019)* : 645 avis sans objection, 88 mises en éveil et 6 avis défavorables.<br>- *Durée moyenne des enquêtes* : 3 mois ½. |
| | ***** | ***** | ***** | ***** | ***** |

| | Structure interne chargée des enquêtes | Ressources humaines | Missions | Populations concernées | Statistiques |
|---|---|---|---|---|---|
| **DGSE** | Service de la sécurité du personnel, rattaché au service de sécurité, lui-même dirigé par le directeur de cabinet (n° 2 du service).<br>*<u>NB</u> : une cellule est dédiée aux enquêtes sur la population des enquêteurs et de l'encadrement supérieur du service. En outre, un bureau est spécialement chargé des échanges avec les autres services de sécurité de la communauté du renseignement.* | *<u>Effectifs</u>* : 50 personnes environ.<br>*<u>Ancienneté moyenne</u>* : 10 ans à la DGSE, 5 ans dans le poste. | - Enquêtes sur les candidats au recrutement ;<br>- suivi du personnel de la DGSE ;<br>- émission des avis de sécurité, des avis d'habilitation et des avis d'opportunité ;<br>- conseil en matière de sécurité ;<br>- liaison avec les services nationaux ;<br>- octroi des badges d'accès ;<br>- avis sur l'encadrement supérieur et les désignations à l'étranger ;<br>- avis sur les congés à l'étranger ;<br>- enquêtes sur les personnes morales de droit privé et les personnes physiques passant des marchés publics avec la DGSE ;<br>- émission d'avis techniques d'aptitude à détenir des informations classifiées au sein des entreprises. | - Personnel de la DGSE ;<br>- entreprises intervenant sur les sites de la DGSE ;<br>- vacataires linguistes accédant au site.<br>*<u>NB</u> : les agents des services du premier cercle placés pour emploi bénéficient d'un accès à la DGSE octroyé sur la base de leur habilitation de sécurité fournie par leur service d'origine. Cet accès est révocable sur décision du service de sécurité.* | - *<u>Recrutements</u>* : 1 831 enquêtes réalisées en 2018 (contre 1 677 en 2017).<br>- *<u>Suivi des agents</u>* : 972 enquêtes réalisées en 2018 (contre 1 521 en 2017).<br>- *<u>Durée moyenne des enquêtes</u>* : de 1 à 3 mois suivant la complexité du dossier. |

| | Structure interne chargée des enquêtes | Ressources humaines | Missions | Populations concernées | Statistiques |
|---|---|---|---|---|---|
| **DRPP** | Section des enquêtes, rattachée à la sous-direction du support opérationnel.<br>*NB : cette structure est opérationnelle depuis 2018. Les agents ont été recrutés en interne, sur la base du volontariat, après entretien avec le sous-directeur. Ils sont tous habilités au niveau « secret défense ».* | *Effectifs* : 14 fonctionnaires de police, dont un commandant de police qui encadre la section. | Une unité est en charge des enquêtes d'habilitation des personnels de la DRPP, et une autre unité est chargée des enquêtes pour le reste de la préfecture de police de Paris. | - Personnels administratifs et actifs de catégories A (hors corps préfectoral), B et C ;<br>- contractuels ;<br>- réservistes ;<br>- stagiaires.<br>*NB : certains cadres de la DRPP sont habilités au niveau « très secret-défense ». Les enquêtes d'habilitation qui les concernent sont réalisées par la DGSI.*<br>*Par ailleurs, aucun étudiant n'est accueilli en stage à la DRPP. Les stagiaires susvisés concernent la préfecture de police.* | - *Nombre d'enquêtes d'habilitation menées en 2018* : 491 (contre 266 en 2017) réparties comme suit :<br>○ 191 pour le niveau « confidentiel défense » (169 admissions et 22 renouvellements) ;<br>○ 300 pour le niveau « secret défense » (227 admissions et 73 renouvellements).<br>- *Durée moyenne des enquêtes* : 3 mois pour les admissions DRPP et de 4 à 9 mois pour les autres directions.<br>Le délai pour les renouvellements est compris entre 6 et 12 mois.<br>- *Nombre d'avis défavorables* : 3 pour la DRPP en 2017 et en 2018 (et au moins 4 en 2019). |

*Source : Délégation parlementaire au renseignement, à partir des réponses des services à son questionnaire écrit.*

### 2. Le cadre juridique

Afin d'initier la procédure d'habilitation, chaque candidat doit constituer un dossier en renseignant une notice individuelle 94 A qu'il remet à son officier de sécurité pour en vérifier la complétude. Il l'adresse ensuite à l'autorité d'habilitation – à savoir le SGDSN, le délégataire du ministre (haut fonctionnaire de défense et de sécurité, préfet) ou l'autorité de sécurité déléguée (ASD)[1] – qui procède également à une vérification du dossier, puis le transmet pour instruction au service enquêteur ou au SGDSN s'il s'agit d'une habilitation au niveau « très secret-défense »[2].

Pour les services du MINARM (hors DGSE), pour les niveaux « confidentiel-défense » et « secret-défense », la demande d'habilitation est adressée directement au service enquêteur via l'application SOPHIA mise à disposition par la DRSD. Pour le niveau « très secret-défense », la demande est adressée au SGDSN.Une enquête est alors diligentée par l'un quatre services précités, d'après un cadre réglementaire commun composé :

- des dispositions du code de la sécurité intérieure et du code de la défense ;

- de l'instruction générale interministérielle n° 1300 (IGI 1300) qui décrit l'organisation générale de la protection du secret de la défense nationale, en clarifiant les obligations juridiques et matérielles inhérentes à cette protection. Cette instruction définit également les procédures d'habilitation et de contrôle des personnes pouvant avoir accès au secret.

À ce cadre juridique s'ajoutent des réglementations propres à chaque service, comme par exemple :

- une déclinaison de l'IGI 1300 par chaque ministère (l'instruction ministérielle du ministère de la défense (MINDEF) n° 900 DEF/CAB/DR du 26 janvier 2012, relative à la protection du secret de la défense nationale au sein du ministère des armées (IM 900), en est une illustration) ;

- le décret n° 2015-386 du 3 avril 2015 fixant le statut des fonctionnaires de la DGSE ;

- des notes internes.

---

[1] *L'article R. 2311-10-1 du code de la défense dispose que :* « Le secrétaire général de la défense et de la sécurité nationale peut, en sa qualité d'autorité nationale de sécurité pour le secret de la défense nationale, nommer dans des domaines particuliers, notamment dans le domaine industriel, sur proposition du ou des ministres intéressés, une autorité de sécurité déléguée. »

[2] *Le SGDSN n'est alors chargé que de l'instruction du dossier, l'enquête étant menée par les services compétents.*

Le service chargé de l'enquête est déterminé suivant le niveau d'habilitation[1], le profil du candidat (civil ou militaire) et l'autorité d'habilitation qui lui soumet le dossier (un service de renseignement, une administration de l'État ou une industrie de défense).

L'enquête se fonde sur des critères objectifs permettant de déterminer si le candidat, par son comportement ou son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour le secret, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions[2] qui pourraient mettre en péril les intérêts de l'État.

À travers cette enquête administrative, le service s'assure donc que le candidat peut connaître d'informations et de supports classifiés sans risque pour la défense et la sécurité nationale, ni pour sa propre sécurité. Les conclusions de l'enquête sont communiquées à l'autorité d'habilitation pour éclairer sa décision.

### 3. Les moyens mis en œuvre pour la réalisation des enquêtes

*a) La consultation des sources ouvertes et les criblages*

Pour réaliser les enquêtes, les services consultent tout d'abord plusieurs sources ouvertes qui permettent, entre autres, de vérifier l'empreinte numérique du candidat (« traces » laissées sur internet à travers les réseaux sociaux, *etc.*).

Les services disposent également des informations portées à leur connaissance par le candidat *via* la notice individuelle 94 A. Ces informations servent au « criblage » du candidat, c'est-à-dire à l'interrogation de plusieurs fichiers[3] qui peuvent permettre de déceler certaines vulnérabilités :

- les fichiers de souveraineté des services de renseignement ; les services enquêteurs se sollicitent mutuellement afin d'interroger leurs fichiers respectifs ;

- les fichiers de police, de gendarmerie et de renseignement comme le traitement d'antécédents judiciaires (TAJ), le fichier des personnes

---

[1] *Pour le niveau « très secret-défense », les enquêtes d'habilitation sur les personnels de la préfecture de police ne sont pas réalisées par la DRPP mais par la DGSI.*

[2] *Exercés par un service de renseignement étranger, un groupe terroriste, ou encore un individu ou une organisation se livrant à des activités subversives.*

[3] *Aux termes de l'article L. 234-1 du code de la sécurité intérieure,* « Un décret en Conseil d'État fixe la liste des enquêtes administratives mentionnées à l'article L. 114-1 qui donnent lieu à la consultation des traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 du code de procédure pénale, y compris les données portant sur des procédures judiciaires en cours, dans la stricte mesure exigée par la protection de la sécurité des personnes et de la défense des intérêts fondamentaux de la Nation. Il déterminera les conditions dans lesquelles les personnes intéressées sont informées de cette consultation. » Cf. *décret n° 2018-141 du 27 février 2018 portant application de l'article L. 114-1 du code de la sécurité intérieure.*

recherchées (FPR), le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT), *etc.*

En tant que de besoin, les services enquêteurs peuvent solliciter la mise en œuvre de techniques de renseignement (investigations techniques), voire la réalisation de vérifications de domicile .

*b) Des méthodes d'enquête hétérogènes*

Certains services procèdent à des recherches sur l'environnement « large » du candidat. À cet effet, des documents complémentaires lui sont demandés :

- pour les candidats au recrutement à la DRSD, une annexe a été ajoutée à la notice individuelle 94 A[1] depuis janvier 2019. Elle vise à identifier toute personne susceptible d'appartenir au cercle relationnel proche du candidat ;

- à la DRPP, la notice individuelle 94 A doit être accompagnée de divers documents pour le niveau « secret-défense » (copie du livret de famille, copie de pièces d'identité, état civil de la fratrie et des conjoints, justificatif de domicile).

Par ailleurs, dans leur processus de recrutement interne, certains services de renseignement font également intervenir un psychologue, et rendent systématique l'entretien de sécurité – ce qui devrait être la règle pour l'habilitation aux niveaux « secret-défense »[2] et « très secret-défense ». Toutefois, ces pratiques sont disparates par manque de temps (*cf.* tableau ci-dessous sur les délais moyens d'enquête) ou de ressources (tous les services ne comptent pas tous un psychologue parmi leurs effectifs). Ces deux entretiens sont pourtant indispensables pour approfondir la recherche de vulnérabilités et déclencher, si nécessaire, de nouvelles investigations.

**Recommandation n° 29 : Harmoniser les procédures d'habilitation des agents des services de renseignement, en systématisant l'entretien de sécurité et l'entretien avec un psychologue.**

Des éléments statistiques portés à la connaissance de la DPR font apparaître de fortes disparités s'agissant des ressources humaines consacrées aux enquêtes et leur durée moyenne.

Par ailleurs, comme l'a souligné la délégation parlementaire au renseignement dans son précédent rapport, le stock de demandes d'habilitation non traitées peut constituer un frein au processus de recrutement et peut même, dans certains cas, le remettre en cause. En effet,

[1] *La notice individuelle 94 A ne s'intéresse qu'aux ascendants, descendants et conjoints.*

[2] *La DGSI a indiqué que toutes les personnes habilitées au niveau « secret-défense » n'étaient pas soumises à l'entretien de sécurité.*

pour les profils les plus recherchés, la durée d'habilitation peut dissuader les candidats de poursuivre la procédure et les conduire ainsi à privilégier d'autres propositions d'emploi.

| Ministère de tutelle | Service enquêteur | | Nombre d'avis rendus par ETP du 1er janvier au 30 septembre 2019 | Stock de demandes d'avis au 30 septembre 2019 | Durée moyenne d'enquête |
|---|---|---|---|---|---|
| Ministère de l'intérieur | DGSI | ***** | ***** | ***** | ***** |
| | | ***** | ***** | ***** | ***** |
| | DRPP | | 29 | 153 | 3 à 12 mois |
| Ministère des armées | DRSD | | 129 | 0 | 30 à 101 jours |
| | DGSE | | 104 | 151 | 1 à 3 mois |

*Source : Délégation parlementaire au renseignement, à partir du rapport de l'inspection des services de renseignement en date du 10 décembre 2019.*

Ces éléments suscitent plusieurs observations et interrogent sur l'homogénéité des enquêtes d'habilitation :

- en premier lieu, l'existence de plusieurs structures d'enquêtes au sein d'un même ministère, voire au sein d'un même service de renseignement, mérite d'être relevée. En théorie, ces structures accomplissent la même mission et les candidats devraient, peu ou prou, faire l'objet de la même enquête, suivant les mêmes critères. Aussi le nombre de structures peut-il engendrer des difficultés d'harmonisation des méthodes d'investigation et d'animation transversale de ces structures par le SGDSN ;

- en second lieu, malgré un nombre d'avis rendus par agent bien supérieur à celui des autres services enquêteurs, la sous-direction de la protection économique peine visiblement à résorber son stock de demandes d'habilitation. Le directeur général de la sécurité intérieure a décidé d'augmenter, dès 2020, les effectifs de ses deux structures d'enquêtes administratives. Toutefois, il faudra veiller à ce que la résorption de l'important stock de demandes ne se fasse pas au détriment de la qualité des enquêtes ;

- en troisième lieu, la durée moyenne d'enquête est comprise entre 1 et 12 mois ce qui, là encore, peut témoigner d'un manque de ressources humaines dans certains services d'enquête, ou de méthodes d'investigation plus ou moins approfondies.

Enfin, dans son rapport d'octobre 2019, l'inspection des services de renseignement (ISR) a souligné le caractère sommaire des enquêtes d'habilitation conduites par la DRPP. D'après l'ISR, ce service enquêteur ne procède qu'au criblage du candidat et de son conjoint, sans s'intéresser aux ascendants et aux descendants pourtant renseignés sur la notice individuelle 94 A.

*c) Des capacités techniques non partagées*

Sur le plan technique, la DRSD a acquis et développé des capacités d'aide à la décision (tris de données complexes) permettant de fluidifier les processus d'habilitation qui supportent le système d'information *Sophia*[1]. L'objectif ambitieux du service est de réduire la durée de l'enquête, qui passerait, dans certains cas, d'un mois[2] à une semaine pour accélérer les procédures de recrutement. Pour ce faire, un effort de numérisation complète des enquêtes administratives devra être entrepris afin de rendre les outils d'intelligence artificielle opérants et efficaces.

La DRSD souhaite disposer, dès 2022, de capacités d'interrogation (vérification des empreintes numériques en masse, *etc.*) pour procéder à des rétro-criblages systématiques des personnes déjà habilitées. Rendus possibles par la loi SILT[3], les rétro-criblages permettront d'assurer un suivi tout au long de l'habilitation, sans attendre son renouvellement ou une saisine par un officier de sécurité.

La DRSD réalise des investissements techniques opportuns pour lui permettre de remplir, de manière plus efficiente, l'une de ses missions essentielles. Une mutualisation, avec les autres services enquêteurs, des efforts financiers et des outils développés, pourrait utilement être étudiée.

*d) Un accès inégal aux fichiers*

Les services enquêteurs ont tous accès au fichier ACCReD[4], par le biais du service national des enquêtes administratives de sécurité (SNEAS), rattaché au directeur général de la police nationale.

En effet, aux termes de l'article 2 de son décret constitutif[5], le SNEAS *« réalise […] des enquêtes administratives destinées à vérifier, au regard de l'objectif de prévention du terrorisme et des atteintes à la sécurité et à l'ordre public et à la sûreté de l'État, que le comportement de personnes physiques ou morales n'est pas*

---

[1] *Synergie pour l'optimisation des procédures d'habilitation des industries et de l'administration.*

[2] *La durée d'enquête portant sur un agent du service est d'un mois, contre 101 jours pour une personne extérieure à la DRSD.*

[3] Cf. *article 11 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT). Les conditions dans lesquelles les personnes intéressées sont informées de cette consultation sont précisées par le décret n° 2018-141 du 27 février 2018 portant application de l'article L. 114-1 du code de la sécurité intérieure.*

[4] *Automatisation de la consultation centralisée de renseignements et de données.*

[5] Cf. *décret n° 2017-668 du 27 avril 2017 portant création d'un service à compétence nationale dénommé « service national des enquêtes administratives et de sécurité ».*

*incompatible avec l'autorisation d'accès à des sites sensibles ou l'exercice de missions ou fonctions sensibles dont elles sont titulaires ou auxquelles elles prétendent. Dans ce cadre, le service :*

*- consulte de manière directe ou indirecte des traitements de données à caractère personnel relatifs à la prévention du terrorisme ou des atteintes à la sécurité et à l'ordre publics et évalue, exploite et analyse les informations ainsi recueillies afin d'émettre un avis, le cas échéant par délégation du ministre de l'intérieur, sur la compatibilité entre le comportement de la personne et l'exercice des missions ou fonctions envisagées ou l'accès aux sites concernés au regard du risque d'atteinte à la sécurité et à l'ordre publics que celle-ci représente ;*

*- élabore une doctrine en matière d'enquêtes administratives pour homogénéiser les pratiques dans les domaines qui lui sont confiés ».*

Le décret n° 2019-1074 du 21 octobre 2019 a modifié le décret portant création de l'ACCReD afin d'autoriser la consultation automatique du N-SIS II (système d'information Schengen II), ainsi que la mise en relation avec les traitements de données à caractère personnel dénommés « SIREX » et « fichier de la DGSE »[1]. Par conséquent, le SNEAS peut aujourd'hui interroger les fichiers de souveraineté des quatre services enquêteurs[2] et plusieurs autres fichiers tels que le TAJ, le FPR et les FSPRT précités, ainsi que le fichier des enquêtes administratives liées à la sécurité publique (FEA), le fichier de prévention des atteintes à la sécurité publique (FPASP) et le fichier des objets et véhicules volés ou signalés (FOVeS).

La DRSD et la DGSE ont fait part de leur souhait d'accéder directement au FPR et au FSPRT. La DPR n'est pas favorable à une telle évolution dans la mesure où leur demande est satisfaite *via* le SNEAS. En revanche, si les délais de réponse sont trop longs, la DPR invite la CNRLT à prendre l'attache du SNEAS pour prévoir une gestion prioritaire de certains dossiers, en particulier ceux des agents de renseignement (ou des candidats au recrutement par les services).

Le SNEAS ne dispose cependant pas d'une consultation automatisée de l'ensemble des fichiers interrogés par les services enquêteurs. En la matière, l'accès aux fichiers de criblage est inégal :

- outre son propre fichier de souveraineté, la DRPP consultait jusqu'à présent ceux de la DGSI et de la DRSD, mais pas celui de la DGSE ;

- la DRPP peut savoir si un candidat a déjà fait l'objet d'une enquête d'habilitation conduite par la DGSI ou la DRSD, mais ne dispose pas de cette information émanant de la DGSE. La DRSD, elle, n'interroge que la DGSI ;

---

[1] *Il s'agit des fichiers de souveraineté de la DRSD et de la DGSE (contre-ingérence).*

[2] *« CRISTINA » pour la DGSI (centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux) et « GESTEREXT » pour la DRPP (gestion du terrorisme et des extrémismes violents).*

- à l'inverse, la DRPP dispose, pour ses enquêtes, de fichiers auxquels certains services enquêteurs ne semblent pas tous avoir accès, comme par exemple :

  - le fichier du bureau des actions de santé mentale (BASM),
  - le fichier de main courante informatisée des commissariats de police du lieu d'habitation du candidat,
  - les fichiers du système de circulation hiérarchisé des enregistrements opérationnels de la police sécurisés (CHEOPS)[1], même si certains d'entre eux sont déjà consultés par le SNEAS.

*e) Tracfin : une ressource précieuse mais inexploitée*

L'enquête administrative porte notamment sur la situation financière et patrimoniale des agents, sur la base de leur déclaration. En tant que de besoin, les services peuvent faire appel au concours de Tracfin. Toutefois, dans la pratique, l'examen de la situation patrimoniale s'opère principalement à partir de la déclaration du candidat à l'habilitation. Aucune coopération n'existe avec le service de Bercy pour détecter des changements de situation patrimoniale suspecte d'un agent ; Tracfin n'a ainsi jamais été sollicité par un service de renseignement pour une levée de doute à la suite d'indices témoignant manifestement d'un changement de situation patrimoniale.

Pourtant, un service enquêteur pourrait saisir Tracfin au titre de l'article L. 561-27 du code monétaire et financier, pour un examen de la situation patrimoniale d'un agent dans le cadre d'une enquête administrative (demande, renouvellement ou réexamen d'habilitation). Le service de renseignement financier pourrait alors consulter les applications de la direction générale des finances publiques sur les patrimoines connus, ainsi que plusieurs autres sources d'information (fichier des comptes bancaires – Ficoba, registre des bénéficiaires effectifs, associés et dirigeants d'entreprise, *etc.*) en exerçant son droit de communication auprès des professionnels assujettis.

Tracfin reçoit en effet des signalements des professionnels assujettis par le code monétaire et financier (CMF) à la lutte contre le blanchiment et le financement du terrorisme. Cependant, l'habilitation au secret de la défense nationale n'est pas connue des professions déclarantes (banques, assurances, notaires, *etc.*), ce qui empêche Tracfin de détecter des changements de situation ou de comportement financier des agents de renseignement à partir des déclarations de soupçons qu'il reçoit. Le service pourrait disposer de

[1] *Ce fichier regroupe le fichier TAJ (traitement d'antécédents judiciaires), le FPR (fichier des personnes recherchées), le FPASP (fichier de prévention des atteintes à la sécurité publique), le FEA (fichier des enquêtes administratives), le FNE (fichier national des étrangers) et AGRIPPA (application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes).*

cette information si une opération financière concernant un agent public entrait dans les critères énoncés par le CMF et entraînait une déclaration de soupçon ; le service pourrait alors diligenter une enquête. Le service ne peut aujourd'hui pas s'autosaisir ; une modification du cadre légal, défini par le code monétaire et financier, serait nécessaire pour accroître ses prérogatives.

*****

Si Tracfin avait été saisi d'une demande du service enquêteur de la DGSI, ou mieux, si Tracfin était associé aux enquêtes administratives réalisées par les services enquêteurs dans le cadre de l'habilitation de leurs propres agents, les vulnérabilités financières pourraient être détectées en recroisant les fichiers auxquels Tracfin a accès avec des bases de données sécurisées contenant l'identité des agents de chaque service de renseignement.

*f) L'harmonisation des procédures d'enquête : une démarche plus que nécessaire*

À la lumière des disparités précédemment évoquées, la délégation souhaite que le SGDSN réinvestisse sa mission de pilotage de la politique de secret, et s'assure que les enquêtes administratives soient toutes menées avec le même niveau de rigueur. Sans préjudice des compétences du SNEAS, les services enquêteurs devraient ainsi :

- conduire leurs enquêtes suivant un référentiel harmonisé, établi par le SGDSN ;

- disposer d'un même accès aux fichiers consultés dans le cadre des enquêtes administratives ;

- bénéficier d'outils technologiques performants, destinés à réduire le délai d'habilitation et permettre un réexamen automatisé des dossiers, c'est-à-dire sans attendre que des risques ne soient identifiés et remontés par la voie hiérarchique ; les outils développés par la DRSD sont très intéressants à cet égard.

Pour ce faire, le SGDSN devra renforcer les effectifs de sa sous-direction de la protection du secret de la défense nationale (PSD) pour lui permettre d'animer le réseau des HFDS et conduire des audits qualité dans le domaine des enquêtes d'habilitation. Le PSD dispose actuellement de ressources limitées pour assurer l'ensemble de ces missions (deux agents seulement, ce qui est à l'évidence insuffisant) ; l'homogénéisation des pratiques en ce domaine constitue pourtant un levier essentiel de maîtrise des risques.

En outre, la délégation parlementaire au renseignement invite le ministère de l'intérieur et le ministère des armées à procéder à une rationalisation du nombre de services enquêteurs placés sous leurs tutelles. En effet, la mutualisation des ressources humaines et techniques devrait prévenir l'apparition de nouveaux « goulots d'étranglement » pouvant

fragiliser le processus de recrutement des services, ou pouvant mettre en péril la protection du secret de la défense nationale en raison d'enquêtes trop sommaires.

Certains services sont réticents à cette idée, préférant garder en interne l'ensemble de la procédure d'habilitation. Par ailleurs, l'un d'entre eux juge la communication des listes d'agents ou de candidats beaucoup trop sensible ; pourtant, les identités de ces personnes sont, aujourd'hui, communiquées aux services concourant à des fins de criblage.

Enfin, la participation active de Tracfin évitera que les vulnérabilités financières ne constituent un « angle mort » pour les enquêtes administratives.

**Recommandation n° 30 : Rationnaliser le nombre de services enquêteurs placés respectivement auprès du ministère de l'intérieur et du ministère des armées, en mutualisant leurs ressources humaines et techniques. Ces services devront conduire leurs enquêtes suivant une méthodologie homogène, établie par le SGDSN, en y associant Tracfin. Les effectifs du SGDSN chargés du pilotage de la politique de protection du secret devront être augmentés afin, notamment, de conduire des audits qualité réguliers en ce domaine.**

### *B. LE RÉSULTAT DE L'ENQUÊTE ET SES CONSÉQUENCES*

#### 1. Le rôle central des hauts fonctionnaires de défense et de sécurité

Le service enquêteur qui instruit une demande d'habilitation, émet un avis de sécurité au terme d'une enquête administrative. L'avis qu'il exprime ne lie pas l'autorité d'habilitation qui dispose d'un pouvoir discrétionnaire en la matière.

Ainsi qu'en dispose l'article 11 de l'IGI 1300, ce sont les ministres qui prennent les décisions d'habilitation pour les niveaux « secret-défense » et « confidentiel-défense »[1]. Pour l'exercice de leurs responsabilités en matière de défense et de sécurité, ils sont assistés par un haut fonctionnaire de défense et de sécurité (HFDS)[2].

À titre d'exemple, au sein du ministère des armées, c'est le chef du cabinet militaire de la ministre qui occupe les fonctions de haut fonctionnaire correspondant de défense et de sécurité (HFCDS) depuis le 1er septembre 2018. Nommé par décret, il est placé sous l'autorité directe de la ministre et

[1] *Pour le niveau « très secret-défense », c'est le SGDSN qui prend les décisions d'habilitation par délégation du Premier ministre.*

[2] Cf. *articles R. 1143-1 et suivants du code de la défense.*

peut disposer d'un ou de plusieurs adjoints[1]. Ses compétences sont définies aux articles R. 1143-1 et suivants du code de la défense :

- conseiller la ministre pour toutes les questions relatives à la défense et aux situations d'urgence affectant la défense, la sécurité et la vie de la Nation ;

- animer et coordonner la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence.

Les officiers de sécurité sont, quant à eux, nommés par les directeurs de service en leur qualité d'« autorités qualifiées ».

*a) Le service enquêteur émet un avis de sécurité…*

Au regard des éventuelles vulnérabilités du candidat détectées lors de l'enquête, le service enquêteur communique à l'autorité d'habilitation un avis de sécurité qui peut être de trois types :

- « avis sans objection », lorsque l'instruction n'a révélé aucune vulnérabilité pouvant constituer un risque pour la sécurité des informations ou supports classifiés, ou celle du candidat ;

- « avis restrictif », lorsque le candidat présente certaines vulnérabilités pouvant constituer des risques directs ou indirects, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;

- « avis défavorable », lorsque des informations précises font apparaître que le candidat présente des vulnérabilités faisant peser sur le secret des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.

Si l'avis de sécurité est émis pour le niveau d'habilitation demandé, un avis « sans objection » est néanmoins valable pour le(s) niveau(x) inférieur(s). S'agissant des avis « restrictifs » ou « défavorables », le service enquêteur se prononce, au cas par cas, sur l'opportunité d'accorder une habilitation à un niveau inférieur à celui initialement sollicité.

Des avis défavorables peuvent être émis pour plusieurs motifs : liens avec l'étranger, manque de loyauté, comportement inapproprié ou manquement caractérisé aux règles de sécurité, comportement professionnel inadapté, environnement familial défavorable, *etc.*

Les avis restrictifs et défavorables font l'objet d'une fiche confidentielle motivant l'avis, transmise à l'autorité d'habilitation pour qu'elle puisse en prendre connaissance ; elle est toutefois conservée par le service enquêteur. Les informations non classifiées qu'elle contient peuvent être communiquées au candidat.

---

[1] *En l'espèce, son adjoint est le directeur de la protection des installations, moyens et activités de la défense (DPID).*

*b) …mais la décision revient à l'autorité d'habilitation*

La décision d'habiliter un personnel, ou de refuser de l'habiliter[1], est prononcée par l'autorité d'habilitation à la lumière des conclusions de l'enquête de sécurité.

L'autorité peut s'affranchir de l'avis émis par le service enquêteur et ainsi habiliter un candidat qui aurait reçu un avis défavorable. Elle peut également décider de n'accorder l'habilitation qu'après avoir pris des précautions particulières lorsque l'enquête a mis en évidence des éléments de vulnérabilité.

Le service enquêteur peut également prendre des mesures de mise en garde et de mise en éveil pour appeler l'autorité d'habilitation ou le candidat à une vigilance renforcée ; ces mesures particulières peuvent être cumulées :

- une mise en garde permet d'informer l'employeur – en l'espèce, l'officier de sécurité compétent – des vulnérabilités que présente l'agent (risques directs et indirects de sécurité), et de le sensibiliser à cet égard en lui adressant des recommandations. Une mise en garde peut conduire l'employeur à revoir la position de l'agent au sein de sa structure ;

- une mise en éveil permet d'informer un agent, à l'occasion de son affectation, de ses propres vulnérabilités (liens entretenus avec un pays étranger, environnement familial défavorable, difficultés financières, *etc.*) et de le sensibiliser à ce titre en lui donnant des consignes de discrétion et des recommandations. Le cas échéant, les informations portant sur ses restrictions d'emploi lui sont communiquées. Si l'entretien avec l'agent s'avère insatisfaisant aux yeux de l'officier de sécurité, ou s'il a permis de déceler d'autres vulnérabilités que celles identifiées par le service enquêteur, il lui est alors loisible de proposer à l'autorité d'habilitation de ne pas habiliter le candidat.

Si de telles mesures sont adoptées, un dialogue se met alors en place entre le service enquêteur, l'autorité d'emploi et son officier de sécurité : les mesures sont proposées au HFDS qui adresse sa décision à l'officier de sécurité du service concerné, pour leur mise en œuvre. Ces mesures font l'objet d'un document écrit, signé par l'employeur et, s'agissant de la mise en éveil, par l'agent concerné.

La décision d'habilitation n'est rendue qu'à l'issue de la procédure. Elle est prise par l'autorité d'habilitation et communiquée à l'officier de sécurité qui la notifie à son tour au candidat. L'intéressé signe un engagement de responsabilité par lequel il reconnaît avoir eu connaissance

---

[1] *En cas de refus d'habilitation, le candidat est informé de la décision prise à son endroit. Comme le précise l'article 26 de l'IGI 1300, un tel refus n'a pas à être motivé lorsqu'il repose sur des informations qui ont été classifiées (*cf. *article 6 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal).*

des obligations particulières imposées par l'accès aux informations et supports classifiés, ainsi que des sanctions prévues par le code pénal en cas d'inobservation, délibérée ou non, de la réglementation protégeant le secret de la défense nationale.

La durée d'habilitation est de 10 ans pour le niveau « confidentiel-défense », 7 ans pour le niveau « secret-défense » et 5 ans pour le niveau « très secret-défense ». Une réduction de ces durées n'est pas souhaitable en ce qu'elle engendrerait un accroissement de la charge de travail pesant sur les services enquêteurs, déjà très sollicités. En revanche, des contrôles inopinés, et le suivi scrupuleux des changements de situation des agents, sont souhaitables pour renforcer l'efficacité des enquêtes et la détection des vulnérabilités.

*c) Le dialogue entre le HFDS, son service enquêteur et le SGDSN mériterait d'être renforcé*

En tant qu'autorité d'habilitation, le HFDS décide donc, sur la proposition du service enquêteur, des restrictions à l'habilitation, à l'occasion d'une première habilitation ou d'un renouvellement. Toutefois, il n'est pas contraint d'informer le service enquêteur des suites réservées à ses avis restrictifs voire défavorables, ni des éventuelles mesures qui ont été adoptées à la suite d'une mise en garde.

Si la décision finale revient au HFDS, le service enquêteur doit rester en mesure d'établir une « cartographie des risques » et d'identifier les individus qui pourront, prioritairement, faire l'objet d'un réexamen inopiné de leur avis de sécurité. Le service enquêteur pourrait également mieux identifier les structures où les HFDS peinent à mettre en œuvre les mesures qu'il préconise.

Par ailleurs, dans les services de l'État (hors services de renseignement), les agents habilités ne sont pas toujours au fait des techniques d'approche dont ils pourraient faire l'objet par les services étrangers, ni même des devoirs qui leur incombent en matière de déclaration de changement de situation. Au Sénat, le secrétaire général, en sa qualité de HFDS de la Haute Assemblée, a donc mis en place des sessions de sensibilisation, dispensées par la DGSI, à destination des sénateurs mais également des fonctionnaires, qu'ils soient ou non habilités[1]. L'Assemblée nationale a également organisé des sessions similaires, au bénéfice des députés.

Les auditions conduites par la DPR sur le thème du renseignement d'intérêt économique ont mis en lumière une culture du secret assez inégale d'un ministère à l'autre. Des formations en la matière, ainsi qu'un fascicule

[1] *La participation à cette session était obligatoire pour les administrateurs et les administrateurs-adjoints de plusieurs commissions (affaires étrangères et défense, finances, affaires économiques).*

informant les personnels habilités de leurs devoirs, seraient donc les bienvenus. Chacun de ces personnels doit, en outre, identifier l'officier de sécurité dont il relève pour dialoguer avec lui en tant que de besoin (déclaration, question, *etc.*).

**Recommandation n° 31 : Informer les personnes habilitées des devoirs qui leur incombent à travers la remise d'un fascicule, concomitamment à leur décision d'habilitation.**

L'article 12 de l'IGI 1300 prévoit que les HFDS doivent adresser chaque année un rapport d'activités au SGDSN dans lequel sont notamment précisés :

- pour chaque niveau d'habilitation, le nombre de personnes habilitées dans l'année et le nombre d'habilitations en cours ;

- le nombre de lieux abritant des éléments couverts par le secret de la défense nationale ;

- le volume des documents classifiés ;

- l'état des catalogues des emplois[1] et des inventaires ;

- le nombre d'inspections ou de contrôles effectués ;

- les déficiences relevées dans le dispositif de protection du secret et les actions correctrices engagées ;

- les cas de compromission constatés et les actions de formation ou de sensibilisation menées.

Ce rapport mériterait de prendre la forme d'un document type, numérisé et enrichi de plusieurs éléments :

- les HFDS peuvent facilement connaître les changements intervenus dans la vie personnelle de leurs agents habilités en interrogeant leur direction des affaires financières et sociales. En effet, certains évènements (mariage/pacs/concubinage, naissance, déménagement, *etc.*) ouvrent des droits à congés ou à indemnités après déclaration à l'employeur. Le HFDS pourrait donc faire état de ces changements au SGDSN, et pourront, par la suite, être pris en compte par les services enquêteurs ;

- les modifications opérées dans le périmètre des postes figurant au catalogue des emplois, afin de déterminer si le niveau d'habilitation est toujours pertinent. Pour ce faire, les HFDS pourront recueillir les informations nécessaires auprès de la direction des ressources humaines et des agents concernés. L'état des catalogues des emplois et des inventaires devront être, chaque année, transmis au service enquêteur compétent afin qu'ils puissent appréhender les informations auxquelles les candidats auront

[1] *Liste des emplois ou fonctions nécessitant l'accès à des informations ou supports classifiés, pour chaque niveau de classification.*

accès, et émettre un avis de sécurité éclairé tenant compte des missions qui leurs sont confiées.

Ainsi, les services enquêteurs disposeront d'une cartographie complète, pour chaque service de l'État (ou entreprise de défense), des postes nécessitant une habilitation, des missions confiées à leur titulaires, de l'identité des agents qui y ont été affectés au cours de l'année écoulée et des changements intervenus dans leur situation personnelle ou professionnelle au cours de la même période.

**Recommandation n° 32 : Enrichir le rapport d'activités visé à l'article 12 de l'IGI 1300 afin de renforcer le dialogue entre les HFDS, le SGDSN et les services enquêteurs, et ainsi mieux identifier les risques liés aux habilitations.**

### 2. L'habilitation des agents des services de renseignement

Les dispositions de l'article L. 114-1 du code de la sécurité intérieure prévoient que les décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, concernant les emplois publics participant à l'exercice des missions de souveraineté de l'État, vont être précédées d'enquêtes administratives afin de vérifier que le comportement des personnes concernées n'est pas incompatible avec l'exercice des fonctions et des missions envisagées.

De même, il est possible de s'assurer que le comportement desdites personnes n'est pas devenu incompatible avec ces fonctions et missions. À l'issue d'une procédure contradictoire, l'administration peut décider l'affectation ou la mutation dans l'intérêt du service, voire, dans certains cas, procéder à une révocation des cadres.

*a) Une procédure similaire à celle des autres agents publics*

Dans les services de renseignement, tous les agents, y compris les cadres nommés en conseil des ministres, font l'objet d'une enquête de sécurité et doivent renseigner, à cet égard, une notice individuelle 94 A. L'affectation est souvent subordonnée à l'obtention d'une habilitation au niveau « secret-défense »[1].

Certains services accueillent des stagiaires qui travaillent, le cas échéant, en milieu cloisonné et sur des domaines non classifiés. À cette fin, ils font l'objet d'une enquête de sécurité *via* la notice 94 A, avec émission d'un avis de sécurité SRA (sous réserve d'audition). En cas de recrutement à

[1] *À titre d'exemple, en application de l'article 3 de l'arrêté du 9 mai 2014 relatif à la protection du secret de la défense nationale au sein de la DGSI, et sur décision du haut fonctionnaire de défense et de sécurité du ministère de l'intérieur, le personnel de la DGSI doit être habilité,* a minima*, au niveau « secret-défense ».*

l'issue du stage, ils sont soumis à la même enquête préalable de sécurité qu'un candidat extérieur au service.

Les agents des services de renseignement font l'objet d'une procédure d'habilitation semblable à celle précédemment décrite. En revanche, les décisions relatives au recrutement, aux avis de sécurité et aux habilitations « secret-défense » et « confidentiel-défense » sont prises, dans la plupart des services, par le directeur du service ou une personne qu'il désigne, et non par le HFDS[1]. Cette procédure est un gage d'efficacité puisque, comme le relève l'ISR, *« la plus-value du HFDS dans les procédures d'habilitation n'étant pas démontrée et compte tenu de la nécessité de raccourcir les délais de traitement des habilitations des services de renseignement, il pourrait être envisagé de prévoir une délégation de pouvoir aux autorités d'emploi »*.

À la DRSD par exemple, les mises en éveil ou en garde sont décidées par le directeur ou son adjoint. À la DRM, l'autorité d'habilitation est le directeur du service, par délégation du ministre des armées[2]. En pratique, le directeur du renseignement militaire a lui-même délégué sa signature à son adjoint[3].

Il faudra cependant veiller :

- à la séparation des fonctions pour éviter de confier ces responsabilités à l'officier de sécurité. Ce cumul de fonctions pourrait constituer une fragilité ;

- à formaliser cette délégation par un arrêté du ministre de tutelle. L'IGI 1300, dans sa future rédaction, devra prévoir cette possibilité.

**Recommandation n° 33 : Formaliser les délégations accordées par les ministres aux services de renseignement en matière d'habilitation de leurs agents, en évitant de cumuler les fonctions d'autorité d'habilitation et d'officier de sécurité. Cette faculté devra être prévue par l'IGI 1300 dans sa nouvelle rédaction.**

---

[1] *L'intervention du HFDS dans le processus d'habilitation des agents de renseignement n'est pas systématique. Certains services relevant du ministère de l'intérieur (DGSI, DRPP, SCRT) ne font pas transiter les notices d'habilitation au HFDS de leur ministère. Dès lors, la pertinence d'avoir un HFDS extérieur au service de renseignement interroge.*

[2] *L'article R. 2311-8-2 du code de la défense prévoit la possibilité pour le ministre des armées de déléguer son pouvoir en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale (*cf. *arrêté du 21 mars 2012).*

[3] *Pour les cas les plus sensibles, le signataire et l'autorité d'habilitation, qui conserve la responsabilité des décisions prises, se concertent.*

| Service | Officier de sécurité (OS) | Haut fonctionnaire de défense et de sécurité (HFDS) |
|---|---|---|
| **DGSE** | Directeur de cabinet adjoint en charge de la sécurité (DIRCAS) | Chef du cabinet militaire de la ministre des armées |
| **DRSD** | Officier de sécurité *(fonction à temps plein)* | |
| **DRM** | Chef du pôle sécurité-défense de la DRM[1] | |
| **DGSI** | Chef de l'inspection générale de la DGSI | Secrétaire général du ministère de l'intérieur |
| **DRPP** | Sous-directeur des supports opérationnels | |
| **SCRT** | Secrétaire général du SCRT | |
| **SDAO** | Commandant du groupement de sécurité et d'appui de la DGGN | |
| **DNRED** | Secrétaire général de la DNRED | Secrétaire général des ministères économiques et financiers |
| **Tracfin** | Responsable de la sécurité des systèmes d'information de Tracfin | |
| **SNRP** | L'adjoint au chef du SNRP | Secrétaire général du ministère de la justice |

*Source : Délégation parlementaire au renseignement, à partir des réponses des services au questionnaire écrit.*

*b) Un avis restrictif, voire défavorable, n'est pas rédhibitoire pour officier au sein d'un service de renseignement*

Certains agents exercent leurs fonctions au sein d'un service de renseignement malgré un avis restrictif ou défavorable. Par ailleurs,

[1] *À la DRM, la fonction d'officier de sécurité est assurée par le chef du pôle défense-sécurité du service, qui est placé sous l'autorité du chef d'état-major de la DRM. Ses missions sont les suivantes : diriger le bureau de protection du secret (gestion des habilitations,* etc.*) ; être l'interlocuteur de la DPID et du service enquêteur ; définir les règles et les consignes de sécurité à mettre en œuvre s'agissant des personnes et des installations, et en contrôler l'application ; contrôler l'accès aux zones protégées ; participer à l'instruction et à la sensibilisation du personnel.*

l'habilitation n'est pas toujours une condition *sine qua non* pour y travailler, comme le prouve le tableau ci-dessous.

Pourtant, la plupart des services affirme qu'un retrait d'habilitation[1] entraîne le départ de l'agent, qu'il soit motivé par une faute (compromission) ou non (mariage avec un ressortissant d'un pays sensible).

*Tableau* *****

(1) À la DGSE

Le décret relatif au statut des fonctionnaires de la DGSE dispose que nul ne peut être recruté ou maintenu dans ses fonctions s'il ne se voit pas conférer une habilitation spéciale de sécurité.

Les avis de sécurité sont validés par le chef du service de sécurité. Si des éléments défavorables au candidat ressortent au cours d'une enquête, des demandes de précisions peuvent être adressées. Au terme de ses investigations, le service enquêteur peut émettre des mises en garde et des mises en éveil. Le cas échéant, il en informe les directions d'emploi ainsi que les agents concernés *via* les officiers de sécurité présents dans toutes les directions. Un dialogue est alors instauré avec la direction d'emploi qui précise son souhait ou son refus de recruter la personne intéressée, au regard de l'avis de sécurité. Une mobilité peut être envisagée, au sein du service comme à l'extérieur.

En cas d'avis défavorable ou restrictif émis par le service de sécurité, une fiche de vulnérabilité est transmise à l'officier de sécurité de la DGSE, en l'espèce le directeur de cabinet adjoint chargé de la sécurité (DIRCAS), qui peut décider de redéfinir le périmètre de la restriction d'emploi pouvant donner lieu à une mobilité interne, voire de déroger à l'avis défavorable[2].

Malgré ses demandes, la DPR n'a pas eu accès au nombre d'agents du service exerçant leurs fonctions avec un avis restrictif ou défavorable.

(2) À la DRSD

Aucun personnel ne peut être recruté si sa demande d'habilitation recevait un avis défavorable. De même, un agent du service ne pourrait plus y exercer ses fonctions si un tel avis était émis lors de la révision de son avis de sécurité.

Le service a émis 130 avis restrictifs à l'encontre de ses propres agents :

---

[1] *Aux termes de l'article 31 de l'IGI 1300, les retraits d'habilitation n'ont pas à être motivés si les motifs sont classifiés. Les intéressés sont informés des voies de recours et des délais qui leurs sont ouverts pour contester les décisions prises à leur encontre.*

[2] *Les raisons de ces avis tiennent, le plus souvent, à une exposition à l'étranger.*

- 126 avis restrictifs ont été émis lors du recrutement (infractions mineures, attaches amicales et/ou familiales étrangères, cursus universitaire et/ou professionnel à l'étranger, forte visibilité numérique, *etc.*) ;

- 4 avis restrictifs ont été émis à la suite d'un changement de situation familiale.

Lors de la révision d'un avis sans objection à un avis restrictif, l'agent est, le plus souvent, maintenu dans ses fonctions. Il est en revanche systématiquement mis en éveil et son commandement de proximité peut être mis en garde si nécessaire.

(3) À la DRM

Les motivations des avis restrictifs émis par le service enquêteur, la DRSD, sont très hétérogènes. Toutefois, plusieurs motifs se dégagent :

- considérations de mobilité géographique : un candidat à l'habilitation a passé une année à l'étranger dans le cadre de sa scolarité, par exemple ;

- considérations de filiation : les parents du candidat possèdent une nationalité étrangère ;

- considérations matrimoniales : le candidat est marié à un ressortissant étranger ;

- considérations de droit commun : le candidat est connu pour consommation de stupéfiants.

L'évolution des profils des candidats à un poste au sein de la DRM conduit à une augmentation du nombre d'avis restrictifs émis par la DRSD[1]. En effet, de nombreux étudiants ont réalisé une année d'échange au cours de leur scolarité, parfois dans une zone sensible (Moyen-Orient, Russie, *etc.*) ou sont mariés avec une personne de nationalité étrangère. Pour prendre sa décision, le directeur du service tient compte de plusieurs éléments : les vulnérabilités que présentent le candidat, le vivier de recrutement et les besoins opérationnels à satisfaire.

Outre la mise en éveil de l'agent, l'autorité d'habilitation peut décider de l'habiliter pour une durée plus courte, comprise entre 6 mois et 2 ans[2]. Au terme de cette période, l'autorité d'habilitation peut décider de

---

[1] *Depuis 2017, le nombre de personnels civils sous contrat a augmenté au sein du service. Il s'agit notamment de personnes diplômées de l'enseignement supérieur dans le domaine des relations internationales, dont le cursus implique une année de césure à l'étranger. La DRM estime que 45 à 65 % des agents habilités sur le fondement d'un avis restrictif font l'objet d'un entretien préalable de mise en éveil ; en outre, la moitié de ces cas donnent lieu à un entretien de mise en garde du supérieur hiérarchique.*

[2] *Des durées d'habilitation contraires à celles prévues par l'IGI 1300 peuvent donc exister. C'est le cas à la DGSE, où les agents ne sont habilités que pour 5 ans.*

reconduire ou non l'habilitation, de manière temporaire ou pour la durée légale[1], suivant la manière de servir de l'agent mis à l'épreuve.

Lorsque l'avis restrictif d'un agent en poste donne lieu, après révision, à un avis défavorable, son habilitation lui est retirée et une mutation sur un poste ne nécessitant pas d'habilitation est envisagée. Deux cas ont été enregistrés depuis 2017.

L'habilitation de candidats ayant reçu un avis défavorable est toutefois possible si le recrutement répond à une nécessité opérationnelle impérieuse, par exemple lorsqu'il s'agit du recrutement d'un linguiste d'écoute compétent dans un dialecte rare. Ces cas sont néanmoins exceptionnels, et donnent lieu à un ajustement des modalités de travail pour réduire le risque identifié par le service enquêteur.

(4) À la DNRED

Les avis défavorables entraînent systématiquement un refus d'habilitation du service du haut fonctionnaire de défense et de sécurité, rattaché au secrétariat général des ministères économiques et financiers. La DNRED se conforme systématiquement à ses décisions.

*****

(5) À la DRPP

En cas d'avis restrictif, le service enquêteur n'est pas informé par le HFDS du ministère de l'intérieur des suites données à une enquête ; seuls les officiers de sécurité[2] concernés sont avisés des décisions prises. Les avis restrictifs donnent rarement lieu à une réaffectation interne, sauf en cas de lien avec un pays étranger sensible (bi-nationalité, ou nationalité d'un proche). En revanche, si un agent recevait un avis défavorable, il devrait quitter la DRPP puisque tous les postes sont soumis au niveau d'habilitation « secret-défense » ; l'agent serait alors remis à la disposition de la direction des ressources humaines de la préfecture de police pour une affectation au sein d'une autre direction.

27 agents du service exercent malgré un avis restrictif et une mise en éveil. Les motifs tiennent pour l'essentiel à des liens avec l'étranger (bi-nationalité, famille originaire et/ou résidant dans un pays sensible), à l'environnement familial (faits de droit commun) et à des vulnérabilités financières légères. Aucun avis restrictif n'a été émis pour une suspicion de radicalisation.

---

[1] *Pour mémoire, les habilitations sont prononcées pour 10 ans au niveau « confidentiel défense », pour 7 ans au niveau « secret défense » et pour 5 ans au niveau « très secret défense ».*

[2] *Le sous-directeur des supports opérationnels, son adjoint, le chef de section en charge des habilitations et son adjoint.*

(6) Au SNRP

*****

(7) Au SCRT

Toute mutation d'un agent habilité à son entrée au SCRT, entraîne la suppression de son habilitation. Si ses nouvelles fonctions nécessitent une habilitation, l'agent doit soumettre une nouvelle demande.

3 agents exercent actuellement leurs fonctions au SCRT malgré un avis défavorable. Ils ont été affectés au sein des services supports.

Le SCRT n'est en revanche pas au courant des avis restrictifs émis à l'encontre des agents affectés dans les services territoriaux, leurs habilitations étant gérées localement par les préfectures, après une procédure instruite par la DGSI.

### 3. Le suivi des personnes habilitées

En application de l'article 26 de l'IGI 1300 et, le cas échéant, des obligations de transparence imposées par le statut spécifique, l'agent est tenu d'informer le service enquêteur de tout changement de sa situation personnelle (nouvelle adresse, relation intime durable en particulier si elle implique un ressortissant étranger[1], divorce, naissance, *etc.*) ou liée à sa sécurité. Ces nouveaux éléments doivent justifier un réexamen de l'avis de sécurité de l'agent.

Les problèmes de comportement d'un agent, dans le cadre professionnel ou extraprofessionnel peuvent également engendrer un réexamen de sa situation. Dans le cas de Mickaël Harpon, la plainte déposée pour violences conjugales par sa concubine aurait dû constituer un indice d'une vulnérabilité comportementale et déclencher un réexamen de son habilitation, mais ce ne fut pas le cas. Pis, à l'occasion du renouvellement de son habilitation, il n'a fait l'objet que d'une mise en éveil alors qu'il aurait pu, au regard de ces faits de violence, recevoir un avis restrictif avec une mise en garde de son employeur.

En cas de concrétisation d'une vulnérabilité, l'agent doit en informer son service d'emploi et le service enquêteur ; le dossier est alors réexaminé. À cette occasion, l'habilitation peut lui être retirée en cours de validité ou à la faveur d'un réexamen de sa situation. L'article 31 de l'IGI 1300 précise à ce

[1] *L'article 26 précité dispose que tout agent* « est tenu d'informer au plus vite, pendant toute la durée de son habilitation, l'officier de sécurité dont il relève de tout changement affectant sa vie personnelle (mariage, divorce, pacs, établissement ou rupture d'une vie commune…), professionnelle ou son lieu de résidence. Il lui est signifié qu'il devra l'informer de toute relation suivie et fréquente, dépassant le strict cadre professionnel, avec un ou plusieurs ressortissants étrangers ».

titre que *« la décision d'habilitation ne confère pas à son bénéficiaire de droit acquis à son maintien »*.

Malgré les demandes de la DPR, les services ne lui ont pas transmis de statistiques sur les réexamens de dossier en cours d'habilitation, invoquant des raisons de sécurité et de protection (DGSE) ou l'absence d'outils adaptés (DRSD, DRM). La DPR ne peut que le regretter.

(1) À la DGSE

Des revues d'effectifs sont réalisées chaque année avec les chefs de service et les officiers de sécurité des directions d'emploi. Des investigations et des vérifications sont alors réalisées, d'initiative ou sur la base de signalements, même anodins, faits par la hiérarchie, les officiers de sécurité ou tout autre personne. Tous les agents de la DGSE ont un accès direct et protégé au service de sécurité pour lui transmettre toute information le concernant.

Le service de sécurité peut adresser des questions complémentaires à l'agent ou le convoquer à un nouvel entretien de sécurité (« levée de doute ») afin d'évaluer les changements intervenus dans sa situation personnelle et les risques qu'ils supposent au regard des missions confiées. *****. Un tel réexamen peut aboutir à la révision de l'avis de sécurité voire, dans de rares cas, à l'éviction de l'agent concerné.

(2) À la DRM

La DRM indique que le mariage, le pacs et le concubinage nécessitent un réexamen de l'habilitation sauf si l'avis de sécurité a été émis depuis moins de 3 ans et que le conjoint/pacsé/concubin est de nationalité française exclusivement et qu'il a déjà été déclaré sur la notice 94 A.

(3) À la DRPP

Un simple changement d'adresse ou une naissance sont simplement enregistrés pour une mise à jour du dossier, sauf s'ils sont susceptibles de révéler une vulnérabilité, par exemple la naissance d'un enfant sans qu'un conjoint ou un compagnon n'ait été déclaré. Un réexamen fait l'objet d'une nouvelle notice de révision, transmise par l'officier de sécurité, sur initiative.

En 2019, au moins 6 révisions ont été réalisées pour des agents de la DRPP, principalement pour des changements de situation. Une demande a été adressée dans le cadre d'une mobilité interne et a abouti à un retrait d'habilitation.

Toutefois, la DRPP relève que les changements de statut matrimonial étaient auparavant peu signalés. D'après elle, les officiers de sécurité, qui remplissent d'autres missions, ne consacrent qu'une infime part de leur temps de travail (estimée à 2 %) à la gestion des habilitations.

Aucun contrôle aléatoire n'est opéré pour une habilitation en cours de validité ; les enquêtes d'habilitation diligentées avant la réforme interne de 2017 font toutefois l'objet d'une révision. En outre, lorsque des informations particulières sur une personne habilitée sont portées à sa connaissance, le service procède à des vérifications pouvant donner lieu à des enquêtes administratives, déclenchées par l'autorité hiérarchique.

(4) Au SCRT

Au SCRT, les changements de situation des agents (situation familiale notamment) sont renseignés au sein du système d'information de gestion des ressources humaines, mais ne sont pas transmises au service enquêteur. Le signalement à l'autorité d'habilitation n'a lieu qu'en cas de radicalisation religieuse ou politique[1], ou de compromission[2] ; elles entraînent alors un réexamen de l'avis de sécurité.

L'absence de remontée d'informations relatives aux changements de situation personnelle interpelle car elles empêchent les services enquêteurs (DGSI ou DDSI – directions départementales de la sécurité intérieure) de réexaminer le dossier des intéressés. La communication de ces informations constitue pourtant une exigence posée par l'IGI 1300.

**Recommandation n° 34 : Notifier aux agents des services du second cercle leur obligation en matière de déclaration de changement de situation personnelle auprès de l'officier de sécurité dont ils relèvent. L'officier devra quant à lui saisir l'autorité d'habilitation de ces nouvelles informations (notice 94 A révisée), qui les transmettra au service enquêteur compétent en vue de l'émission d'un nouvel avis de sécurité.**

(5) À la SDAO

*****

### *C. UN DISPOSITIF À MODERNISER ET À HOMOGÉNÉISER*

En vertu de l'article 21 de la Constitution, le Premier ministre est responsable de la défense nationale. Sous son autorité, le secrétariat général de la défense et de la sécurité nationale (SGDSN) définit et coordonne, sur le plan interministériel, la politique de sécurité en matière de protection du secret de la défense nationale.

Il revient donc au SGDSN d'entreprendre le chantier de modernisation et d'harmonisation des procédures d'habilitation, comme le recommande la DPR. Pour ce faire, plusieurs axes de travail se dégagent.

---

[1] *Il s'agit d'un signalement hiérarchique. L'inspection générale de la police nationale traite des affaires au sein d'une cellule dédiée ou oriente le suivi vers un service partenaire.*

[2] *La compromission est un délit. L'enquête judiciaire est réalisée par la DGSI, sous l'autorité du procureur de la République.*

### 1. Sur le plan réglementaire

La révision de l'IGI 1300, entamée depuis plusieurs années, offre l'opportunité de prendre en considération les conclusions du rapport de l'ISR et les recommandations de la DPR.

Pour ce qui concerne l'autorité d'habilitation, l'IGI 1300 devra prévoir, pour les services de renseignement, la délégation du ministre de tutelle aux directions d'emploi placées sous son autorité.

Le SGDSN devra veiller à l'adoption, par chaque ministère, d'une instruction particulière définissant les conditions d'emploi des niveaux de classification « secret-défense » et « confidentiel-défense », ainsi que les informations qui doivent être classifiées au niveau « très secret-défense ». Par ailleurs, il interdira aux employeurs d'affecter un candidat sur un poste nécessitant la consultation d'informations classifiées avant qu'il n'ait reçu l'avis de sécurité qui le concerne, ou qu'il n'ait fait l'objet d'un pré-criblage (empreinte numérique) et d'un entretien préalable de sécurité.

La notice 94 A devra évoluer pour comporter des informations utiles aux candidats (engagements liés à l'habilitation) et aux services enquêteurs (date souhaitée de prise de fonctions afin de pouvoir prioriser les dossiers à traiter). Elle devra surtout permettre d'élargir le criblage, en intégrant une nouvelle rubrique sur l'entourage proche du candidat (précédent conjoint, frères et sœurs et leurs conjoints).

### 2. Sur le plan procédural

L'IGI 1300 devra consacrer la numérisation de toute la procédure de demande d'habilitation à des fins d'archivage des informations relatives aux candidats et de bon fonctionnement des outils d'intelligence artificielle utilisés dans le cadre de l'enquête administrative.

Les séances de sensibilisation aux risques de compromission, ainsi qu'aux menaces d'investigations ou d'approches par des individus ou des organisations étrangères, seront rendues obligatoires. Par souci d'économies, ces séances pourront prendre la forme de MOOCs.

Le SGDSN devra également favoriser l'échange de bonnes pratiques entre les services enquêteurs et mutualiser – ou faire partager – les outils d'aide à la décision (rétro-criblages, *etc.*). À terme, des contrôles inopinés devront être rendus possibles, soit par rétro-criblages automatisés, soit au regard de la cartographie des risques de chaque structure.

Le secrétariat général devra également s'assurer que les services disposent d'un égal accès aux fichiers nécessaires aux enquêtes administratives, et mettre en place un « audit qualité » transversal pour harmoniser les méthodes d'enquêtes.

Les enquêtes administratives portant sur les enquêteurs eux-mêmes ne devront pas être réalisés au sein de la même entité, comme c'est le cas à la DRPP[1]. Bien que les investigations soient identiques à celles réalisées pour les autres personnels, le fait que les contrôleurs et les contrôlés appartiennent à la même unité peut constituer un risque.

**Recommandation n° 35 : Engager l'actualisation du cadre réglementaire relatif à la protection du secret de la défense nationale, avec pour objectif d'homogénéiser les procédures qui l'entourent, en particulier en matière d'enquêtes administratives.**

## II. LA SÉCURITÉ ET LA SÛRETÉ DES SERVICES DE RENSEIGNEMENT

L'IGI 1300 traite également de la protection physique et informatique du secret de la défense nationale :

- le titre IV concerne la protection des lieux (zones protégées et réservées, salles de travail et de conférence, accès des personnes non qualifiées et des magistrats aux lieux abritant des secrets de la défense nationale) ;

- le titre V concerne les mesures de sécurité relatives aux systèmes d'information (organisation des responsabilités et protection des systèmes d'information). Ses dispositions sont complétées par des instructions spécifiques d'application émises par l'agence nationale de sécurité des systèmes d'information (ANSSI) qui relève du SGDSN.

### *A. LA DÉTECTION DES SIGNAUX FAIBLES, UN ENJEU ESSENTIEL*

La prévention de la radicalisation est consubstantielle des services de renseignement dans la mesure où elle constitue l'une de leurs missions à l'échelle nationale, et que ce risque doit également être détecté en leur sein. L'enjeu réside dans leur capacité à anticiper les risques : la détection constitue la première étape d'un processus destiné à écarter les agents présentant un comportement à risque ; viennent ensuite le signalement puis l'action d'entrave.

La procédure d'habilitation et l'évaluation de la manière de servir des agents doivent constituer des premiers moyens de contrôle robustes. Toutefois, ils ne sont pas suffisants et doivent être complétés par une procédure de détection des signes de radicalisation. L'efficacité de ce dispositif repose sur plusieurs socles :

---

[1] *Il est toutefois à noter que l'ensemble des enquêteurs sont soumis à un entretien de sécurité à la DGSI.*

- la qualité de la formation des agents qui doivent être en mesure de déceler les bons signaux chez les personnes radicalisées ou en voie de l'être. Leur parole doit en outre être facilitée, voire décomplexée, même si elle peut porter préjudice aux collègues visés par les signalements ;

- la qualité de la remontée d'informations grâce à une approche ascendante, qui part des agents vers leur encadrement de proximité. La forme écrite peut générer une autocensure chez celui qui détecte les premiers signes ; en revanche, elle doit être privilégiée par sa hiérarchie de proximité afin de nourrir le dossier des individus visés par les signalements. La chaîne hiérarchique doit contrôler ce dispositif d'informations et mettre en œuvre les investigations nécessaires, en toute impartialité, pour confirmer ou infirmer les informations recueillies, sans éveiller de soupçon ;

- la qualité du contrôle externe. Afin de mettre à jour d'éventuels dysfonctionnements et les corriger, un audit de certains services peut s'avérer utile.

Dans l'affaire Harpon, certaines informations n'ont pas été remontées à la hiérarchie, peut-être en raison du handicap de l'intéressé qui suscitait une certaine mansuétude de la part de ses collègues. En outre, la plainte déposée par son épouse pour violences conjugales n'a pas été considérée comme un motif de nature à remettre en question son habilitation (*cf.* I. B. 3.).

### 1. La formation en ce domaine doit être continue

Tous les services indiquent que leurs agents sont formés ou sensibilisés aux enjeux liés à la radicalisation dans le cadre de leur formation initiale ou de leur stage d'accueil. En revanche, ces formations ne font pas toujours l'objet d'un module complémentaire au cours de leur carrière administrative.

Il est essentiel que les agents soient régulièrement sensibilisés pour actualiser leurs connaissances et garder à l'esprit les consignes et les procédures en vigueur dans leur service. Ces modules doivent revêtir un caractère obligatoire et être conçus à partir des mêmes grilles d'analyse afin qu'une culture commune puisse se diffuser, ce qui n'est pas le cas aujourd'hui.

L'académie du renseignement a notamment pour missions de concevoir et de mettre en œuvre des activités de formation initiale et continue au profit du personnel des services de renseignement, et de favoriser la coopération entre ces services en matière de formation. À ce titre, elle pourrait être chargée de concevoir, avec l'appui des services compétents, des outils de formation à la détection des signes de radicalisation sur la base de référentiels communs. Ces outils seront harmonisés, et adaptés à la connaissance des agents sur le sujet (formation initiale, ou modules

complémentaires) ainsi qu'à leur positionnement hiérarchique (afin d'adapter leurs réflexes), pour que chaque niveau de responsabilités connaisse son rôle, ses droits et ses devoirs en la matière.

**Recommandation n° 36 : Confier à l'académie du renseignement la conception d'outils de formation et de sensibilisation aux enjeux de lutte contre la radicalisation, en lien avec les services compétents.**

### 2. Les dispositifs de remontée d'informations doivent permettre un signalement rapide et étayé

Chaque service a mis en place un système de remontée d'informations propre à son organisation et aux risques qu'il a pu identifier, mais peu d'entre eux ont été éprouvés.

Les dispositifs sont disparates suivant le ministère de tutelle ou la taille du service. Dès lors, un audit serait utile pour vérifier la mise en œuvre effective de ces dispositifs et les tester afin d'en repérer les éventuels dysfonctionnements.

**Recommandation n° 37 : Mettre en place un audit externe des dispositifs de détection et de lutte contre la radicalisation mis en place dans les services de renseignement.**

*a) À la DGSE*

En 2018, le service a créé un bureau en charge de l'anticipation qui agit sur la base des signaux faibles qui lui sont remontés soit par le service de sécurité, soit par d'autres canaux (officiers de sécurité, *etc.*). Ces signaux faibles peuvent notamment porter sur des risques de radicalisation.

La radicalisation d'un agent fait l'objet d'un signalement à la DGSI et à la DRSD. Le service peut en outre prendre différentes mesures pour se séparer d'un élément radicalisé : retrait d'habilitation, mutation, non renouvellement de contrat de travail ou engagement d'une procédure de licenciement.

Les suspicions de radicalisation demeurent toutefois très rares à la DGSE ; à ce jour, aucun retrait n'a été prononcé pour ce motif dans ce service.

*b) À la DRSD*

Si le comportement d'un agent du service éveillait des soupçons, un compte rendu devrait alors être adressé à l'officier de sécurité. Celui-ci informerait l'adjoint du directeur des éléments constatés qui pourrait décider, à la lumière de ces éléments, de diligenter une enquête interne, pilotée par l'officier de sécurité avec l'aide du chef du BEPS.

Le cas échéant, la DRSD enquêterait elle-même sur les faits portés à sa connaissance, et assurerait le suivi des agents radicalisés dans sa sphère de compétence. Ces agents seraient signalés aux services partenaires lors des groupes d'évaluation départementaux (GED) et éventuellement inscrits, après évaluation, au fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT). La cellule Allat et l'EMaP (état-major permanent) seraient également alertés, notamment pour assurer la continuité du suivi de l'agent qui quitterait la DRSD.

La DRSD n'a jamais été confrontée à un cas de radicalisation en son sein. Le service n'a d'ailleurs pas sollicité la réunion d'une commission de radiation[1]. Néanmoins, des mesures sont prévues pour écarter un agent radicalisé ; elles sont identiques à celles mises en place au ministère des armées, à savoir :

- entraves « administratives » comme la mobilité interne vers un poste non sensible, la mutation, la contribution à une sanction, la révision ou la perte d'habilitation, le non-renouvellement du contrat de travail, ou encore le déclenchement d'un conseil d'enquête en vue de rompre le contrat de travail ;

- entraves policières et judiciaires en lien avec les services partenaires (visite domiciliaire, mesure individuelle de contrôle administratif et de surveillance – MICAS, *etc.*).

La radicalisation islamiste au sein des armées est en effet marginale comme le souligne un rapport du centre d'analyse du terrorisme (CAT) de décembre 2019. Néanmoins, selon ce même rapport, une vingtaine de militaires français ont rejoint des organisations terroristes depuis 2012, ou sont eux-mêmes impliqués dans des projets d'attentats. Ces statistiques doivent appellent une vigilance continue de l'encadrement militaire.

*c) À la DRM*

Les procédures de détection des signes de radicalisation sont identiques à celles des armées : le commandement de proximité est chargé de faire remonter les signaux faibles à l'officier de sécurité de son entité, et les éléments d'alerte sont rapportés à la DRSD afin qu'elle puisse engager les investigations qu'elle estime nécessaires.

Depuis 2010, trois agents ont fait l'objet d'une attention particulière motivée par une aggravation de leur vulnérabilité à l'Islam radical[2], et d'un retrait d'habilitation ayant entraîné leur départ du service.

---

[1] *Dispositions prévues au IV de l'article L. 114-1 du code de la sécurité intérieure et à l'article L. 4139-15-1 du code de la défense, portant sur l'incompatibilité du comportement des agents publics avec leurs fonctions lorsqu'ils occupent un emploi participant à l'exercice de missions de souveraineté de l'État ou relevant du domaine de la sécurité et de la défense.*

[2] *Évolution de leur sensibilité religieuse ou de celle de leur entourage.*

Afin de ne pas éveiller l'attention des personnels à risque, la DRSD peut solliciter leur maintien en fonctions le temps de l'enquête. Une fois les agents mutés, la DRSD continue d'assurer leur suivi s'ils restent employés au sein de la « sphère défense », ou transmet leur dossier aux services de renseignement relevant du ministère de l'intérieur.

*d) À la DGSI*

La remontée d'informations s'opère oralement, en dehors de toute chaîne hiérarchique afin d'éviter toute forme de censure. Pour ce faire, le service central chargé des enquêtes de contrôle s'appuie sur les chefs de services, ses correspondants locaux implantés sur tout le territoire français (y compris dans les collectivités ultramarines), les psychologues et tout agent sensibilisé au risque de radicalisation. Des enquêtes de sécurité peuvent être diligentées ; menées à charge et à décharge, elles visent à déterminer si l'agent concerné par le signalement présente des vulnérabilités susceptibles de conduire au retrait de son habilitation, ou si son comportement peut mettre en péril sa sécurité ou celle de ses collègues.

La DGSI rapporte que 12 enquêtes de ce type ont été conduites depuis 2014 et ont conduit à 3 retraits d'habilitation[1]. En outre, une douzaine d'enquêtes sont en cours pour réaliser une « levée de doute ».

*e) À la DRPP*

L'encadrement est chargé de sensibiliser les effectifs placés sous leur autorité à ces enjeux et de faire remonter tout signalement au directeur. Le psychologue du service peut également porter l'alerte.

Les signalements peuvent être opérés par tout moyen ; la voie hiérarchique et l'écrit sont toutefois encouragés afin de formaliser les signalements et d'en conserver la trace. Les agents peuvent également contacter le centre national d'assistance et de prévention de la radicalisation[2] (CNAPR), en prenant le soin de préciser qu'ils sont soumis au respect du secret de la défense nationale.

Les agents relevant du préfet de police soupçonnés de radicalisation sont suivis par un comité placé sous l'autorité de son directeur de cabinet. Les signalements sont donc centralisés auprès de l'IGPN qui se réunit tous les mois en format « groupe d'étude central » pour décider des suites à donner.

Le directeur du service ou son adjoint peuvent diligenter une enquête administrative interne en cas de doute sur le comportement d'un agent. La section en charge des habilitations peut également s'autosaisir. À ce titre, elle peut solliciter le concours de services partenaires.

---

[1] *Toutefois, aucun de ces retraits d'habilitation n'a été décidé pour le seul motif de radicalisation.*
[2] *Plateforme téléphonique nationale.*

Le directeur du service peut également saisir, sous couvert du préfet de police, l'inspection générale de la police nationale (IGPN), soit à la lumière des résultats de l'enquête, soit dès la prise de connaissance des faits reprochés à l'agent suivant leur caractérisation et leur gravité. Une saisine des autorités judiciaires en vertu de l'article 40 du code de procédure pénale est également possible. Les agents appelés à témoigner dans le cadre d'une procédure judiciaire sont protégés par l'article L. 656-1 du code de procédure pénale (anonymat).

En 2019, un retrait d'habilitation pour cause de radicalisation présumée a été prononcé et l'IGPN a été alertée de ce cas. Compte tenu des impératifs de sécurité et de confidentialité, le service s'est séparé de l'agent radicalisé en lui retirant son habilitation[1] et en le remettant à la disposition de la direction des ressources humaines de la préfecture de police qui détermine alors les suites administratives à donner (réaffectation, sanctions disciplinaires, *etc.*).

*f) Au SCRT*

Un seul signalement a été rapporté par l'encadrement de proximité. Une évaluation a été effectuée par la hiérarchie, avec le soutien du SCRT, et s'est avérée négative ; le signalement était vraisemblablement mu par des difficultés relationnelles.

Une procédure spécifique a été mise en place pour la gestion des signalements portés à la connaissance du SCRT. À cet égard, une circulaire de la direction générale de la police nationale de 2015 a confié à l'IGPN la centralisation des signalements. De nouvelles instructions sont en cours de rédaction.

*g) À la SDAO*

*****

*h) À la DNRED*

*****

*i) À Tracfin*

Les doutes qui entourent le comportement d'un agent sont remontés auprès d'une entité hiérarchique qui en informe l'officier de sécurité, par ailleurs référent « lutte contre la radicalisation ». La taille du service, qui compte quelque 170 agents au total, permet une remontée d'informations rapide. *****. Un comportement anormal, ou l'impossibilité d'effectuer une levée de doute, conduirait à saisir le directeur du service qui saisirait à son tour le HFDS.

[1] *Il n'existe pas de procédure de retrait temporaire d'habilitation.*

Si nécessaire, l'agent peut être suspendu (accès informatiques, carte d'accès aux locaux) dans l'attente des consignes du HFDS sur la conduite à tenir et de sa décision quant à l'habilitation de l'intéressé.

*j) Au SNRP*

Les critères de détection des signes de radicalisation sont basés sur ceux employés par les agents de la direction de l'administration pénitentiaire à l'endroit des personnes détenues. Le service s'appuie également sur son expérience pour identifier des critères additionnels.

Si un agent de l'administration pénitentiaire détecte des signes de radicalisation chez l'un de ses collègues, il est tenu de remplir une fiche de signalement type, sous couvert, le cas échéant, de son chef d'établissement (ou de service) et de son directeur interrégional qui l'envoie à une adresse électronique dédiée. *****.

*****

La loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice octroie au renseignement pénitentiaire de nouvelles possibilités d'emploi de techniques de recueil de renseignement, dont la mise en œuvre n'est plus limitée aux seules personnes détenues mais concerne également les intervenants en détention, pour la finalité de sécurité pénitentiaire.

Le décret n° 2019-1503 du 30 décembre 2019 modifiant diverses dispositions relatives au renseignement pénitentiaire a parachevé l'arsenal juridique dont dispose le SNRP en matière de techniques de renseignement. Il étend notamment ces techniques à l'encontre des intervenants en détention, dans l'enceinte des établissements pénitentiaires, pour les finalités de prévention du terrorisme et de lutte contre la criminalité organisée.

### *B. LA PROTECTION PHYSIQUE DES EMPRISES*

La plupart des emprises des services de renseignement sont classées en « zones protégées » telles que définies à l'article 73 de l'IGI 1300 et à l'article 413-7 du code pénal. Elles sont toutes équipées de systèmes de contrôle centralisé (lecteur de badges, vidéosurveillance) pour filtrer les visiteurs extérieurs et tracer les entrées et les sorties de leurs agents.

*****

### *C. LA SÉCURITÉ INTERNE DES SYSTÈMES D'INFORMATION*

La sécurité des systèmes d'information concerne tant les directions informatiques pour la sécurité logique, que les directions métiers pour la

définition des droits d'accès aux informations, et les responsables de la sécurité physique des locaux.

Placée sous l'autorité du HFDS ou d'une structure de sécurité équivalente, la chaîne fonctionnelle de sécurité des systèmes d'information est chargée de prescrire, d'appliquer et de contrôler les mesures de sécurité nécessaires. Ces mesures doivent être proportionnées aux enjeux des informations et des systèmes concernés et doivent avoir pour objectif la disponibilité, la confidentialité et l'intégrité de ces informations.

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est responsable de la sécurité des systèmes d'information pour une structure donnée (service, direction d'un ministère, organisme ou établissement relevant d'un ministère, *etc.*). Elle est désignée par le ministre et ne peut déléguer sa responsabilité. Elle peut néanmoins se faire assister par un ou plusieurs agents, responsables ou officiers de sécurité des systèmes d'information (ASSI, RSSI ou OSSI) qui assurent principalement des fonctions opérationnelles en ce domaine.

Après une évaluation des risques, l'autorité responsable procède à l'homologation du système d'information qui certifie que sa protection, et celle des informations qu'il contient, sont assurées au niveau requis :

- pour le niveau « très secret-défense », l'autorité d'homologation est le SGDSN ;

- pour les niveaux inférieurs, l'autorité d'homologation est désignée par l'autorité qualifiée. Il s'agit en principe de l'autorité chargée de l'emploi du système d'information, mais l'autorité qualifiée peut se désigner elle-même.

L'autorité d'homologation met en place une commission *ad hoc* à laquelle l'ANSSI peut participer en sa qualité d'autorité nationale en matière de sécurité des systèmes d'information.

### 1. À la DGSE

Afin d'assurer la protection des données informatiques sensibles, les agents bénéficient de droits d'accès définis suivant les fonctions qu'ils occupent et leur besoin d'en connaître. Chaque agent accède au système d'information du service à l'aide d'une carte à puce individuelle, ce qui permet à la direction technique de tracer les actions qu'il effectue.

S'agissant des prestataires du service, ils font l'objet d'une enquête administrative préalable, suivant le type de prestations à réaliser. Leurs prestations peuvent nécessiter des interventions sur site ou la manipulation d'informations classifiées (administration de systèmes industriels et techniques classifiés, par exemple) ; le cas échéant, des postes informatiques dédiés sont mis à leur disposition, et ce uniquement dans l'enceinte du

service. En outre, l'introduction de supports informatiques sur site doit être préalablement déclarée au service de sécurité.

Compte tenu de la sensibilité de leurs fonctions, les administrateurs réseaux font l'objet d'une attention accrue. À l'issue de l'enquête d'habilitation, ils signent un engagement de responsabilité et un stage de sensibilisation leur est dispensé. Dans l'exercice de leurs missions, leurs actions sont particulièrement surveillées grâce à une « gestion de comptes à privilèges » traçables par rebonds[1].

Des outils ont été développés en interne pour détecter l'extraction massive de données. Par ailleurs, l'ANSSI participe à la sécurité des systèmes d'information de la DGSE grâce à la mise à disposition, depuis l'été 2019, de sondes sur les accès extérieurs du réseau. L'exploitation et le traitement des alertes restent toutefois de la compétence du service.

### 2. À la DRSD

La plupart des données informatiques sont classifiées au niveau « confidentiel-défense » et stockées au sein du réseau et du socle applicatif *IntraRSD*, support de *Sirex*, fichier souverain de la DRSD, qui gère le besoin d'en connaître dans l'accès aux informations relatives aux enquêtes administratives. Les données classifiées au niveau « secret-défense » sont quant à elles stockées au sein du réseau *Troie*.

Ces systèmes bénéficient de protections contre l'accès et la fuite de données ; l'export de données est ainsi tracé par un système dédié dénommé *Cerbère*, et la fuite massive de données est surveillée par le système de contrôle du bureau de surveillance. À terme, le service prévoit la mise en place d'une infrastructure de gestion de clés.

Le socle applicatif du service *IntraRSD* est isolé et protégé par la DRSD elle-même, avec des chiffreurs *Crypsis* administrés par le service. Les systèmes sont déployés dans toutes les emprises de la DRSD, y compris à l'étranger et en opérations extérieures. Les administrateurs réseaux sont habilités à un niveau supérieur à celui de l'exploitation.

### 3. À la DRM

Les mesures adoptées par le service sont celles du ministère des armées. Elles assurent et réglementent un cloisonnement logique et/ou physique, la gestion des droits d'accès, l'authentification forte[2], l'édiction des

---

[1] *Le rebond est un serveur à l'accès limité, défini comme point de passage obligatoire. Toutes les requêtes (flux entrants et sortants) sont archivées.*

[2] *Utilisation d'au moins deux facteurs d'authentification de nature distincte (par exemple un login et un mot de passe, ainsi qu'une carte à puce ou un élément biométrique) afin de compliquer la tâche d'un éventuel attaquant.*

décisions d'accès, le verrouillage des ports, le filtrage des pièces jointes, la visualisation distante des données sans rapatriement sur le disque, *etc.*

Le système de « double-clés » est fréquemment utilisé. À titre d'illustration, le système d'information de base est accessible à l'aide d'une carte à puce qui permet d'identifier l'agent et d'un hexagramme. Un accès avec une clé unique[1] reste possible (mode dégradé) mais il empêche la consultation des données sensibles.

Les administrateurs systèmes reçoivent une habilitation spécifique. Comme à la DRSD, ils doivent obtenir un niveau d'habilitation supérieur à celui du système qu'ils administrent. Pour les réseaux ministériels utilisés par le service et administrés par la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI), cette contrainte a contribué à une réduction drastique – de l'ordre de plusieurs centaines à plusieurs dizaines – des personnels disposant de droits étendus sur les systèmes, ce qui a permis de renforcer les investigations de la DRSD pour la production des avis de sécurité concernant ces personnels qui font l'objet de revues périodiques de leurs droits d'administration.

Les prestataires externes disposent quant à eux de comptes spécifiques à l'accès limité, et sont systématiquement accompagnés et surveillés. Ils doivent se conformer aux dispositions contractuelles[2], inscrites dans les cahiers des clauses particulières, et destinées à assurer la sécurité des données.

Le service utilise plusieurs systèmes d'information ministériels, gouvernementaux, internationaux ou de partenaires dont la DRM n'est pas l'opérateur. Leur sécurité est assurée par le fournisseur d'accès, c'est-à-dire la DIRISI ou un prestataire extérieur. En revanche, la sécurité des systèmes métier propres à la DRM est quasiment de son seul ressort (développement et implémentation technique, corpus documentaire, *etc.*).

La DIRISI informe systématiquement la chaîne de sécurité des systèmes d'information de la DRM des blocages de mails utilisant la passerelle du réseau ministériel *Intradef* vers l'internet, ce qui a permis de dissuader et même de sanctionner des compromissions de documents classifiés. En revanche, la DRM ne semble pas disposer d'alertes pour son propre système d'information. Le service met en avant le coût humain, financier et organisationnel induit par l'implémentation de systèmes d'alertes et de blocages des données.

---

[1] *Login et mot de passe.*

[2] *Elles font l'objet d'une « annexe de sécurité ». Les dispositions sont plus ou moins contraignantes suivant la sensibilité de la prestation fournie.*

**Recommandation n° 38 : Mettre en place sur les réseaux informatiques de la DRM, avec le soutien du COMCYBER, un système qualifié visant à analyser les flux en sortie de réseau pour repérer d'éventuelles fuites de données. Son exploitation et le traitement des alertes resteront assurés en interne.**

### 4. À la DGSI

*****

### 5. À la DRPP

Les données sensibles de la DRPP sont abritées dans un réseau privé (LAN) auquel les agents du service accèdent avec des données de connexion qui leurs sont propres. Les informations auxquelles ils ont accès sont déterminées par leur unité d'affectation et leur positionnement hiérarchique. Les serveurs possèdent tous un outil de traçabilité.

La sécurité des systèmes d'information est confiée à un responsable de direction et à un responsable zonal[1] qui dépendent directement du préfet, secrétaire général pour l'administration. La gestion des équipements actifs du réseau (interventions sur site et à distance sur les équipements de la DRPP) et le chiffrement des liens intersites sont du ressort de la préfecture de police, contrairement à la sécurisation des postes de travail et des serveurs qui est du ressort de la DRPP.

Le centre de cyberdéfense du ministère de l'intérieur est en mesure d'alerter la DRPP en cas d'anomalies constatées sur le réseau public du service, adossé au réseau interministériel de l'État. Les anomalies sont alors transmises au bureau de la sécurité des systèmes d'information qui rédige des billets de sensibilisation à destination des personnels ; les manquements sont passibles de sanctions administratives.

Les « logs » des agents du service informatique font l'objet d'une analyse hebdomadaire, et ce pour tous les serveurs du réseau privé. Leur procédure d'habilitation est identique à celles des autres agents du service, à l'exception des cyber-patrouilleurs qui disposent d'une habilitation spéciale justifiée par la mise en œuvre de techniques de renseignement.

Dans le cadre de la refonte de son système d'information et de sa classification au niveau « confidentiel-défense », un système de gestion globale des authentifications sera mis en place sur la base d'une application utilisée au sein d'un service de renseignement du premier cercle ; la

[1] *Le responsable zonal effectue des audits et émet des préconisations en matière de sécurité du système d'information.*

remontée des alertes sur le nouveau système d'information sera automatisée[1]. En outre, la gestion des équipements actifs sera internalisée.

Dans son rapport d'octobre 2019, l'ISR pointait le manque de revue des droits accordés aux personnels, et en particulier aux techniciens de maintenance informatique. Aussi Mickaël Harpon disposait-il de droits d'accès trop étendus au regard de ses fonctions : accès à plusieurs fichiers de police, et habilitation générale à mettre en œuvre des techniques de renseignement. Le service doit donc procéder à des revues plus régulières des droits d'accès de ses agents, surtout en l'absence d'outils permettant de tracer leurs actions.

En outre, nul ne sait si des données ont été récupérées par Mickaël Harpon sur un support USB ; la DRPP doit être en mesure de détecter et de contrôler la connexion de périphériques externes à son système d'information.

Un rapport d'audit SSI de la DRPP, en date du 21 février 2019, a fait apparaître plusieurs fragilités :

- intervention de personnes non identifiées sur le système d'information ;

- pas de politique de sauvegarde des données informatiques ;

- présence de serveurs obsolètes, dépourvus d'antivirus ;

- enregistrement de documents classifiés sur des postes de travail non protégés.

Ce service n'est pas le seul à présenter des faiblesses dans la sécurité de ses systèmes d'information. En effet, d'autres services ont fait part à la DPR de lacunes en la matière, ce qui témoigne à la fois d'une volonté de transparence vis-à-vis du contrôleur, mais également d'une prise de conscience des points à améliorer, ce qui est heureux.

La DPR ne dispose toutefois ni des ressources ni des compétences pour entreprendre de tels audits, mais sollicite des services compétents – en l'espèce l'ANSSI et le GIC pour les techniques de recueil de renseignement – la conduite de telles missions qui permettront aux services de mieux protéger les informations et les supports classifiés dont ils disposent. Le CNRLT pourrait veiller à ce qu'un plan d'audits soit établi au bénéfice des services qui n'ont pas encore reçu d'homologation.

**Recommandation n° 39 : Procéder à un audit régulier des systèmes d'information des services de renseignement et, en tant que de besoin, accompagner ces services dans la démarche d'homologation visant à protéger le secret de la défense nationale.**

[1] *Acquisition d'un SIEM (Security Information and Event Management, ou gestion des informations et des évènements de sécurité).*

### 6. À la DNRED

*****

**Recommandation n° 40 : *****

### 7. À Tracfin

*****

### 8. Dans les services du second cercle (SNRP, SCRT et SDAO)

Au SNRP, la sécurité des systèmes d'information n'est pas assurée en interne. Les services des ministères de la justice et de l'intérieur (principalement ceux de la DGSI), ainsi que le groupement interministériel de contrôle (GIC), y participent. L'ensemble des accès au système d'information et des modifications apportées aux données est tracé. En revanche, aucun système d'alerte n'a été mis en place pour prévenir la fuite de données.

Le SCRT est quant à lui soumis à la politique du ministère de l'intérieur en matière de sécurité de ses systèmes d'information. Le service n'a pas de mesures propres en ce domaine.

Enfin, à la SDAO, les accès et actions techniques sont tracés et un suivi des actions des administrateurs systèmes est actuellement en cours de mise en place. La gestion des accès des personnels de la gendarmerie nationale au fichier de renseignement est assurée par le niveau central. La maintenance logicielle est en revanche assurée par une société privée qui n'a techniquement pas accès aux données ; *****. Les différents réseaux (internet, intranet, réseaux isolés) sont cloisonnés et étanches. Les flux sortants hors des systèmes d'information de la gendarmerie sont fortement bridés pour éviter les fuites massives de données.

## III. LA DÉONTOLOGIE DES AGENTS DE RENSEIGNEMENT

### *A. LE CADRE EN VIGUEUR*

#### 1. Des dispositions propres aux différents statuts

En matière de déontologie, les agents des services de renseignement relèvent :

- pour le personnel militaire, des dispositions qui lui sont propres et de la commission de déontologie des militaires ;

- pour les fonctionnaires de police et de gendarmerie[1] d'une part, et les agents de l'administration pénitentiaire d'autre part, des dispositions propres à chacune de ces catégories de personnels ;

- pour les autres fonctionnaires, des dispositions applicables aux fonctionnaires et contractuels de la fonction publique d'État.

Certains agents, comme ceux de la DGSE, bénéficient d'un statut autonome, régi par le décret n° 2015-386 du 3 avril 2015 fixant le statut des fonctionnaires de la DGSE, dont les dispositions en matière de déontologie sont également applicables aux contractuels.

En outre, des dispositions spécifiques aux agents des services de renseignement ont été prévues par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement[2].

### 2. Une information essentiellement concentrée sur le début de la carrière

À leur arrivée dans le service, les agents sont informés des règles déontologiques qui s'appliquent à eux. À cette occasion, ils signent divers engagements relatifs à la manipulation d'informations classifiées[3], et bénéficient d'une formation initiale au cours de laquelle les questions de déontologie sont abordées.

Les agents peuvent également être sensibilisés au sujet à travers une charte, établie par leur ministère de tutelle ou par leur service d'emploi :

- la DRSD a diffusé, en 2017, une « charte de déontologie » qui actualise sa « charte éthique » de 2013. La charte de déontologie rappelle les valeurs de discrétion, de compétence, d'intégrité et d'impartialité du service, et ce qu'elles impliquent pour les agents dans leur manière de servir. En outre, elle donne des conseils aux agents pour sa mise en pratique et, pour ce faire, les invite à se poser trois questions en cas de confrontation à un problème d'ordre déontologique : *est-ce conforme au cadre juridique applicable ? Est-ce conforme à la charte de la DRSD ? En cas de doute, à qui puis-je demander conseil ?* Enfin, une douzaine de cas concrets sont présentés à la fin du fascicule sous forme de questions-réponses, avec le bon comportement à adopter ;

- la DRM a également élaboré une charte éthique, au caractère non contraignant, qui recommande les comportements appropriés au métier d'agent de renseignement ;

---

[1] *Livre IV, titre 3, chapitre 4 du code de la sécurité intérieure portant code de déontologie de la police nationale et de la gendarmerie nationale ; décret n° 95-654 du 9 mai 1995 modifié, fixant les dispositions communes applicables aux fonctionnaires actifs des services de la police nationale.*

[2] Cf. *notamment les articles L. 862-1 et L. 862-3 du code de la sécurité intérieure.*

[3] *Par exemple, un engagement de responsabilité sur le modèle de l'annexe n° 8 de l'IGI 1300.*

- la DGSI remet quant à elle la charte de sécurité du comportement et le guide de déontologie de la police nationale à ses agents ;

- le guide de déontologie élaboré par la direction générale des douanes et droits indirects (DGDDI) est diffusé auprès des agents de la DNRED, ainsi qu'une « charte des valeurs » fondamentales pour la communauté douanière ;

- le commandant des écoles de la gendarmerie nationale a publié, en juin 2016, un ouvrage de réflexion sur les valeurs éthiques et déontologiques destiné aux formateurs et qui comporte un commentaire de chaque article du code de déontologie, exemples concrets à l'appui, pour mieux identifier les comportements fautifs ;

- enfin, le SNRP remet à ses agents une charte de déontologie propre au service.

En revanche, aucune formation obligatoire portant sur la déontologie n'est suivie par les agents de renseignement au cours de leur carrière. Ils peuvent généralement prendre connaissance de l'évolution des règles déontologiques grâce aux notes internes diffusées sur le site intranet de leur service.

### 3. Le dispositif mis en place dans les services et les sanctions prononcées

*a) Dans les services relevant du ministère des armées*

La DRSD a engagé un travail d'actualisation de son dispositif interne en matière de déontologie, à la lumière des notes de la commission de déontologie des militaires et des conseils du déontologue du ministère des armées. Cette actualisation s'est traduite par la désignation d'un référent déontologue au sein du service et l'identification des situations nécessitant la saisine de la commission de déontologie.

Les agents peuvent saisir le référent déontologue qui est chargé de leur livrer tout conseil utile sur la question.

Pour tout manquement aux obligations de dignité, neutralité, laïcité, secret professionnel, le contrôle sera exercé conjointement par le référent déontologue du service et l'officier de sécurité. Quelle que soit la situation, la division des ressources humaines et le bureau des affaires juridiques de la DRSD peuvent être sollicités pour de tels contrôles : constitution des dossiers disciplinaires[1] ou pour la commission de déontologie, examen des questions posées, *etc.* Les commissions sont saisies par la voie hiérarchique, aussi bien par l'officier de sécurité que par la division des ressources humaines.

[1] *Mesures disciplinaires prises par le service ou la direction d'armée. En cas d'infraction grave, constitutive d'un délit pénal, la direction des affaires juridiques transmet le dossier aux autorités judiciaires.*

Depuis 2017, 8 cas de manquement aux obligations déontologiques ont été mis à jour au sein de la DRSD : 5 cas de non-respect des règles internes et 3 cas de comportements inadaptés. Ces cas ont fait l'objet d'un compte rendu transmis à la « chaîne sécurité » et ont donné lieu à une enquête interne qui s'est conclue par une révision de l'habilitation et une mutation hors du service.

En revanche, la DGSE et la DRM n'ont pas fourni de statistiques sur ce point, la DRM invoquant l'absence de base de données répertoriant les sanctions prononcées. Il serait pourtant utile que le service se dote d'un tel outil, sans préjudice des règles relatives à l'effacement des sanctions disciplinaires et professionnelles, afin de mettre en lumière les manquements les plus fréquents, de sensibiliser les agents à cet égard et, éventuellement, de faire évoluer son corpus réglementaire.

*b) Dans les services relevant du ministère de l'intérieur*

Le référent déontologue pour la DGSI est le chef de l'inspection générale. Placé sous l'égide du référent déontologue du ministère de l'intérieur, il est chargé d'élaborer un guide déontologique interne au service. Un réseau de correspondants déontologues a été mis en place en mars 2020 au sein de la direction générale et des directions territoriales[1]. Leur rôle sera de faire remonter les dossiers au référent déontologue de la DGSI et de répondre aux obligations prévues par la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires.

Lorsque des manquements sont constatés à la DGSI, l'inspection générale est chargée de conduire des audits et des inspections. Si ces manquements sont constitutifs d'infractions pénales ou entrent dans le cadre d'une enquête pré-disciplinaire, le bureau central disciplinaire et judiciaire sera saisi. À la DRPP, en cas de manquement déontologique et professionnel sérieux[2], et à la suite d'une enquête administrative, le directeur de service peut demander au préfet de police de saisir l'IGPN ou de renvoyer le dossier devant le conseil de discipline. Cette commission administrative paritaire formule une proposition de sanction transmise au ministre de l'intérieur qui est la seule autorité à disposer du pouvoir disciplinaire. Selon la nature des

---

[1] Cf. *arrêté du 16 novembre 2018 relatif à la fonction de référent déontologue au sein du ministère de l'intérieur.*

[2] *Faits commis en service sur les motifs suivants : manquements au devoir d'obéissance et au crédit et au renom de la police nationale, à l'obligation de loyauté, au principe hiérarchique, au discernement. Ces faits donnent lieu à des sanctions des premier, troisième et quatrième groupes (avertissement, exclusion temporaire et révocation avec ou sans sursis). Depuis 2015, 11 cas ont été recensés.*

*Faits commis en dehors du service sur les motifs suivants : manquements au crédit et au renom de la police nationale, au principe de probité, à l'obligation de rendre compte, à l'obligation de discrétion et au devoir d'exemplarité. Ces faits donnent lieu à des sanctions des premier et quatrième groupes (blâme, exclusion temporaire avec ou sans sursis). Depuis 2015, 6 cas ont été recensés.*

infractions commises, et indépendamment de la procédure disciplinaire, l'habilitation peut être retirée.

Au SCRT, aucune sanction pour des cas de fraude ou de compromission n'a été infligée à l'encontre d'un agent. Seules des sanctions administratives pour des problèmes comportementaux ont été prononcées (alcoolémie en service, accident de la route avec un véhicule de service, perte d'arme ou de carte professionnelle, *etc.*). Le bureau des affaires disciplinaires de la direction des ressources et des compétences de la police nationale (DRCPN) tient à jour l'ensemble des sanctions prononcées pour les personnels de la police nationale ; la DGGN possède un service équivalent en son sein.

Si un agent du service commet un délit pour lequel il a été interpellé et gardé à vue, le service menant l'enquête informera le service d'affectation du personnel. Toutefois, si le délit commis n'a pas entraîné d'interpellation, l'agent n'est pas tenu de faire état de sa qualité, mais il a l'obligation d'en rendre compte. En cas de main courante ou de plainte déposée contre un agent, le service ayant pris la déclaration en avise la hiérarchie de l'agent mis en cause ; une enquête peut alors être diligentée, en plus de l'enquête judiciaire, et pourra conduire à une sanction en cas de manquement avéré.

Pour la SDAO, le référent déontologue et alerte est le chef de l'IGGN. En cas de manquement constaté, le sous-directeur de l'anticipation opérationnelle décide ou propose les suites qu'il entend donner d'un point de vue statutaire et disciplinaire. Lorsqu'un manquement constaté par l'IGGN est manifestement susceptible de constituer un crime ou un délit, il est proposé au DGGN de saisir le procureur de la République en recourant à la procédure de l'article 40 du code de procédure pénale[1].

*c) Dans les services relevant des ministères économiques et financiers*

*****

*d) Dans le service relevant de la chancellerie*

*****

### 4. Les délits commis dans un cadre extraprofessionnel ne sont pas systématiquement remontés aux services

Les agents de la DGSE sont tenus de déclarer auprès du service de sécurité toute mise en cause dans une affaire judiciaire, y compris pour des délits mineurs. Le service de sécurité peut également en être tenu informé par les services de police ou de gendarmerie. En cas de manquement aux

[1] *En effet, pour garantir la neutralité et l'impartialité de l'IGGN à laquelle les magistrats du parquet ou de l'instruction sont susceptibles de confier les investigations, le chef de l'IGGN ne signe jamais un article 40.*

obligations en matière de protection du secret ou de déontologie, la hiérarchie de proximité et le service de sécurité en sont informés. Les responsables hiérarchiques peuvent ainsi proposer des sanctions et le service de sécurité peut, en tant que de besoin, instruire le dossier à charge et à décharge en vue de suites disciplinaires.

La DRSD n'est pas systématiquement informé des délits commis par ses agents dans un cadre extraprofessionnel. Le cas échéant, les signalements qui lui sont adressés proviennent essentiellement des services partenaires (DGSE, DGSI, *etc.*).

La DRM est quant à elle informée des délits commis par ses agents militaires *via* une fiche de renseignement spécifique portée à la connaissance de l'autorité militaire, dès lors que les agents sont gardés à vue ou qu'ils sont mis en cause dans un procès pénal. S'agissant des agents civils, la juridiction judiciaire ne notifie au service que les condamnations pénales desdits agents. Toutefois, la DRM est souvent informée par la direction centrale de la police judiciaire des mains courantes ou des plaintes visant l'un de ses agents, à condition qu'ils fassent état de leur qualité d'agent de renseignement.

Si un délit constaté fait l'objet d'un rapport de police ou de gendarmerie, d'une procédure judiciaire ou d'un simple déplacement des forces de l'ordre sans pour autant qu'il y ait de poursuites engagées, la DRPP est informée *via* un télégramme. Cette information n'exonère pas l'agent de son devoir de rendre compte.

Les agents de la DNRED doivent rendre compte à leur hiérarchie des infractions pénales qu'ils ont commises. En application de la circulaire du 11 mars 2015, l'administration peut solliciter des juridictions les décisions pénales qui concernent ses agents ; les parquets sont tenus de répondre avec diligence. En outre, les directives du ministère de la justice aux parquets demandent d'aviser les supérieurs hiérarchiques de l'engagement de poursuites pénales à l'encontre de leurs agents, ou du prononcé de condamnations définitives. Toutes les condamnations pénales sont susceptibles d'entraîner des poursuites disciplinaires.

Pour résumer, les agents des services de renseignement sont en principe tenus de rendre compte des délits, même mineurs, qu'ils commettent en dehors du cadre professionnel. Néanmoins, si ce délit n'entraîne pas de garde-à-vue ou de poursuites judiciaires, les agents n'ont pas à faire état de leur appartenance à un service de renseignement, ce qui empêche la remontée d'informations *via* les services de police ou de gendarmerie. Dans la mesure où l'anonymat des agents de renseignement doit être préservé, toute procédure de remontée automatique d'informations est impossible à mettre en œuvre. Elle serait pourtant utile aux services pour détecter d'éventuelles vulnérabilités chez leurs agents ; la vérification (consultation du fichier de main courante informatisée des commissariats de

police du lieu d'habitation du candidat) incombe donc aux services enquêteurs dans le cadre des enquêtes administratives qu'ils mènent.

**Recommandation n° 41 : Contraindre l'ensemble des agents des services de renseignement à rendre compte à leur officier de sécurité des délits qu'ils ont commis dans un cadre extraprofessionnel, quelle qu'en soit la nature. Lors du renouvellement de leur habilitation, le service enquêteur prendra l'attache des services de police et de gendarmerie afin de recueillir des informations utiles sur les candidats et mettre en lumière toute omission de leur part.**

### 5. La prévention des conflits d'intérêt

En cas de départ du service ou de retrait d'habilitation, l'agent signe le second volet de l'engagement[1], conservé par l'autorité d'habilitation. Ce volet précise que les obligations relatives à la protection des informations classifiées auxquelles l'agent a pu avoir accès perdurent au-delà du terme mis à ses fonctions ou à son habilitation.

L'agent peut également signer un document interne au service par lequel il atteste sur l'honneur avoir rendu l'intégralité des informations et supports professionnels manipulés lors de sa présence dans le service, et s'engage à ne communiquer aucune information métier ou technique dont il aurait eu connaissance dans l'exercice de ses fonctions à des tiers.

Afin de garantir leur indépendance, les agents qui cessent temporairement ou définitivement leurs fonctions pour exercer une activité lucrative doivent éviter tout conflit d'intérêts. Dans ce cas précis, une commission de déontologie apprécie la compatibilité avec les fonctions précédemment exercées :

- pour le personnel militaire, il s'agit de la commission de déontologie des militaires ;

- pour le personnel civil, c'est la haute autorité pour la transparence de la vie publique (HATVP) qui est désormais compétente pour connaître de ces questions.

À l'occasion de l'instruction du dossier, ces commissions peuvent procéder à des auditions, y compris celles des agents concernés, afin de se prononcer sur les relations directes ou indirectes des intéressés avec les entreprises concernées. Le cadre juridique applicable en cas de prise illégale d'intérêt (exercice d'activités lucratives dans des entreprises privées) leur est également rappelé.

Certains agents passent devant une commission ministérielle de déontologie : c'est le cas des agents de la DGSI. La commission ministérielle

[1] *Le premier volet est signé par la personne habilitée lorsque la décision d'habilitation lui est notifiée.*

émet des restrictions à l'accès de certaines professions réglementées pour lesquelles les personnels actifs sont réputés bénéficier réglementairement de l'aptitude professionnelle (métiers de la sécurité, directeur ou agent de recherche privée, reconversion d'ingénieur dans le secteur privé, *etc.*).

La DRSD a également mis en place certaines restrictions pour ses agents rejoignant le secteur privé. Ainsi, si l'un de ses agents a eu un lien quelconque avec une entreprise privée dans le cadre de ses fonctions (surveillance, contrôle, conclusion de contrats, formulation d'avis, *etc.*), il doit alors respecter un préavis de 3 ans avant de pouvoir l'intégrer.

Les agents de Tracfin, titulaires ou contractuels, souhaitant exercer une activité annexe (enseignement, publication d'articles, *etc.*) ou quittant le service pour rejoindre le secteur privé, doivent en informer le référent déontologue. En cas de départ du service, Tracfin joint au dossier constitué par l'agent un courrier relatif aux missions qu'il a exercées, ainsi qu'un document relatif à l'appréciation de la demande d'exercice d'une activité privée dans lequel le service doit répondre à plusieurs questions (par « oui », « non », ou « possible ») :

- en application de l'article 432-13 du code pénal, l'agent a-t-il été chargé, au cours des années précédant le début de son activité privée en raison de ses fonctions :

  - de la surveillance ou de contrôle de l'entreprise ou de l'organisme dans lequel il souhaite travailler,
  - de la conclusion de contrat ou de formulation d'un avis sur de tels contrats,
  - de proposer directement à l'autorité compétente des décisions relatives à des opérations réalisées par cette entreprise ou cet organisme ou de formuler un avis sur de telles décisions ;

- en application du quatrième alinéa du III de l'article 25 *octies* de la loi du 13 juillet 1983, l'activité envisagée nous semble-t-elle de nature :

  - à compromettre ou mettre en cause le fonctionnement normal du service,
  - à compromettre ou mettre en cause l'indépendance ou la neutralité du service,
  - à méconnaître un principe déontologique mentionné à l'article 25 de la loi du 13 juillet 1983 (en particulier les obligations de dignité, d'impartialité, de probité, le principe de laïcité, *etc.*).

### *B. LE SUIVI DES ANCIENS AGENTS DE RENSEIGNEMENT*

Comme indiqué précédemment, les anciens agents sont tenus au secret concernant les informations qu'ils ont eu à connaître au cours de leur carrière et les méthodes opérationnelles qu'ils ont employées. En outre, leur identité ainsi que leur appartenance actuelle ou passée à un service de renseignement restent protégées par les dispositions de l'article 413-13 du code pénal.

Les anciens agents restent donc soumis, après leur départ du service, à un devoir de discrétion. Toutefois, le comportement de plusieurs de ces agents a retenu l'attention de la délégation parlementaire au renseignement. Les dérives constatées, et relayées par la presse, plaident en faveur d'un contrôle accru de leurs agissements, même après la fin de leurs fonctions :

- le 21 mars 2019, un ancien militaire du service action de la DGSE a été tué par balles. Cet ancien agent aurait projeté d'assassiner un opposant politique congolais. Il était auparavant auteur de livres d'espionnage, dans lesquels il narrait ses missions en France et à l'étranger ;

- en décembre 2017, deux anciens agents de la DGSE ont été déférés devant le juge d'instruction pour des faits susceptibles de constituer les crimes et délits de trahison par livraison d'informations à une puissance étrangère, provocation au crime de trahison et atteinte au secret de la défense nationale. D'après les informations parues dans la presse, les intéressés auraient été recrutés par les autorités chinoises qui s'intéressaient aux méthodes opérationnelles du renseignement extérieur français. Ces faits ont été détectés et dénoncés au procureur de la République par la DGSE elle-même ;

- le 18 juin 2016, l'ancien directeur technique de la DGSE donnait une conférence publique dans une grande école d'ingénieurs, au cours de laquelle il a révélé l'implication de la France dans une campagne de cyberespionnage, et confirmé l'existence d'une campagne similaire menée par les États-Unis et visant l'Élysée pendant l'élection présidentielle.

Aucun de ces manquements graves aux obligations déontologiques, par ailleurs constitutives d'infractions pénales, n'a été remonté à la DPR, ni au moment où les faits ont été rendus publics, ni à travers les réponses au questionnaire adressé aux services. En tant que contrôleurs de l'activité des services de renseignement, les membres de la délégation devraient être tenus informés des manquements déontologiques graves et des procédures judiciaires engagées par les services à l'encontre de leurs agents ou de leurs anciens agents. La bonne information de la DPR lui permettra de mieux appréhender les risques auxquels les services sont confrontés et les accompagner dans leur maîtrise.

**Recommandation n° 42 : Informer la délégation parlementaire au renseignement des manquements déontologiques graves commis par leurs agents ou leurs anciens agents, et des procédures juridiques initiées à leur encontre.**

### 1. Le contrôle de leur expression publique : un exercice délicat

Arnaud Danjean, député européen et ancien agent de la DGSE « *regrette que […] d'anciens agents de la DGSE se considèrent omniscients sur toutes les questions de sécurité* »[1]. Pour sa part, il « *décline énormément de sollicitations, d'abord parce que cela fait longtemps [qu'il n'est] plus à la DGSE […], deuxièmement, lorsqu'[il était] à la DGSE, [il n'était] pas spécialiste du contre-espionnage ou du contre-terrorisme* ». Ainsi, malgré une douzaine d'années passées dans ce service, Arnaud Danjean « *ne se sent pas autorisé à donner son avis sur tout* », et appelle à un renforcement du contrôle des anciens agents des services de renseignement qui, pour certains d'entre eux, auraient révélé des sources dans des ouvrages qu'ils ont écrits.

Le contrôle de l'expression publique des agents est un exercice délicat dès lors qu'aucune information classifiée n'est délivrée. Seules leur rigueur et leur déontologie personnelles, et celles des médias qui les invitent, permettront de mesurer leurs prises de parole et d'éviter de livrer des analyses – voire des informations – erronées à un public peu sensibilisé aux questions de renseignement.

En revanche, si des informations classifiées sont livrées publiquement, les services doivent être en mesure d'entamer des poursuites judiciaires, notamment à des fins dissuasives, tant les peines encourues sont lourdes.

### 2. Les jeunes retraités constituent une cible de choix pour les services étrangers

Les cadres des services de renseignement ne sont pas les seuls à faire l'objet de tentative de « retournement » par un service étranger. La DRSD relève que les cadres de l'industrie de défense font eux aussi l'objet de tentatives de recrutement par des puissances étrangères à des fins de transferts de technologies. Ces puissances agissent par des ciblages réfléchis de cadres à haute valeur ajoutée, qu'ils soient actifs ou jeunes retraités, en raison de leur positionnement ou de leur accès à des données classifiées.

*****

[1] *Source : émission* « Conversations secrètes, le monde des espions », *France Culture.*

### 3. Les moyens d'action

Le premier moyen d'action, déjà utilisé par la DRSD et la DGSI, consiste à rendre publiques les méthodes employées par des services étrangers pour recruter des sources ou s'accaparer de secrets industriels. Ce procédé, en plus de sensibiliser les cibles potentielles aux tentatives d'approche et d'appeler à leur vigilance, adresse un message aux acteurs malveillants qui se savent alors surveillés.

Le second moyen d'action est de consacrer une partie des ressources des services au suivi des anciens agents de renseignement et cadres des entreprises stratégiques (industrie de défense, opérateur d'intérêt vital, *etc.*). Une approche par les risques permettra de cibler les profils devant faire l'objet d'un suivi régulier. Ces ressources existent déjà au sein de nos services de renseignement puisqu'elles ont permis de détecter des cas de compromission ; mais combien échappent à leur surveillance et jusqu'à quand cette surveillance doit-elle s'opérer ?

Là aussi, Tracfin pourrait être un partenaire très utile. Le service de renseignement financier pourrait détecter des comportements financiers anormaux chez d'anciens agents ou cadres, et pousser ses investigations le cas échéant.

## *C. LA JUDICIARISATION DES MANQUEMENTS AUX OBLIGATIONS DÉONTOLOGIQUES*

Si les manquements constatés sont constitutifs d'un crime ou d'un délit, les services peuvent décider d'ester en justice sur le fondement de l'article 40 du code de procédure pénale, et dans le respect du secret de la défense nationale. Si les autorités judiciaires sont déjà saisies, les services peuvent décider de leur apporter leur concours[1] et se porter partie civile.

En cas de saisine des juridictions pénales, les documents portés au dossier peuvent être déclassifiés conformément aux dispositions des articles L. 2311-1 à L. 2312-8 du code de la défense nationale et 413-9 du code pénal ; seul le ministre de tutelle a compétence pour ordonner leur déclassification au profit des autorités judiciaires, après avis de la commission consultative du secret de la défense nationale (CSDN)[2]. Cette procédure est censée éviter la divulgation d'informations classifiées à des personnes non habilitées ou que leur publication ne porte préjudice au service. Dans une décision du 10 novembre 2011, le Conseil constitutionnel a estimé que l'existence, le

[1] *En cas de compromission (méconnaissance de règles relatives à la protection du secret), la DGSI est tenue de saisir l'autorité judiciaire, seule compétente pour apprécier l'opportunité des poursuites. Le cas échéant, elle assure la gestion du volet judiciaire du dossier.*

[2] *Cette commission rend un avis (favorable, défavorable ou favorable à une déclassification partielle) dans un délai de 2 mois. Cet avis, publié au* Journal officiel*, est généralement suivi par l'autorité administrative.*

statut et la mission de la CSDN permettait une conciliation non déséquilibrée entre les objectifs constitutionnels de protection des intérêts fondamentaux de la Nation et d'exercices des missions fondamentales de la justice.

Malgré l'existence de cette procédure, certains services déplorent quedes documents soient très souvent rendus publics à l'occasion de procédures judicaires[1] ; ce risque peut les conduire à ne pas judiciariser certaines affaires. En outre, le caractère contradictoire de la procédure oblige la communication de documents classifiés à la partie adverse. D'une manière générale, la judiciarisation de certaines affaires, et la déclassification de documents qu'elle suppose, peut porter atteinte à l'image du service.

Les sanctions administratives peuvent faire l'objet d'un recours devant le juge administratif et nécessiter de déclassifier des documents. Dans le cas des militaires, le recours administratif préalable obligatoire a pour effet de limiter considérablement le volume des recours exercés devant la juridiction administrative.

À la DGSE, quatre avis ont été initiés par le service en application de l'article 40 du code de procédure pénale depuis septembre 2016. L'un de ces dossiers a abouti à un rappel à la loi ; les trois autres sont en cours.

Ces trois dernières années, plusieurs agents de la DRPP ont comparu devant le tribunal de grande instance de Paris ou de Créteil pour violences avec armes ou accident mortel de la circulation commis en service. Ils ont été condamnés à des peines d'emprisonnement avec sursis, d'interdiction temporaire de port d'arme ou d'annulation de permis de conduire, et au versement de dommages et intérêts. Le conseil de discipline ou l'IGPN ont été saisis de ces deux dossiers. En outre, un agent a consulté indûment des fichiers dans le cadre d'un litige personnel et a fait l'objet d'une plainte. Son habilitation lui a immédiatement été retirée et il a été remis à la disposition de la direction des ressources humaines de la préfecture de police. Là aussi, l'IGPN a été saisie du dossier, dont la DRPP ignore les suites judiciaires et administratives.

Enfin, en 2013, un agent de Tracfin a publié des éléments à charge sur le blog de *Mediapart*. Son directeur de service a alors déposé une plainte auprès du procureur de la République pour violation du secret professionnel. Une enquête de police a été ouverte et a permis d'identifier l'auteur des faits, renvoyé devant le tribunal correctionnel de Paris. Le parquet a communiqué son identité à Tracfin qui l'a suspendu de ses fonctions. L'intéressé a réintégré son administration d'origine et a été condamné en 2014 à 2 mois d'emprisonnement avec sursis[2].

---

[1] *Violation du secret de l'information régie par l'article 11 du code de procédure pénale et les articles 226-13 et 226-14 du code pénal.*

[2] *L'absence d'inscription au casier judiciaire lui a permis de conserver son emploi.*

## *D. LE STATUT DE LANCEUR D'ALERTE DANS LE MONDE DU RENSEIGNEMENT*

### 1. L'exigence de protection du secret de la défense nationale

Le secret de la défense nationale est un régime de protection des informations classifiées dont la divulgation pourrait nuire à la défense nationale, dans sa définition la plus large (lutte contre le terrorisme, cybersécurité, protection des infrastructures essentielles et critiques, *etc.*). Dans sa décision n° 2011-192 QPC du 10 novembre 2011, le Conseil constitutionnel a jugé *« que le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, réaffirmés par la Charte de l'environnement, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire »*.

**Article 413-9 du code pénal**

Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'État.

Cette protection prend la forme d'une répression pénale[1] contre toute divulgation à des personnes n'ayant ni le droit, ni le besoin d'en connaître.

Si l'exécutif a l'apanage du secret de la défense nationale, sa protection, dans un État de droit, doit néanmoins être conciliable avec le contrôle judiciaire ou juridictionnel, ainsi qu'avec le contrôle parlementaire. En effet, le contrôle ne compromet en rien le secret ; il doit éviter au Gouvernement de prendre de mauvaises décisions, et doit permettre de déceler des défaillances ou des irrégularités.

Le parlement n'a à connaître des informations classifiées relatives au domaine du renseignement qu'à travers la délégation parlementaire au renseignement, au format très restreint, et dont l'ensemble des membres, de

[1] Cf. *articles 413-10 et suivants du code pénal.*

même que le secrétariat qui l'accompagne dans l'exercice de ses missions, est habilité au niveau « secret-défense ».

Les prérogatives de la DPR sont bien encadrées par la loi, tout comme son pouvoir d'information. Afin de rendre ce contrôle démocratique plus efficace, les sénateurs ont proposé d'améliorer le degré d'information de la délégation, mais leurs propositions n'ont, pour l'heure, pas trouvé d'issue législative[1].

Conscient de l'importance de protéger le secret de la défense nationale, le pouvoir législatif poursuit en la matière le même objectif que le pouvoir exécutif. Les parlementaires veillent toutefois à une application raisonnable et proportionnée de ce principe, pour ne protéger que les informations nécessaires à la préservation des intérêts fondamentaux de la Nation ; il s'agit donc de trouver un juste équilibre entre la transparence absolue qui n'est pas souhaitable, et le secret absolu qui entrave l'exercice de ses missions démocratiques. Les parlementaires doivent avoir accès aux informations nécessaires voire essentielles à son contrôle, sans laisser l'exécutif décider seul des éléments qu'ils portent à la connaissance du parlement : c'est là toute la différence entre un véritable contrôle parlementaire – c'est-à-dire un contrôle approfondi qui légitimerait l'action du Gouvernement – et une caution parlementaire – à savoir un contrôle démocratique superficiel qui donnerait, malgré tout, *quitus* à l'exécutif.

D'ailleurs, force est de reconnaître que le parlement ne s'est jamais rendu responsable d'une quelconque fuite d'informations classifiées ; pis, les fuites qui ont eu lieu ces derniers mois[2] concernaient des informations dont le parlement ne disposait pas. Par conséquent, certains agents relevant des services de l'exécutif – qu'il s'agisse des services de renseignement ou de tout autre service concourant à la défense et à la sécurité nationale – peuvent éprouver le besoin d'informer la représentation nationale, voire les citoyens eux-mêmes, de certains agissements ou comportements observés au sein de leur service. Or, pour ce faire, ils n'ont à ce jour aucun moyen d'action, à l'exception du dispositif prévu pour les seules techniques de renseignement (*cf. infra*).

En l'absence de dispositif de lanceur d'alerte couvrant l'ensemble des activités des services, toute fuite est alors portée à la connaissance de personnes non habilitées ce qui peut, dans certains cas, aller à l'encontre de l'intérêt général puisque des acteurs malveillants peuvent aussi en être informés.

---

[1] *Proposition de loi n° 470 (2017-2018) de MM. Philippe Bas, Christian Cambon, François-Noël Buffet et plusieurs de leurs collègues, tendant à renforcer le contrôle parlementaire du renseignement. Cette proposition de loi avait été introduite par voie d'amendement dans le projet de loi de programmation militaire 2019-2025, en première lecture au Sénat, mais retirée à l'issue de la commission mixte paritaire.*

[2] *Par exemple, la note de la direction du renseignement militaire (DRM) sur l'utilisation d'armes vendues par la France et utilisées par la coalition anti-Houthis au Yémen.*

La délégation parlementaire au renseignement identifie cette lacune législative comme un risque et propose, à cet égard, de compléter le dispositif de lanceur d'alerte existant en poursuivant un double objectif :

- protéger le secret de la défense nationale en réservant les signalements aux seules instances dûment habilitées ;

- protéger les lanceurs d'alerte « de bonne foi » contre toute sanction de leur administration.

Il importe, en conséquence de compléter le dispositif de lanceur d'alerte introduit par la loi de juillet 2015.

### 2. Le dispositif existant, limité aux techniques de renseignement, mérite d'être complété

La loi de 2015 a prévu un dispositif de lanceur d'alerte qui se limite aux seules techniques de renseignement. L'examen du projet de loi s'est déroulé dans un contexte fortement marqué par les attentats de janvier 2015 et la prégnance de la menace terroriste, mais aussi par les révélations d'Edward Snowden sur les agissements de la NSA, ce qui explique peut-être que le législateur ait circonscrit ce champ aux seules techniques de renseignement. Jusqu'à présent, ce dispositif n'a jamais trouvé à s'appliquer.

Un autre dispositif de lanceur d'alerte a été instauré par la loi dite « Sapin 2 »[1], pour les agents publics, mais elle exclut de son champ d'application les informations couvertes par le secret de la défense nationale.

Or, les activités des services ne se limitent pas aux seules techniques de recueil de renseignement ; le champ déontologique doit donc être appréhendé dans son acception la plus large.

La DPR pourrait être une instance de recueil et d'examen des signalements offrant une garantie de préservation du secret et de sécurité pour les lanceurs d'alerte. Avec un tel dispositif, elle aurait pu connaître de dysfonctionnements majeurs des services, par exemple *****.

Grâce à un dispositif de lanceur d'alerte élargi, un agent de ce service aurait pu alerter la délégation parlementaire au renseignement des graves dysfonctionnements de son service d'emploi, sans risquer de sanction ou de discrimination en raison de son signalement. Il aurait laissé aux

[1] *L'article 6 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, précise qu'*« un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, […] ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance. Les faits, informations ou documents […] couverts par le secret de la défense nationale […] sont exclus du régime de l'alerte […]. »

parlementaires le soin de saisir le procureur de la République de ces faits s'ils le jugeaient nécessaire.

Par ailleurs, la DPR pourrait être destinataire d'informations qu'un agent de renseignement souhaiterait communiquer à la représentation nationale sans pour autant les rendre publiques (une note classifiée, *etc.*).

### 3. Le modèle américain

Aux États-Unis, une loi de 1998[1] protège les agents des services de renseignement dénonçant un acte présumé illégal au sein des services.

Ces agents peuvent saisir l'inspection générale des services de renseignement (ICIG) de toute « préoccupation urgente » (« *urgent concern* ») qui concernerait :

- un abus ou une violation du cadre juridique relatif au financement, à la gestion ou aux opérations des services de renseignement impliquant des informations classifiées, dès lors qu'elles ne portent pas sur des divergences de vues à propos de questions de politique publique ;

- une fausse déclaration au Congrès ou une omission volontaire portant sur le financement, la gestion ou le fonctionnement d'une activité de renseignement ;

- des représailles ou des menaces de représailles envers un lanceur d'alerte.

L'ICIG, organe indépendant, dispose alors de 14 jours pour étudier le signalement et, s'il le juge crédible, l'adresser au directeur du renseignement national (DNI). Ce dernier doit, à son tour, transmettre le signalement aux commissions parlementaires du renseignement du Sénat et de la Chambre des représentants, sous 7 jours.

Si l'inspecteur général ne transmet pas le signalement au DNI, les agents peuvent saisir directement la commission du renseignement du Congrès. Le cas échéant, ils doivent en informer l'inspecteur général et demander conseil au DNI pour contacter les commissions de manière sécurisée, et suivre ses « bonnes pratiques » en matière de révélation d'informations classifiées au Congrès afin d'être protégé.

Ce dispositif a trouvé à s'appliquer le 12 août 2019 lorsqu'un agent de renseignement[2] a adressé un signalement à l'ICIG, portant sur une conversation téléphonique du 25 juillet 2019 entre le président américain et son homologue ukrainien. D'après cet agent, Donald Trump aurait utilisé sa fonction pour solliciter l'ingérence d'un pays étranger dans la prochaine élection présidentielle américaine.

---

[1] *Intelligence Community Whistleblower Protection Act (ICWPA).*

[2] *D'après le* New York Times*, il s'agirait d'un agent de la CIA.*

L'inspecteur général, Michael Atkinson, a jugé cette plainte crédible et l'a donc fait suivre au DNI, Joseph Maguire. Mais après avoir consulté la Maison blanche et le ministère de la justice, le DNI, récemment nommé par le président américain, a conclu qu'il n'était pas contraint d'en informer le Congrès et a classé le dossier.

Or, le directeur du renseignement national n'a pas l'autorité juridique pour casser une décision de l'inspecteur général et dissimuler au Congrès le signalement d'un lanceur d'alerte. Bien que la loi soit muette sur ce point, l'inspecteur général a alors décidé d'informer lui-même le Congrès de ce signalement, sans toutefois en révéler le contenu.

Lorsqu'il l'avait signée, Bill Clinton avait précisé que cette loi ne saurait restreindre son autorité constitutionnelle de contrôler la communication de certaines informations classifiées au Congrès. Cette prérogative permettrait de ne pas affaiblir le pouvoir exécutif.

### 4. Le dispositif proposé par la DPR

Le modèle américain n'est pas transposable en l'état. En effet, l'équivalent français de l'ICIG est l'ISR (inspection des services de renseignement) ; or, contrairement à son homologue américain, l'ISR ne constitue pas un corps d'inspection en tant que tel : ses membres, issus de plusieurs corps d'inspection ministérielles (inspection générale des finances, inspection générale de l'administration, contrôle général des armées, *etc.*) sont désignés par le Premier ministre, sur proposition de leur ministre de tutelle, et après avis du CNRLT[1]. L'ISR agit uniquement lorsqu'il est diligenté par le Premier ministre qui en arrête la composition, variable d'une mission à l'autre.

Par conséquent, l'ISR n'est pas un organe indépendant, pas plus que la CNRLT qui est rattachée à la présidence de la République. En outre, le coordonnateur national n'a pas de pouvoir hiérarchique sur les directeurs des services de renseignement. Aussi la saisine directe de la DPR par un lanceur d'alerte se justifierait-elle par son indépendance vis-à-vis de l'exécutif et son champ de compétences qui, contrairement à celui de la CNCTR, dépasse le champ des techniques de renseignement.

Ainsi, la DPR souhaiterait mettre un place un dispositif de lanceur d'alerte protecteur pour les agents de renseignement, qui prévoirait :

- la possibilité de saisir la CVFS, qui émane de la DPR, pour toutes les questions relatives à l'emploi des fonds spéciaux ;

- la possibilité de saisir la DPR pour toutes les questions liées à l'activité des services, à l'exclusion de celles des techniques de

[1] *La CNRLT assure le secrétariat de l'ISR dont le secrétaire général est affecté auprès de la coordination nationale.*

renseignement déjà couverte par la loi du 24 juillet 2015, et des fonds spéciaux qui serait renvoyée à sa formation spécialisée.

Avec un tel dispositif, la DPR et la CVFS pourraient investiguer à partir d'un signalement sans pour autant mettre en péril la défense et la sécurité nationale. Par cohérence, cette évolution devra s'accompagner de la possibilité d'auditionner des agents de renseignement en l'absence de leur hiérarchie, ce que l'article 6 *nonies*, dans sa rédaction actuelle, n'autorise pas.

Si la délégation (ou la commission) estime que l'illégalité constatée est susceptible de constituer une infraction, son président saisirait le procureur de la République au titre de l'article 40 du code de procédure pénale. Le cas échéant, il en informerait le secrétariat général de l'ISR, placé auprès de la CNLRT. Le Premier ministre pourra alors diligenter l'ISR, comme il l'a fait après les assassinats perpétrés au sein de la préfecture de police de Paris.

**Recommandation n° 43 : Compléter le dispositif de lanceur d'alerte créé par la loi de juillet 2015 et étudier la possibilité de confier une partie de ces missions à la DPR.**

### *E. UN DÉFAUT D'INFORMATION DU PARLEMENT RÉGULIÈREMENT POINTÉ PAR LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT*

Malgré les demandes de la DPR, certains services ont refusé de lui communiquer les documents inhérents à la déontologie de leurs agents ou certains éléments statistiques sur les manquements observés. Par ailleurs, peu de cas concrets ont été remontés à la DPR malgré ses questions écrites très précises ; la presse s'est pourtant fait l'écho de manquements déontologiques graves dans plusieurs services de renseignement.

Dès lors, ce manque d'information de la délégation, déjà souligné à plusieurs reprises dans ses rapports d'activité, constitue un frein à ses pouvoirs de contrôle.

Bien entendu, la DPR n'a pas vocation à se substituer aux commissions de discipline ou à la justice pour sanctionner et juger les agents fautifs. Les parlementaires doivent néanmoins pouvoir s'assurer que les mesures ont été prises en interne pour mieux maîtriser les risques, afin d'éviter que les « dérives » observées ne puissent se reproduire ; c'est d'ailleurs dans cet état d'esprit que la commission de vérification des fonds spéciaux (CVFS), qui émane de la DPR, assure son contrôle. Les membres de la délégation doivent pouvoir nourrir leur réflexion pour être en mesure d'adresser des recommandations pertinentes à l'exécutif et, le cas échéant, de traduire ces recommandations sur le plan législatif.

En matière de déontologie, l'information du parlement est exclusivement assurée par voie de presse, ce qui n'est pas acceptable : les

membres de la délégation ne sauraient se contenter de telles « fuites » pour accomplir leurs missions de contrôle, alors même que leurs travaux sont couverts par le secret de la défense nationale et qu'ils ont toujours veillé à respecter leur devoir de discrétion en ce domaine.

Dans cette même optique, la DPR souhaiterait être tenue informée des saisines du procureur de la République par la CNCTR, sur le fondement de l'article L. 861-3 du code de la sécurité intérieure. Cette information est destinée à orienter ses travaux qui, bien entendu, n'ont pas vocation à se substituer au travail de la justice.

Enfin, la délégation souhaiterait que la CNCTR lui communique les recommandations qu'elle adresse au Premier ministre et aux services au titre de l'article L. 833-6 du code de la sécurité intérieure, tendant à l'interruption de la mise en œuvre d'une technique de renseignement et à la destruction des renseignements collectés, en cas d'irrégularité constatée.

**Recommandation n° 44 : Améliorer l'information de la délégation parlementaire au renseignement par la commission nationale de contrôle des techniques de renseignement. Prévoir dans la loi une transmission à la DPR des recommandations adressées par la CNCTR en application de l'article L. 833-6 du code de la sécurité intérieure et, le cas échéant, des signalements adressés au procureur de la République sur le fondement de l'article L. 861-3 du même code.**

# CHAPITRE IV :
# LE NOUVEL UNIVERS DU RENSEIGNEMENT SPATIAL

En annonçant en juillet 2018 l'élaboration d'une stratégie spatiale de défense, le Président de la République a souligné à quel point l'espace, « *par les incroyables potentialités qu'il offre mais également par la conflictualité qu'il suscite* » est devenu un véritable enjeu de sécurité nationale. Ce qui se passe à plusieurs kilomètres au-dessus de nos têtes produit des effets de plus en plus prégnants sur notre vie quotidienne et bien au-delà, sur l'exercice de la souveraineté nationale. La création en septembre 2019 d'un véritable « Commandement de l'espace » rattaché à l'Armée de l'Air et de l'espace, marque incontestablement l'entrée dans une ère nouvelle ; la stratégie spatiale de défense présentée à l'été 2019 en constitue le nouveau cadre d'action.

Si l'espace n'est pas, pour le moment, un théâtre de guerre, force est de constater qu'il est de moins en moins un univers de paix. Les grandes puissances se préparent à se défendre, et le cas échéant à passer à l'offensive, comme en témoigne la volonté du Président américain, Donald Trump, de hisser le sujet de la puissance spatiale au rang de ses priorités politiques. L'arsenalisation de l'espace n'est plus une hypothèse ; elle ne semble plus être désormais qu'une question de temps.

Et si la guerre dans l'espace n'est pas encore militaire, elle est déjà économique avec la montée en puissance du « *New Space* » et des révolutions qui l'accompagnent. Les frontières sont de plus en plus ténues entre le public et le privé, entre les grandes puissances et les petits États, entre les opérateurs historiques et les nouveaux entrants… La vitesse de ces bouleversements oblige à renforcer notre capacité d'adaptation et notre agilité dans un environnement de plus en plus instable.

Dans ce contexte, le renseignement d'intérêt spatial est appelé à occuper une place de plus en plus stratégique pour améliorer notre connaissance de la situation spatiale, pour protéger nos satellites, y compris de manière active, mais aussi en appui à nos opérations militaires. En quelques années, les révolutions en cours dans le domaine spatial ont revisité les modalités d'exercice de notre souveraineté, à l'échelle nationale comme européenne, et défient notre capacité à conserver notre statut de puissance mondiale.

## I. L'ESPACE, NOUVELLE FRONTIERE DU RENSEIGNEMENT

L'espace extra-atmosphérique appartenant à tous, il devient, au fur et à mesure des avancées technologiques, de plus en plus investi, à des fins tant civiles que militaires. L'occupation de l'espace est de moins en moins le privilège de la puissance publique qui doit désormais le partager avec des entreprises privées à l'assaut de nouveaux marchés.

La conquête spatiale a également ouvert de nouveaux champs en termes d'acquisition de renseignement, faisant de l'espace un domaine stratégique essentiel à nos opérations de défense. Observation, écoute, communication, navigation : l'espace est devenu le nouvel Eldorado du renseignement. Indispensable à la défense de nos intérêts et à la sécurité nationale, le renseignement spatial tire pleinement profit des révolutions technologiques en cours.

### *A. L'ESPACE, NOUVEL ELDORADO DU RENSEIGNEMENT*

Le renseignement spatial couvre un champ très large qui concerne tout à la fois notre capacité à surveiller la Terre depuis l'espace et l'espace depuis la Terre. Les progrès technologiques rendent aussi désormais possible l'observation de l'espace depuis l'espace, ouvrant la voie à une arsenalisation de l'espace.

#### 1. Observer la Terre depuis l'espace

L'acquisition du renseignement depuis l'espace présente un intérêt majeur dans la mesure où le recueil d'informations peut s'opérer de manière très discrète, sans la moindre entrave liée à la souveraineté des frontières. La surveillance de la Terre depuis l'espace peut se faire soit par le recueil d'images, soit par des écoutes électromagnétiques.

*a) Le renseignement d'origine image (ROIM)*

S'agissant du recueil d'images, il faut distinguer les capteurs optiques des capteurs radar.

Grâce au programme civil SPOT initié dans les années 1980 et développé par le CNES, la France dispose d'un savoir-faire d'excellence en matière d'imagerie optique. Notre pays a été pionnier en Europe dans la reconnaissance spatiale militaire. SPOT fut à l'époque de son lancement le premier satellite, non américain ou soviétique, à prendre une image de la Terre ; ses clichés furent les premiers à faire l'objet d'une commercialisation.

L'expertise acquise par le CNES grâce au programme civil SPOT a permis le développement de programmes militaires dont la dimension duale est évidente. La famille de satellites de reconnaissance militaires HELIOS

trouve en effet son origine dans le programme SPOT. Les satellites HELIOS sont aujourd'hui en fin de cycle ; seuls les deux satellites HELIOS II sont encore opérationnels, *****. Les programmes HELIOS I et HELIOS II ont été ouverts à des partenaires (l'Espagne et l'Italie pour HELIOS I ; l'Espagne, l'Italie, la Belgique et la Grèce pour HELIOS II), la participation financière de ces nations partenaires aux programmes *****. Le Centre satellitaire de l'Union européenne de Torrejon utilise également ces satellites.

La nouvelle génération de satellites de reconnaissance optique est dénommée CSO (Composante Spatiale Optique). Dédiée à l'observation spatiale, CSO est une constellation de trois satellites faisant partie du programme d'armement français MUSIS (*Multinational Space-based Imaging System*). Le premier satellite a été lancé en 2018 ; le deuxième aurait dû l'être en avril 2020[1] tandis que le troisième le sera en 2022. Cette nouvelle génération de satellites offre des performances technologiques très supérieures à HELIOS en améliorant sensiblement l'imagerie délivrée et la qualité du renseignement produit. CSO est en mesure de fournir un nombre conséquent de prises de vue en un seul survol sur une même zone géographique.

Néanmoins, quelles que soient les avancées technologiques, l'imagerie optique a ses limites, qui sont liées aux conditions météorologiques. Il n'est en effet pas possible d'observer la Terre sous une couche nuageuse, ce que seuls les radars permettent. Aussi, la France a conclu des accords bilatéraux avec l'Italie en 2001 (accord de Turin) et l'Allemagne en 2002 (accord de Schwerin) afin d'avoir accès aux moyens radars COSMO-SkyMed italien et SAR-Lupe allemand, en échange d'images HELIOS et CSO.

*b) Le renseignement d'origine électromagnétique (ROEM)*

La collecte du renseignement électromagnétique revêt une dimension stratégique qui a conduit le CNES à mettre au point des démonstrateurs dans le cadre du programme ELISA (*Electronic Intelligence by Satellite*), développé pour le compte de la DGA *****. L'interprétation combinée des mesures des signaux effectuées par satellite permet de localiser et de caractériser les radars.

Ces quatre satellites ont été placés en orbite en décembre 2011. Ce sont des démonstrateurs qui permettent de fixer le cadre du programme opérationnel CERES (capacité d'écoute et de renseignement électromagnétique spatial) *****. Le lancement du premier de ces trois satellites est prévu au cours de cette année 2020.

*Airbus Defence and Space* fournit les satellites et *Thales Alenia Space* la charge utile. Le coût du programme est estimé à 400 millions d'euros.

[1] *Le lancement a été reporté en raison de la crise sanitaire liée au coronavirus.*

### 2. Surveiller l'espace depuis la Terre

L'observation de l'espace depuis la Terre peut se faire à partir de radars ou de télescopes. La surveillance de l'espace vise à pouvoir caractériser et identifier les objets dans l'espace, en se dotant de la capacité d'attribuer, le cas échéant, des actes hostiles commis dans l'espace.

*a) Le système GRAVES développé par l'ONERA*

Entré en service opérationnel en 2005, le système de surveillance de l'espace GRAVES (grand réseau adapté à la veille spatiale) détecte les objets en orbite basse, entre 400 et 1000 km d'altitude. Il est constitué d'un système radar fixe implanté sur deux sites, qui observent les cibles traversant le ciel.

Développé par l'ONERA dans les années 2000, le système GRAVES permet de suivre quotidiennement et de cataloguer plus de 3 000 objets spatiaux en orbite basse. Faute d'industriel intéressé, l'ONERA a développé GRAVES à titre de démonstrateur, pour un coût relativement modeste – environ 30 millions d'euros – au regard de son intérêt stratégique. Cependant, le radar GRAVES ne permet pas de détecter cette nouvelle génération de nano satellites.

Pour pouvoir le faire il faudrait disposer d'une autre technologie et totalement changer le système. Dans son discours de présentation de la stratégie spatiale de défense, le 25 juillet 2019 sur la Base aérienne 942 de Lyon, la ministre des armées, Mme Florence Parly, a indiqué que « *le successeur de Graves devra être conçu pour déceler des satellites de la taille d'une boîte de chaussures à une distance de 1500 kilomètres* ».

C'est ce à quoi s'emploie l'ONERA qui s'est lancée dans la refonte du système GRAVES, dans le cadre d'un contrat pour la DGA. L'objectif est de garantir son fonctionnement jusqu'en 2030, tout en améliorant certaines de ses performances. Pour détecter des satellites de plus en plus petits, le successeur de GRAVES devra s'appuyer sur une fréquence de détection plus élevée, en fonctionnant dans le domaine UHF.

*b) Les télescopes*

Pour la surveillance des satellites en orbites moyennes et géostationnaires les armées s'appuient sur le réseau TAROT (Télescopes à Action Rapide pour les Objets Transitoires) du CNRS et sur le système GEOTracker d'ArianeGroup.

Pour bénéficier d'informations sur les satellites se trouvant en orbite à 36 000 km de la terre, le Commandement de l'espace a en effet signé un contrat avec ArianeGroup pour bénéficier des données recueillies par son réseau mondial d'observation GEOTracker.

Le système GEOTracker est le fruit de dix années de travaux. Il repose sur six télescopes basés au Chili, en Espagne, en France et en Australie afin de couvrir l'ensemble de l'orbite géostationnaire.

### 3. Surveiller l'espace depuis l'espace

L'existence mise à jour en 2018 d'un satellite effectuant du recueil de renseignement russe s'approchant de satellites appartenant à différents pays, dont le nôtre, a accéléré la prise de conscience de l'urgence à se doter de moyens de surveillance de l'espace depuis l'espace. La surveillance de l'espace depuis l'espace représente sans nul doute aujourd'hui la nouvelle frontière du renseignement spatial. Thales Alenia Space a ainsi investi dans le premier projet civil de l'espace depuis l'espace : un projet canadien dénommé « *North Space* ».

S'agissant du volet militaire, comme cela a été rappelé par la ministre des Armées dans son discours du 25 juillet 2019 sur la présentation de la stratégie spatiale de défense, les moyens de gêner, neutraliser ou détruire les capacités spatiales adverses existent et ils se développent à travers des satellites espionnés, brouillés, ou encore éblouis.

Dans ce contexte, la ministre a estimé nécessaire que la France se dote de nano-satellites patrouilleurs dès 2023.

Les missions de ces nano-satellites seront :

- *****  ;

- *****.

L'échéance de 2023 est très ambitieuse, certaines technologies n'étant pas encore disponibles. Elle est néanmoins atteignable à condition de mettre en place un dispositif de développement et de production suffisamment agile et intégré. Pour tenir le calendrier d'un lancement d'ici à la fin de l'année 2023, c'est l'ensemble de la chaine des acteurs qu'il convient de mobiliser autour de cet objectif stratégique, en privilégiant le développement, la production et la mise en orbite de nano-satellites « démonstrateurs opérationnels ».

## *B. L'OBSERVATION SPATIALE AU SERVICE D'INTÉRÊTS STRATÉGIQUES*

L'observation de l'espace sert de multiples finalités à commencer par la connaissance de l'état de l'espace où les débris sont de plus en plus nombreux. La collecte de renseignements depuis l'espace est également stratégique en appui des opérations militaires au sol tandis que l'espace devient à son tour le théâtre de manœuvres d'espionnage.

### 1. La connaissance de l'état de l'espace

D'ici une dizaine d'années, le nombre de satellites qui graviteront autour de la Terre devrait pratiquement quintupler, passant de 1 500 aujourd'hui à près de 7 000, avec la mise en orbite de plus en plus fréquente de constellations de nano-satellites.

La fonction « connaissance de l'espace » répond à trois besoins distincts :

- l'évaluation des menaces que des systèmes spatiaux adverses peuvent faire peser sur nos satellites, sur notre territoire ou sur nos forces déployées ;

- la prévention des risques de collision dans l'espace ;

- la coordination avec les autres acteurs de l'espace, notamment en matière de brouillage involontaire.

Il existe aujourd'hui un très grand nombre de débris spatiaux. Selon le CNES, on estime à 23 000 le nombre d'objets suivis dont la taille est supérieure à 10 cm. Seulement 5 % de ces débris sont actifs et la plupart se situent en orbite basse.

Mais si l'on considère les débris de plus petite taille, les chiffres sont nettement plus importants : il y aurait au-dessus de nos têtes 35 000 objets compris entre 1 et 10 cm et environ 35 millions de débris intérieurs à 1 cm.

Le trafic spatial est surveillé depuis la base aérienne 942 de Lyon Mont-Verdun, où se trouve le Centre opérationnel de surveillance militaire des objets spatiaux (Cosmos). Ce centre contrôle près de 4 000 objets par jour, toutes altitudes confondues. 85 % sont des débris, des pièces de fusées ou des satellites en fin de vie, susceptibles de détruire un satellite en cas de collision.

Dans l'espace, chaque collision d'objets peut déclencher une cascade d'accidents ; c'est ce qu'on appelle le « syndrome de Kessler », du nom du scientifique américain Don Kessler qui a montré, à la fin des années 1970 qu'il pouvait exister un phénomène de collisions en chaîne entre objets spatiaux, chaque collision créant des débris susceptibles d'aller détruire d'autres objets en orbite, provoquant l'apparition de nouveaux débris, *etc.*

Le risque de collision pourrait également être renforcé par l'effet du réchauffement climatique. En effet, quand l'atmosphère se réchauffe, la densité de ses couches supérieures diminue. À 300 kilomètres d'altitude, elle s'amenuise d'environ 5 % chaque décennie, estiment des scientifiques de l'université de Southampton, Hugh Lewis et Graham Swinerd. Moins freinés, les satellites mais aussi les débris orbitaux sont donc susceptibles de rester plus longtemps en orbite.

Deux problématiques principales sont associées à l'évolution de la pollution spatiale, très différentes l'une de l'autre. Il s'agit, d'une part, des rentrées aléatoires dans l'atmosphère et, d'autre part, des risques de collision pour les satellites actifs et les vols habités.

Ce ne sont pas là des risques théoriques puisque, par exemple, un satellite de la constellation SpaceX a contraint le 2 septembre 2019 un satellite de l'Agence spatiale européenne (ESA) à changer légèrement de trajectoire pour réduire le risque de collision. L'évitement fait en effet partie des moyens mis en œuvre pour éviter une collision.

Dans ce contexte, pouvoir disposer d'une cartographie exhaustive de l'espace est essentiel pour prévenir les risques de collision. Les États-Unis fournissent ainsi gratuitement à tous les opérateurs de satellites des alertes en cas de risques de collision. Mais cette dépendance aux États-Unis n'est pas satisfaisante. Le monde entier dépend en effet des données transmises par les Américains à travers le catalogue des objets spatiaux qu'ils mettent à disposition, avec pour chacun d'entre eux des données orbitographiques plus ou moins précises. Ces informations nous sont indispensables dès lors que nous ne suivons, avec nos seuls moyens propres, environ dix fois moins d'objets en orbite que les États-Unis.

### 2. L'appui aux opérations militaires

Pendant la première guerre du Golfe (1990-1991), 98 % du renseignement image était fourni par les États-Unis.

La « Stratégie spatiale de défense » présentée en 2019 souligne la fonction stratégique que représente le renseignement d'origine spatiale pour l'appui aux opérations et la nécessité de garantir notre indépendance.

Au sein de la communauté du renseignement, cette fonction incombe à la direction du renseignement militaire (DRM) qui assure le contrôle opérationnel des charges utiles de nos satellites d'observation et d'écoute, hiérarchise les demandes de prises de vues pour assurer la satisfaction des besoins prioritaires des utilisateurs et analyse les images à des fins de renseignement *via* le Bureau capacité stratégique interarmées (BCSI) de la DRM.

L'appui aux opérations est un domaine d'intérêt vital pour nos armées. La conduite d'opérations militaires de grande envergure ne peut plus se dérouler sans l'apport des satellites, indispensables pour se projeter, connaître son théâtre d'opération, recueillir du renseignement, surveiller et naviguer. Les armées observent et écoutent depuis l'espace. Situé principalement sur la base aérienne 110 de Creil, le Centre militaire d'observation par satellites (CMOS) a ainsi pour mission de garantir l'accès permanent du ministère des Armées à l'imagerie spatiale.

Pour planifier efficacement, il faut disposer d'informations sur des régions dont le libre accès n'est pas garanti tout en préservant une certaine discrétion. Capables de recueillir des données en tout point du globe, sans contraintes juridiques, les capteurs spatiaux permettent d'analyser l'évolution des crises sans dépendre d'un quelconque partenaire étranger. Cette autonomie d'analyse contribue aux prises de décisions qui engagent notre pays.

L'espace participe également à la mise en œuvre des armements. Le système de navigation par satellites GPS permet la localisation précise des objectifs en mouvement. Le terrain situé dans l'environnement des objectifs fixes est numérisé à partir de prises de vue satellites : ces informations permettent d'assurer le guidage d'armes de précision.

Enfin, nos capacités de surveillance de l'espace contribuent discrètement à la protection des forces engagées en les renseignant notamment sur les moyens satellitaires dont dispose l'adversaire. À terme, la composante spatiale du système d'alerte avancée permettra à nos forces de prendre, si nécessaire, les mesures adaptées face à la menace que représentent les missiles balistiques.

L'espace est devenu aujourd'hui un fournisseur formidable et indispensable de moyens au profit des opérations.

### 3. L'espionnage et le contre-espionnage

En septembre 2018, dans son discours prononcé au Cnes sur les enjeux de l'espace pour la Défense, Florence Parly, ministre des Armées françaises révélait que le satellite russe Louch-Olymp avait été surpris à proximité immédiate du satellite de télécommunications militaires franco-italien Athena-Fidus, vraisemblablement pour tenter d'en intercepter les communications cryptées.

L'observation des manœuvres de ce satellite russe à proximité de près d'une dizaine d'autres satellites appartenant à différents pays a mis en évidence la réalité d'une utilisation de l'espace à des fins de renseignement.

Ces manœuvres d'approche d'un satellite par un autre satellite peuvent servir à recueillir du renseignement (écoutes et prises de vues) ou mener des actions plus offensives et réversibles comme le brouillage ou l'éblouissement, ayant pour effet de neutraliser un satellite. Sur l'arc géostationnaire, de telles opérations sont réalisables sans difficulté excessive et plusieurs pays disposent des capacités et des compétences requises pour les conduire.

Ainsi, cette forme de recueil de renseignement spatial pourrait se développer à travers des cyberattaques susceptibles d'accéder aux données du satellite, voire de rendre inopérants ou brouiller ses capteurs. Le risque n'est donc pas véritablement celui de la destruction d'un satellite, en ce sens

où les milliers de débris générés deviendraient également une menace pour la flotte de satellites de l'attaquant.

C'est pourquoi il est essentiel de disposer d'une capacité d'identification et de caractérisation de ces manœuvres hostiles, ou pour le moins inamicales ; en d'autres termes, il faut pouvoir attribuer les actes hostiles que nous subissons.

### *C. LES RÉVOLUTIONS EN COURS DU RENSEIGNEMENT D'ORIGINE SPATIALE*

En quelques années, les progrès technologiques ont profondément et durablement changé la donne du renseignement d'origine spatiale. Très haute résolution, miniaturisation, mise en orbite de constellations, développement de l'intelligence artificielle : de véritables révolutions sont à l'œuvre qui viennent élargir considérablement le champ des possibles.

#### 1. Mieux voir (la très haute résolution)

Il y a vingt ans, le satellite SPOT 4 pesait plus de deux tonnes et offrait résolution couleur de 20 mètres. En quelques années, les progrès technologiques ont été considérables puisque les nouveaux satellites proposent une résolution permettant de photographier depuis l'espace des objets de la taille d'une boîte de chaussures et pouvant même aller jusqu'à quelques centimètres de résolution.

Ces nouvelles performances en matière de très haute résolution valent tant pour l'imagerie optique que radar.

En matière d'imagerie optique, de nouveaux concepts de télescopes sont en développement, équipés de miroirs segmentés et déployables, avec des structures considérablement allégées. La technique de l'hyperspectral est également développée pour détecter non pas seulement ce qui est visible et en surface, mais également la nature des matériaux, la classification des sols, la détection de gaz, d'anomalies spectrales, *etc.*

Dans le domaine de l'imagerie radar, la très haute résolution se décline autour de la 3D et du recours à l'interférométrie pour la détection d'activité tels que les passages de véhicules et les activités humaines.

Cette très haute résolution témoigne de la valeur ajoutée des satellites militaires d'observation au regard de l'offre commerciale qui existe dans le secteur civil. Elle procure à notre pays une avance technologique qu'il s'agit de conforter dans un secteur de plus en plus stratégique et concurrentiel.

### 2. Voir plus souvent (constellations et taux de revisite)

Il ne s'agit pas seulement de voir de mieux en mieux, mais aussi de disposer d'une capacité d'observation la plus continue possible. L'amélioration du taux de revisite, c'est-à-dire la fréquence d'actualisation des images, est en effet au cœur des programmes de développement des nouvelles générations de satellites.

La mise en orbite de constellations permet ainsi d'optimiser le taux de revisite en tout point du globe.

Par rapport aux satellites HELIOS II, les trois nouveaux satellites CSO vont permettre aux armées de disposer d'un système agile capable d'enchaîner les prises de vues sur une zone de crises. À l'instar du système PLÉIADES développé par Airbus, CSO permettra d'accroître le nombre d'objectifs pouvant être imagés sur un théâtre géographiquement restreint en un seul passage et ainsi de satisfaire un maximum de besoins opérationnels. La constellation CSO offrira en outre une meilleure revisite améliorant le suivi des objectifs d'intérêt et la détection de changement. En contact toutes les 90 minutes en moyenne avec chaque satellite CSO, la station polaire de Kiruna est un élément clé du système pour s'adapter à la temporalité des opérations et actualiser l'information le plus souvent possible. La programmation de CSO s'effectue ainsi selon trois degrés de priorité, le niveau « très prioritaire » garantissant l'accès aux théâtres d'opération.

Les industriels développent leurs offres commerciales fondées sur une amélioration des taux de revisite, qu'il s'agisse d'Airbus grâce à un système de relais de données SpaceDataHighway ou de Thales Alenia Space avec la constellation de Spaceflight Industries (BlackSky) avec qui l'entreprise a noué un partenariat industriel et commercial.

Il s'agit, pour exister dans un secteur industriel de pointe mais de plus en plus concurrentiel, d'être en capacité de proposer des offres combinant des satellites de très haute résolution avec des constellations de satellites moins résolus mais bénéficiant de hautes capacités de revisite, de l'ordre de plusieurs dizaines par jour.

### 3. La miniaturisation

Le marché des nano satellites est en pleine expansion. La réduction de la taille des satellites permet en effet à la fois de rationaliser les coûts de production mais surtout de mise en orbite grâce à un poids bien inférieur à celui des satellites d'observation traditionnels. A travers la miniaturisation, Il s'agit également de diminuer l'énergie consommée dont la production peut mobiliser jusqu'à 30 % de la masse d'un engin spatial.

De dimension beaucoup plus compacte et avec un poids inférieur à 10 kilogrammes, les nano satellites offrent des résolutions d'image bien supérieures aux anciennes générations. C'est un nouveau modèle industriel qui se développe dans un secteur jusqu'alors très fermé et très peu concurrentiel. Cette nouvelle approche permet de produire des satellites en série et d'optimiser les coûts comme de faire évoluer rapidement les générations de matériels. Le faible coût d'infrastructure incite désormais des investisseurs privés, non issus du secteur spatial, à investir dans ce domaine d'activités.

### 4. L'intelligence artificielle

L'amélioration continue du niveau de résolution des images, associée à l'augmentation du taux de revisite grâce à la mise en orbite de constellations provoque une hausse considérable du nombre de données disponibles. Des acteurs privés, à l'instar des GAFA, mettent sur le marché des offres commerciales de plus en plus nombreuses qui ont pour effet de démocratiser l'accès aux données issues de l'espace.

Dans ces conditions, les capacités de recueil et d'exploitation des données sont absolument centrales. Car la donnée brute présente un intérêt très limité ; il faut être capable de la traiter, d'en extraire la valeur ajoutée, ce qui suppose de développer des systèmes d'exploitation et des services associés.

L'exploitation « intelligente » des images ou archives d'images suscite ainsi l'intérêt grandissant d'acteurs dont le modèle économique repose essentiellement sur la valorisation des données issues de l'observation spatiale. Cette approche donne lieu au développement de partenariats avec des entreprises bénéficiant des savoir-faire dans le domaine de l'intelligence artificielle susceptibles de valoriser l'offre commerciale des entreprises spatiales. Il existe là un marché dual très prometteur qui repose notamment sur la mise au point d'algorithmes permettant de faire le tri face à l'augmentation sans fin du nombre de données collectées.

Cette exploitation des données représente un défi majeur pour la communauté du renseignement. Les services de renseignement doivent en effet gérer un volume d'images de plus en plus important. *****.

La question des données soulève un sujet de souveraineté nationale, qu'il s'agisse de la constitution de bases de données souveraines issues de l'observation spatiale, de la mise au point d'outils d'exploitation et de transformation des données collectées.

## II. LA SOUVERAINETE SPATIALE FRANCAISE A LA CROISEE DES CHEMINS

*Les développements qui suivent ne concernent pas directement le sujet du renseignement mais permettent d'appréhender les conséquences pour le monde du renseignement des révolutions en cours au sein d'un secteur industriel stratégique pour l'exercice de notre souveraineté.*

Depuis la fin de la seconde guerre mondiale et jusqu'à une période récente, la maîtrise de l'espace fut le pré carré de quelques grands pays et un attribut évident de puissance, et donc de souveraineté, dans le concert des nations. Ce privilège de souveraineté se trouve aujourd'hui mis à mal par l'émergence du « *New Space* » qui rebat totalement les cartes. Ce changement de paradigme nous contraint à nous adapter plus rapidement que prévu et à porter un regard lucide tant sur les forces que sur les fragilités de l'écosystème spatial française et européen.

### *A. LES RÉVOLUTIONS DU « NEW SPACE »*

Le « *New Space* » est né aux États-Unis il y a une dizaine d'années. Il résulte d'une part, de la numérisation de l'économie et d'autre part, de l'émergence de nouveaux acteurs, aussi bien d'entreprises privées que d'États qui ne s'estimaient jusqu'alors pas concernés par les affaires spatiales.

Le « *New Space* » se conçoit en opposition avec ce qu'il convient de facto d'appeler le « *Old Space* », à savoir l'industrie spatiale telle qu'elle existait jusqu'à présent autour d'acteurs limités à quelques grandes puissances – d'abord, historiquement les États-Unis et l'URSS – poursuivant des objectifs essentiellement politiques et stratégiques. A cet égard, le « *New Space* » s'apparente à une redéfinition des possibles, qu'il s'agisse des acteurs ou des usages.

Contrairement à ce qu'il suggère, le terme de « *New Space* » ne désigne pas un renouveau mais une ouverture de l'espace à de nouveaux acteurs et un redéploiement des technologies spatiales vers des champs d'application jusqu'alors inexplorés. Il est une résultante de la digitalisation de l'économie comme de nos sociétés. L'essor du « *New Space* » est souvent comparé à celui d'internet dans les années 2000 parce qu'il a recours à des méthodes, des technologies, des équipements et une ingénierie financière (capital-risque) développée par la « nouvelle économie » : miniaturisation, électronique, impression 3D, intelligence artificielle, *etc*.

Ainsi, le « *New Space* » est l'extension au secteur spatial de logiques économiques et industrielles qui ne lui étaient jusqu'à présent étrangères. Il

entraîne ainsi le décloisonnement du domaine spatial traditionnel, le propulsant en quelque sorte dans l'ère industrielle et concurrentielle.

### 1. Standardisation et baisse des coûts

L'écosystème du « *New Space* » est en grande partie fondé sur la miniaturisation des composants. Alors qu'on ne fabriquait autrefois que de gros satellites, avec de couteuses pièces construites spécifiquement pour l'environnement spatial, on développe désormais de plus petits engins à partir de composants provenant de l'électronique grand public ou du secteur automobile. Le développement d'un marché des nano-satellites permet désormais à de nouveaux acteurs d'acquérir leurs propres satellites, les coûts de lancement et de mise en orbite payés par les clients dépendant avant tout du poids de la charge utile à transporter. De plus petits satellites, ce sont des satellites plus légers, donc moins chers. Cela permet également de transporter plus de satellites à la fois : l'Inde a, par exemple, en début d'année, mis en orbite 104 satellites en un seul lancement.

### 2. Multiplication des usages

Le « *New Space* » ouvre des horizons nouveaux quant aux usages issus des données de l'espace, au-delà des seuls objectifs stratégiques et politiques poursuivis jusqu'alors par les grandes puissances.

Le phénomène n'est pas si nouveau. Dès les années 80, l'économie spatiale n'est plus simplement une affaire militaire mais devient aussi un enjeu commercial comme en témoigne l'émergence de la télévision par satellite et le GPS américain.

L'économie du « *New Space* » fait de la donnée spatiale un produit à forte valeur ajoutée. Pour rentabiliser les investissements consentis, elle doit être immédiatement disponible et utilisée pour une très grande variété d'applications et de services commerciaux, y compris dans des domaines jusqu'ici réservés aux acteurs gouvernementaux, tels que la recherche scientifique ou l'exploration spatiale.

Les données spatiales sont ainsi appelées à irriguer de plus en plus des pans entiers de l'économie et rendent nos modes de vie de plus en plus dépendants des informations issues de l'observation spatiale.

Quelques exemples concrets illustrent cette réalité. Ainsi, le système EGNOS est utilisé par de plus en plus d'agriculteurs pour la navigation satellite et l'agriculture de précision, tandis que Copernicus permet le suivi des cultures et des récoltes. Dans le secteur aérien, le même système est utilisé dans 350 aéroports en Europe pour la gestion des atterrissages en conditions météo difficiles.

Ce sont également les images prises par Copernicus qui ont permis d'aider les secours à intervenir plus efficacement lors de catastrophes naturelles.

En matière de sécurité routière, Galileo est depuis 2018 intégré à tous les nouveaux véhicules compatibles pour servir de système d'appel d'urgence et permet également désormais de surveiller les temps de conduite des chauffeurs de poids lourds.

### 3. Multiplication des acteurs

L'intensité capitalistique des activités spatiales a longtemps créé des barrières à l'entrée d'un marché jusqu'alors réservé à quelques grandes puissances, mettant le secteur tout entier à l'abri de nouveaux entrants. Les grandes nations européennes avaient ainsi été contraintes de se coordonner pour parvenir à créer leur propre industrie spatiale.

Le creuset du « *New Space* » réside dans multiplication des « start-ups » spatiales américaines qui ont pour ambition de révolutionner le marché spatial. Ainsi sont apparues aux côtés des géants du secteur aérospatial comme Boeing ou Lockheed Martin une multitude d'entreprises souhaitant abaisser le prix de l'accès à l'espace en cassant les coûts. La plus célèbre d'entre elles est la société SpaceX, avec son lanceur Falcon 9.

Mais le « *New Space* » se traduit également par l'arrivée dans l'économie spatiale d'acteurs plus « périphériques », issus de la Silicon Valley et des Gafa (Google, Apple, Facebook, Amazon). Ces nouveaux entrants dans un secteur d'activité qui était jusqu'alors réservé aux États et Institutions publiques font bénéficier le spatial traditionnel d'innovations et de technologies issues d'autres secteurs tels que le numérique, le *big data* ou l'aéronautique.

L'apparition de nouveaux acteurs ne concerne pas que le secteur privé. L'abaissement des coûts et la démocratisation de l'accès à l'espace qui en découle permet désormais à des États d'entrer dans le club des nations présentes dans cette communauté de moins en moins fermée. C'est ainsi que la Pologne en 2015 et le Luxembourg en 2018 ont créé leur propre agence spatiale.

Pour les pays en développement, l'avènement du « *New Space* » est aussi une opportunité inédite dans l'histoire de la conquête spatiale pour accéder et utiliser l'espace à bon compte. C'est aussi un moyen d'affirmation politique, comme en témoigne, en Asie, la course à l'espace qui n'est pas sans lien avec les relations politiques régionales.

### *B. NOS FORCES FACE AU « NEW SPACE »*

La France fait partie des rares pays au monde à maîtrise l'ensemble des compétences et technologies spatiales. C'est à la fois le fruit de notre Histoire et la démonstration d'une excellence scientifique et industrielle qui reste un atout de taille de l'univers du « *New Space* ».

#### 1. Notre avance historique

La politique spatiale de la France est née avec la Cinquième République et les premiers pas de notre conquête spatiale furent motivés par une forte ambition nationale, impulsée par le général De Gaulle. Conséquence de la course à l'espace lancée par les soviétiques et les américains en pleine guerre froide, De Gaulle décide en effet dès janvier 1959 de créer un Comité de recherches spatiales (CRS) chargé d'étudier le rôle que la France peut et doit jouer dans ce nouveau domaine.

Notre programme spatial, d'abord national avant de devenir également européen, va ainsi bénéficier d'investissements importants à compter des années 1960 dans le but d'atteindre une autonomie nationale.

Afin de fournir une structure chargée de développer et de coordonner les activités spatiales françaises, le Gouvernement de Michel Debré annonce la création, le 19 décembre 1961, du Centre national d'études spatiales (CNES). Suivra le 26 novembre 1965 le lancement d'Astérix, le premier satellite artificiel français, à l'aide de la fusée nationale Diamant-A. Il s'agissait alors pour la France, et au-delà pour les Européens, de ne pas se laisser distancer par les Américains et les Soviétiques.

Cette volonté permettra à notre pays de jouer un rôle moteur au moment de la mise en œuvre d'une véritable politique spatiale européenne. Celle-ci commence tôt, dès 1964, quand six pays – l'Allemagne, la Belgique, la France, l'Italie, les Pays-Bas et le Royaume-Uni – fondent la première organisation spatiale chargée de développer des lanceurs : l'ELDO. Puis, avec le Danemark, l'Espagne, la Suède et la Suisse, ces mêmes pays créent une organisation pour assurer le développement de satellites scientifiques : l'ESRO. Ainsi, dès le début, science et lanceurs sont les deux piliers de la stratégie spatiale européenne.

En 1975 sera signée entre onze États européens la convention portant création de l'Agence spatiale européenne (ESA) qui prendra en charge le développement d'Ariane, le lanceur européen. Le vol inaugural du lanceur Ariane 1, le 24 décembre 1979, a permis à l'Europe d'acquérir son autonomie et d'occuper une place significative sur le marché mondial du spatial, en réalisant plus de la moitié des lancements commerciaux dans le monde. La localisation à Kourou en Guyane, en territoire français, du pas de tir d'Ariane fut décisive pour notre avance dans le domaine des lanceurs.

Cette ambition politique portée depuis l'après-guerre avec constance au plus haut niveau de l'État a permis à la France de devenir et de rester l'une des grandes puissances spatiales mondiales avec les États-Unis et la Russie.

La France est ainsi le seul pays européen à maîtriser l'ensemble des technologies spatiales. Notre pays est en effet un acteur de rang mondial dans des domaines aussi variés que les systèmes de lancement, les satellites d'observation optique, les satellites météorologiques, les satellites scientifiques ou encore les satellites de télécommunication. Ce succès national repose sur un modèle original autour d'une agence spatiale, le CNES, d'un organisme de recherche, l'ONERA et d'un secteur industriel qui peut s'appuyer sur des investissements majeurs consentis par l'État.

### 2. Notre excellence scientifique

Pour conserver son avance historique, notre pays doit continuer à investir massivement dans la recherche. La filière spatiale française tout entière repose en effet sur cette excellence scientifique qui garantit sur le long terme notre position face aux nouveaux acteurs qui émergent du fait du « *New Space* » et de la démocratisation de l'accès aux activités spatiales.

Le ministère de la recherche et de l'innovation est cœur de notre dispositif d'une part, à travers la tutelle qu'il exerce en partage avec le ministère des Armées sur le CNES et d'autre part, en négociant les arbitrages budgétaires liés au Programme 193 (recherche spatiale). Pour sa part, le ministère des Armées, *via* la direction générale de l'armement (DGA) finance et accompagne la recherche spatiale duale (programme 191).

La performance de notre recherche technologique spatiale s'apprécie notamment à travers les succès français enregistrés dans les réponses aux appels d'offre du programme européen « Horizon 2020 ». Pour l'exercice 2016, la France est ainsi arrivée largement en tête en Europe avec un retour de près de 28 % du budget alloué par la commission européenne.

En matière de recherche aéronautique et spatiale, l'Office national d'études et de recherches aérospatiales (ONERA) occupe une place centrale. Ses activités consistent à :

- développer et d'orienter les recherches dans le domaine aérospatial ;

- concevoir, réaliser et mettre en œuvre les moyens nécessaires à l'exécution de ces recherches ;

- assurer, en liaison avec les services ou organismes chargés de la recherche scientifique et technique, la diffusion sur le plan national et international des résultats de ces recherches, d'en favoriser la valorisation

par l'industrie aérospatiale et de faciliter éventuellement leur application en dehors du domaine aérospatial

Près de 300 doctorants sont rattachés à l'ONERA qui compte environ 2000 agents. En liaison avec le CNES, l'ONERA constitue un véritable pont entre la recherche et l'industrie.

La mise au point de « GRAVES », le système de détection de satellites évoluant en orbite terrestre basse, développé par l'ONERA et en service depuis 2005, est une illustration emblématique de l'intérêt stratégique à investir dans la recherche, avec à la clé, un intérêt évident pour la communauté du renseignement.

Bien que peu onéreux - il n'a coûté « que » 30 millions d'euros -, ce système qui a représenté 15 ans d'investissements et d'études a montré son efficacité, en détectant une trentaine de satellites espions principalement américains et chinois jusqu'alors non répertoriés Il s'agissait au départ d'un simple démonstrateur technologique, commandé par la DGA et développé par l'ONERA, qui s'est mué en dispositif opérationnel, le tout utilisant des technologies disponibles dans le commerce, comme des émetteurs de télévision.

Il est plus que jamais essentiel de maintenir cette capacité à innover et à développer des démonstrateurs, en lien avec les industriels, pour conserver ce temps d'avance face à un nombre croissant de pays qui ont désormais des ambitions aéronautiques et spatiales, en particulier à visée de défense.

**Recommandation n° 45 : Soutenir les modes collaboratifs entre la recherche publique et le secteur privé afin de développer les démonstrateurs nécessaires pour conserver notre avance technologique et stratégique.**

Aussi, et pour faire face à ces nouveaux défis, l'État cherche à initier de nouveaux modes collaboratifs entre la recherche publique et les entreprises, à l'instar de la technopole spatiale de Toulouse qui est une référence mondiale avec l'implantation, à côté de deux grands sites industriels (Airbus et Thales), d'un tissu d'ETI et de PME et de plusieurs centres de recherches et de laboratoires qui peuvent s'appuyer sur un creuset de 16 500 étudiants formés au spatial à l'université et dans des écoles qui proposent jusqu'à une centaine de formations différentes.

### 3. Notre excellence industrielle

La filière industrielle spatiale est un fleuron national et européen qui contribue à l'exercice de notre souveraineté. La France compte en effet parmi les rares pays au monde à maîtriser l'ensemble des compétences, de la conception des satellites à leur réalisation, leur lancement et leur

exploitation. Cela confère à notre pays une posture politique d'interlocuteur face aux grandes puissances spatiales.

Notre industrie spatiale se caractérise par un écosystème dual qui représente un atout majeur pour la France. L'espace a en effet d'abord été exploité à des fins militaires avant que ne s'ouvrent des perspectives commerciales, en particulier avec le marché des télécommunications. C'est vrai autant pour la fabrication des satellites pour que les activités de lancement.

Les investissements et la commande publique dans les domaines de la défense et de la sécurité ont rendu possibles les succès commerciaux qui font d'Airbus Space & Defense, de Thales Alenia Space et d'Ariane Group des leaders sur un marché mondial de plus en plus concurrentiel, grâce à l'écosystème de chercheurs et de fournisseurs qui s'est construit autour d'eux.

Le secteur spatial représente aujourd'hui en France près de 16 000 emplois directs et y a réalisé en 2017 un chiffre d'affaires consolidé de 4,6 milliards d'euros. Ce modèle très performant permet à l'industrie spatiale française de présenter cette particularité unique au monde qui est de réaliser près de 60 % de son chiffre d'affaires sur le seul secteur commercial, alors que ses concurrents sont partout ailleurs majoritairement financés par les États pour répondre à leurs besoins institutionnels, en particulier dans les domaines de la défense et de la sécurité.

La composante « renseignement » est un moteur du développement de notre industrie spatiale dont la vitalité est elle-même essentielle à notre souveraineté. Airbus et Thales ont sans aucun doute permis à la France de se donner les moyens de son autonomie dans l'optique et dans l'écoute.

L'industrie spatiale doit être protégée car elle n'est pas tout à fait une industrie comme les autres. Les conséquences économiques de la crise sanitaire liée au Coronavirus vont fragiliser toute une filière qui doit absolument être accompagnée par les pouvoirs publics. L'effectivité de notre souveraineté dépend en effet de la capacité de nos industriels à développer les outils et les technologies indispensables à notre protection. Nos satellites d'observation sont vulnérables, qu'il s'agisse de la structure même du satellite ou des stations au sol pouvant être la cible de virus et logiciels malveillants. On peut également citer le brouillage électronique des satellites, leur aveuglement au laser, voire leur désorbitation par un satellite tiers, ou leur prise de contrôle à distance par des forces ennemies. Pour identifier et cartographier ces menaces dans l'espace, Airbus a par exemple conduit un groupe de travail spécifique sur ces sujets et mené, en partenariat avec la FRS, un exercice sous la forme d'un « jeu de guerre de l'espace » pour simuler un certain nombre de situations ; convaincue qu'un jour se produira un « Pearl Harbour » numérique, et qu'il s'agira d'être en capacité d'y faire face.

### *C. NOS FRAGILITÉS*

Et si nos forces devenaient des faiblesses ? Aussi paradoxal que cela puisse paraître, ce qui a fait l'avance de la France et de l'Europe dans la maîtrise de l'espace se transforme en fragilité dans le contexte du « *New Space* ». Il nous faut relever plusieurs défis qui concernent autant la compétitivité de nos lanceurs dans un secteur de plus en plus concurrentiel, que notre capacité à garantir notre indépendance stratégique et à investir l'économie de la donnée.

#### 1. Une perte de compétitivité : l'exemple des lanceurs (rentabilité v/ souveraineté)

Comme le souligne la stratégie spatiale de défense, « *la conservation de notre autonomie d'accès à l'espace repose bien aujourd'hui sur la pérennité du lanceur européen Ariane dont l'avenir doit passer par une politique de réduction des coûts assumée* ». Notre autonomie d'accès à l'espace repose sur Ariane 5 depuis les années 1990 et sur un modèle mixte, entre lancements commerciaux et institutionnels, pour soutenir un cadencement suffisant. Un lancement d'Ariane 5 coûte environ 200 millions d'euros si l'on prend en compte toutes les subventions d'exploitation, ce qui n'est absolument plus compétitif dans le contexte du « *New Space* ». Le coût d'un lancement avec Ariane est en effet d'environ 30 % supérieur à celui proposé par SpaceX.

Dans ces conditions, les craintes portent sur le programme Ariane 6, confronté à plusieurs difficultés :

- les conditions actuelles du marché n'ont rien à voir avec celles qui existaient en 2014 lors du lancement du programme, du fait du processus de miniaturisation des charges utiles qui permet des lancements à moindre coût puisqu'à moindre poids ;

- Ariane 6 est calibrée pour lancer des satellites en géostationnaire ; or la demande est de moins en moins forte, et ce au profit des constellations en orbite basse ;

- SpaceX est en train d'imposer un nouveau standard mondial avec un seul type de moteur contre trois pour Ariane – ce qui augmente son coût –, un second étage très puissant et un premier étage réutilisable.

Dès lors, quelle que soit la viabilité commerciale d'Ariane 6, le développement d'un lanceur supplémentaire de type « SpaceX » paraît s'imposer pour rester dans la course.

Remplacer purement et simplement Ariane 6 par Ariane Next (replique du Falcon 9 de Space-X) avec une motorisation Prometheus, qui est encore au stade du prototype, induirait un risque considérable en matière d'autonomie stratégique pour la France compte tenu des délais de développement – une dizaine d'années – et de coût, autour de 5 milliards

d'euros. Un tel projet n'aurait en tout état de cause de sens que s'il était porté à l'échelle européenne.

C'est aussi des Européens que pourrait venir le salut de la viabilité commerciale d'Ariane 6, au travers d'un « *Buy European A*ct » pour les lanceurs, à l'image des Américains et de leur « *Buy American Act* ». C'est effectivement par un accroissement de la demande institutionnelle que nous réduirons la dépendance d'Ariane 6 au marché commercial[1] : les commandes institutionnelles représentent environ un tiers des lancements européens contre près des trois quarts pour les États-Unis. Un « *Buy European Act* » permettrait de sécuriser la pérennité d'un lanceur européen.

**Recommandation n° 46 : Afin d'améliorer la compétitivité du lanceur Ariane 6, introduire un « *Buy European Act* » pour garantir un nombre de commandes institutionnelles nécessaires à la viabilité financière et commerciale du programme.**

Il ne doit pas s'agir de renoncer au programme d'Ariane 6, mais d'y ajouter une offre que les Européens ne proposent pas aujourd'hui pour les mises en orbite basse. La France a tout intérêt à la viabilité d'Ariane 6, car il en va de la pérennité du centre de tir de Kourou qui ne se justifie que pour les mises en orbite géostationnaire, les lancements en orbite basse pouvant s'opérer de n'importe où. Quoi qu'il en soit, le maintien de notre capacité en matière de « grands lanceurs » est avant tout une question de souveraineté, et non de rentabilité.

Du point de vue de la rentabilité, l'enjeu pour Ariane c'est donc la diversification de son offre dans le contexte du « *New Space* » qui pourrait passer par le développement d'un lanceur réutilisable dédié aux minisatellites. Dans le cadre du projet Altair porté par l'ONERA, un démonstrateur de drone emportant à 10 000 ou 12 000 mètres d'altitude un petit lanceur classique a ainsi été testé à Kourou en 2019. En plus du drone, réutilisable, au moins un des étages du lanceur serait en outre réutilisable.

### 2. Notre dépendance

Alors que le « *New Space* » rebat les cartes, la souveraineté française dans le domaine spatial se trouve doublement fragilisée, d'une part en raison de notre dépendance, au moins partielle, à l'égard des États-Unis, mais aussi du fait des stratégies nationales observées au sein de l'Union européenne.

*a) A l'égard des États-Unis*

Notre dépendance envers les États-Unis est liée à notre incapacité à disposer seuls d'une connaissance exhaustive de l'état de l'espace. Le Pentagone publie un catalogue des objets spatiaux avec, pour chacun, des

[1] *Ariane 5 est pour sa part dépendante à 75 % du marché commercial.*

données orbitographiques plus ou moins précises. Bien que la France fasse partie des très rares pays au monde capables d'apporter un regard critique sur ces informations grâce aux moyens de surveillance dont nous disposons, nous n'en sommes pas moins dépendants de ce que nos partenaires américains veulent bien nous dire. Les analyses conduites par les armées et le CNES ont déjà permis de mettre en évidence l'absence dans ce catalogue de certaines plateformes américaines et, dans d'autre cas, des trajectoires sensiblement différentes de celles qui y étaient décrites[1].

Les États-Unis fournissent par ailleurs gratuitement à tous les opérateurs de satellites des alertes en cas de risques de collision. L'essentiel des procédures françaises d'anticollision sont fondées sur ces données américaines. Il s'agit d'une réelle dépendance, dont la portée doit toutefois être nuancée compte tenu de la communauté d'intérêts dans laquelle se trouvent tous les opérateurs de satellites. Chacun d'entre eux souhaite en effet se soustraire autant que possible au risque de collision de ses plateformes orbitales, à commencer par les États-Unis qui sont de loin les plus exposés.

Disposer de nos propres capacités de moyens de surveillance et d'analyse est essentiel dans l'exercice de notre souveraineté. Il ne s'agit pas seulement de pouvoir acheter des images à nos partenaires, encore faut-il être en mesure de garantir leur intégrité, ce qui suppose une forme de traçabilité en amont.

**Recommandation n° 47 : Mettre fin à notre dépendance à l'égard des États-Unis en nous dotant de capacités propres – *a minima* européennes sinon nationales – d'observation et d'analyse de la situation de l'eEspace et lancer un programme français de développement d'un nouveau système plus performant de surveillance de l'espace pour succéder au démonstrateur GRAVES.**

On a en effet pu constater par le passé combien la « guerre des images » pouvait emporter des décisions historiques. Ainsi en a-t-il été de la réunion du conseil de sécurité d'octobre 1962 au cours de laquelle les Américains avaient apporté la preuve en images que les Soviétiques installaient des missiles à Cuba. Plus récemment, en 2003, on se souvient que le secrétaire d'État américain Colin Powell avait accusé l'Irak de cacher des armes prohibées et de tromper les inspecteurs de l'Onu, lors d'un réquisitoire très sévère devant le Conseil de sécurité, étayé par des bandes sonores et de nombreuses photos satellite. Or les services de renseignement français, disposant de leurs propres images, avaient pu éclairer les plus hautes autorités de l'État sur la véracité des affirmations américaines ; ce qui ne fut pas sans conséquences sur la politique étrangère et de défense de notre pays.

*1* *****

Avec le « *New Space* », notre dépendance aux États-Unis s'analyse également au regard des acteurs privés américains et de leur position émergente ou déjà dominante. Qu'il s'agisse de nouveaux entrants dans l'industrie spatiale, comme Space X ou Blue Origin, ou des GAFA qui multiplient les projets d'intérêt spatial :

- Facebook envisage de lancer son propre satellite, dénommé ATHENA, permettant d'offrir un accès Internet haut débit aux communautés en développement non desservies et mal desservies dans le monde ;

- Google a lancé son initiative « *Project Loon* », visant à utiliser des ballons solaires pour diffuser internet dans les foyers, les entreprises et les appareils personnels dans les régions du monde dépourvues d'infrastructure à haut débit ;

- Amazon se lance aussi dans course avec le projet Kuiper. Dans le cadre de cette nouvelle initiative, le géant de la vente en ligne enverrait 3 236 satellites en orbite basse afin de fournir un accès à Internet aux populations qui en sont privées aujourd'hui.

*b) Entre Européens*

En matière de coopération spatiale européenne, l'Allemagne et l'Italie sont les deux principaux partenaires de la France.

Cette coopération prend la forme d'accords bilatéraux : l'accord de Turin conclu en 2001 avec l'Italie et l'accord de Schwerin conclu en 2002 avec l'Allemagne. Ces accords prévoient des échanges d'images d'observation spatiale radars (fournies par l'Allemagne et l'Italie) et optiques (fournies par la France). Cette spécialisation s'est fondée sur une complémentarité autour d'un partage des coûts et d'une mutualisation des capacités. Dans ces conditions, la France a renoncé à développer une capacité propre en matière d'imagerie radar.

Or, conscients qu'un service de renseignement crédible ne peut aujourd'hui se passer d'une capacité d'imagerie optique, le BND allemand a récemment obtenu de développer un système autonome d'imagerie optique. Cela traduit outre-Rhin une volonté de rattrapage, voire même de dépassement dans le domaine technologique. A l'actuelle dépendance mutuelle, facteur de stabilité, risque désormais de se substituer une dépendance unilatérale de la France à l'égard de l'Allemagne sur l'imagerie radar.

**Recommandation n° 48 : Développer une capacité autonome d'imagerie radar.**

Ce changement stratégique opéré unilatéralement par notre partenaire allemand interroge en termes de gouvernance européenne. Il confirme la rivalité stratégique, technologique et industrielle qui se fait de plus en plus prégnante dans la relation bilatérale franco-allemande et pose

sérieusement la question du développement d'une capacité d'observation spatiale par imagerie radar en France.

### 3. L'exploitation des données

Le domaine de la donnée est en train de vivre une véritable révolution et le secteur spatial n'échappe pas à cette transformation que les dynamiques du « *New Space* » viennent accélérer.

Le progrès technologique, associé à l'augmentation considérable du nombre de satellites placés en orbite a pour effet de démultiplier la quantité de données disponibles. Selon Jean-Marc Nasr, vice-président exécutif d'Airbus Space Systems, en quelques années, le flux d'images prises depuis l'espace a été multiplié par cinq, et cette évolution va se poursuivre grâce à des systèmes de plus en plus performants. L'arrivée de constellations de plusieurs dizaines, voire centaines, de satellites, va en effet générer une véritable explosion du volume d'images disponibles qu'aucun opérateur humain ne pourra traiter et analyser en temps réel.

Le spatial est, par exemple, l'un des plus gros fournisseurs de données climatiques et environnementales. C'est ainsi un véritable *big data* spatial qui se forme au-dessus de nos têtes, avec d'importants marchés à la clé. L'observation de la Terre recèle un potentiel commercial inédit pour l'industrie spatiale tant les champs d'application possibles sont nombreux : environnement, défense, géologie, agriculture, climatologie, télécommunications, *etc*.

Dès lors, le développement d'outils de traitement de données de masse est indispensable pour éviter que trop de données ne tuent la donnée. La communauté du renseignement est depuis longtemps confrontée à ce défi avec l'augmentation exponentielle des données issues de la mise en œuvre de techniques de renseignement ; c'est dans ce contexte que la loi « renseignement » du 24 juillet 2015 a autorisé, à titre expérimental jusqu'au 31 décembre 2020, la mise en place de la technique de l'algorithme visant à détecter une menace terroriste. En faisant appel à des ordinateurs pour traiter des masses d'informations dont le volume ne permet pas l'exploitation par des ressources humaines limitées, l'intelligence artificielle est la clé de la transformation de la donnée en renseignement, que ce soit à des fins civiles ou militaires.

À partir de ces algorithmes capables d'extraire les informations utiles, il devient possible de développer tout un champ de nouveaux services : détection de zones polluées, érosion des sols, surveillance des réserves maritimes, gestion durable des forêts, *etc.*

Pour ce qui relève plus particulièrement de la sécurité et de défense, il ne s'agit en effet pas de tout surveiller, mais de s'attacher à des individus

ou à des biens susceptibles de constituer, du point de vue de notre pays, une menace ou un risque.

EarthCube, une start-up parisienne, a ainsi développé pour le compte du ministère de la Défense, un logiciel à base d'intelligence artificielle d'analyse d'images, capable d'identifier automatiquement les éléments clés (aéronefs, dépôts de munitions, véhicules, *etc.*) des clichés réalisés et de remonter des alertes en cas de détection d'activité suspicieuse dans des zones de crise. Ce logiciel d'intelligence artificielle est fondé sur la technique de l'apprentissage profond en partenariat avec l'ONERA et l'INRIA.

Tirer le meilleur parti des informations collectées depuis l'espace suppose d'investir massivement dans l'économie de la donnée, et de bâtir un écosystème qui n'est encore qu'embryonnaire. C'est une économie éminemment duale et, comme pour la production de satellites ou le sujet des lanceurs, les intérêts souverains et commerciaux sont interdépendants.

Il s'agit tout à la fois de réussir à traiter les flux et d'industrialiser les processus de traitement. Cela implique la constitution de base de données et pose la question du stockage et de l'archivage.

Cette économie de la donnée, c'est la chaîne aval sur laquelle les Français et plus largement les Européens sont en retard par rapport au reste du monde. On ne peut ainsi éluder la question de l'utilisation par les GAFA de leurs données acquises depuis l'espace. On connaît la sensibilité de certaines d'entre elles au regard d'enjeux liés à la lutte contre le terrorisme, à la sûreté nucléaire et à de nombreux sujets de sécurité nationale. Dans ces conditions, et en l'absence de règles du jeu internationales, le comportement des GAFA est un paramètre à prendre en compte pour nos services de renseignement au vu de l'exploitation de données de souveraineté… impossibles à protéger. Il en découle des enjeux d'éthique qui ne se poseront évidemment pas dans les mêmes termes selon qu'on est face à des puissances amies ou hostiles. Dans ce contexte, il est indispensable de garantir un accès indépendant aux systèmes et aux données spatiales autour d'une filière souveraine de la donnée spatiale, sur l'ensemble de la chaîne, de l'amont (collecte) à l'aval (usages).

**Recommandation n° 49 : Favoriser un accès indépendant aux systèmes et aux données spatiales en développant une filière souveraine de la donnée spatiale, sur l'ensemble de la chaîne, de l'amont (collecte) à l'aval (usages), notamment en ce qui concerne nos capacités de stockage de données.**

## III. CONSERVER NOTRE CAPACITE DE RENSEIGNEMENT SPATIAL : CONDITION DE NOTRE STATUT DE PUISSANCE MONDIALE

L'espace est un levier stratégique majeur, non seulement parce qu'il est devenu indispensable à la conduite des opérations militaires mais aussi car il participe au statut de la France comme grande puissance mondiale. Le renouvellement de nos capacités spatiales est impératif si nous voulons conserver notre indépendance et exercer la plénitude de notre souveraineté. Et face à la menace de plus en plus prégnante d'une arsenalisation de l'espace, il s'agit également de repenser la gouvernance d'un secteur pour défendre au mieux nos intérêts et promouvoir la coopération plutôt que de se résigner à la confrontation.

### *A. RENOUVELER NOS CAPACITÉS SPATIALES*

La France a engagé en 2018 le renouvellement de l'ensemble de ses capacités spatiales avec la mise en service progressive d'une nouvelle génération de satellites de renseignement. Ce renouvellement de nos capacités se traduit par augmentation des moyens alloués au spatial dans la loi de programmation militaire 2019-2025. A plus long terme, il s'agit pour notre pays de se donner les moyens d'investir massivement dans des technologies de rupture qui conditionnent notre capacité à rester dans la course.

#### 1. Déployer la mise en service d'une nouvelle génération de satellites de renseignement

Le lancement du satellite espion CSO-1 le 19 décembre 2018 a marqué le début du cycle de renouvellement des capacités spatiales de la France, qui concerne les composantes suivantes :

- *l'observation spatiale militaire* : les trois satellites CSO, destinés à succéder aux satellites HELIOS II actuellement en service, depuis 2004 pour le premier et 2009 pour le second, devraient être tous lancés d'ici fin 2021. Le programme suivant sera lancé en réalisation en 2023. CSO doit nous garantir de conserver un accès souverain à l'imagerie optique et permettra d'accroître le nombre d'objectifs pouvant être imagés sur un théâtre géographiquement ;

- *l'écoute spatiale militaire* : les trois satellites CERES devraient tous être lancés d'ici fin 2020 (en remplacement des satellites ELISA) et le programme suivant réalisé à partir de 2023.

Sans qu'il s'agisse à proprement parler de renseignement, il convient aussi de mentionner :

- *s'agissant des télécommunications spatiales militaires* : les deux premiers satellites SYRACUSE IV seront lancés d'ici 2022 et complétés d'ici à

2030 par un troisième satellite répondant aux besoins croissants et spécifiques des plateformes aéronautiques ;

- *s'agissant de la surveillance de l'espace* : les moyens de veille (GRAVES) et de poursuite (SATAM) des orbites basses seront modernisés en priorité ;

- *s'agissant de la navigation par satellite* : les équipements de navigation par satellite des armées seront modernisés à partir de 2024 au travers du programme OMEGA, résistant aux interférences comme au brouillage, qui devra apporter une capacité autonome de géolocalisation capable d'utiliser à la fois les signaux GPS et GALILEO.

Dans les prochaines années, les huit satellites souverains dont nous disposons seront ainsi intégralement remplacés, ce qui n'est pas sans incidences budgétaires.

### 2. Se donner les moyens budgétaires de nos ambitions : les enjeux de la LPM 2019-2025

La LPM 2019-2025, en cours d'exécution, accorde une priorité à la fonction stratégique « connaissance et anticipation » au profit de laquelle les capacités spatiales apportent une contribution très substantielle. Elle prévoit que nos capacités nationales de surveillance de l'espace exo-atmosphérique (*Space Surveillance and Tracking*, SST) et de connaissance de la situation spatiale (*Space Situational Awareness*, SSA) soient consolidées, notamment par le renforcement du Commandement de l'espace et du Commandement de la Défense Aérienne et des Opérations Aériennes. Cette LPM doit permettre, d'ici son terme, de doter les armées de premières capacités permettant de conduire les opérations dans l'espace.

Les montants consacrés à nos moyens spatiaux de défense dans la LPM 2019-2025 sont en augmentation de 1,9 milliards d'euros par rapport à la LPM précédente sur la période 2014-2019. Ils sont en effet passés de 2,9 milliards d'euros à 4,8 milliards d'euros (pour les programmes budgétaires 144 et 146). Ces 4,8 milliards euros incluent le supplément de 700 millions d'euros ajouté après le vote de la loi par le Parlement, pour tenir compte des nouvelles orientations issues de l'annonce de la création du Commandement de l'espace.

Comme l'avait en effet clairement affirmé la ministre des Armées dans son discours de présentation de la stratégie spatiale de défense, le 25 juillet 2019 à Lyon, « les ressources financières seront dégagées pour avoir les moyens de nos ambitions ».

D'ici à 2025, une nouvelle génération de systèmes orbitaux de renseignement optique (CSO) et électromagnétique (Ceres) aux performances nettement accrues sera mise en service. La LPM prévoit en outre que trois nouveaux satellites de communications militaires Syracuse 4

viendront remplacer les Syracuse 3. Le successeur de MUSIS sera quant à lui commandé au cours de la LPM afin être livré avant 2030. Le programme « CERES successeur » devra assurer, à l'horizon 2028-2030, la pérennité de la capacité spatiale d'écoute électromagnétique.

Mais la durée de vie des nouveaux programmes, tels CSO, est estimée à une dizaine d'années. La ministre des Armées a ainsi dévoilé lors du Salon du Bourget de juin 2019, la mise en chantier de deux nouveaux programmes spatiaux appelés à remplacer la génération en cours de déploiement : baptisés « Iris » et « Céleste », ils proposeront, pour le premier, des capacités d'observation optique renouvelées, et pour le second, de nouvelles capacités de renseignement d'origine électromagnétique.

Aussi, dès la période suivante 2026-2030, la contribution budgétaire de la nation devra être du même ordre, avec même un effort supplémentaire à faire sur le programme budgétaire 78 relatif aux achats de service.

**Recommandation n° 50 : Confirmer la trajectoire budgétaire permettant le renouvellement de nos capacités de renseignement spatial contribuant à la fonction stratégique prioritaire « connaissance et anticipation ».**

### 3. Investir dans les technologies de rupture

La très forte accélération de l'innovation dans le domaine spatial impose des investissements accrus pour ne pas se laisser dépasser par le raccourcissement des cycles d'innovation. Plus que jamais se trouve renforcée la nécessité pour notre pays de conserver une avance à la fois dans la technologie et dans les architectures innovantes. Cela passe par des transferts de technologie du domaine commercial au secteur spatial, avec de nouveaux modes de production fondés sur des innovations de rupture. Cela suppose aussi de soutenir les programmes de démonstrateurs visant justement des technologies de rupture et non des évolutions incrémentales.

Parmi les dix technologies de rupture identifiées par le MIT en 2016 figurait par exemple les fusées réutilisables développées par SpaceX et Blue Orign. Au vu des gains financiers considérables à la clé, cette innovation de rupture a conduit l'Agence spatiale européenne à travailler à son tour sur la conception d'un lanceur réutilisable. C'est également à la recherche de nouvelles technologies de rupture que l'ONERA travaille, parmi d'autres projets, sur une piste prometteuse consistant à incorporer de plus en plus de technologies issues du transport aérien dans l'univers du spatial.

Appliquée au secteur spatial, la théorie dite de la « disruption » est redoutable pour les entreprises en place, car elle peut rapidement entraîner un changement de leadership.

La rupture s'appuie en effet sur deux mécanismes complémentaires. Premièrement, elle vient changer les normes et les critères de performance industrielle. Deuxièmement, en modifiant les compétences et les ressources nécessaires à la performance, elle frappe d'obsolescence celles qui opéraient jusqu'alors, et transforme les forces en faiblesses. Les actifs des entreprises installées deviennent graduellement obsolètes et constituent des freins à leur adaptation aux nouvelles normes, tandis que les normes et pratiques des nouveaux entrants s'imposent comme les nouveaux standards de performances à acquérir.

Dans ces conditions, nos fleurons industriels que sont *Airbus Defence and Space* et *Thales Alenia Space* ont mis en place de nouveaux programmes pour conserver leur avance stratégique sur un marché en pleine mutation.

Avec le programme OneWeb, *Airbus Defence and Space* ambitionne de faire passer les méthodes de fabrication des satellites de télécommunication de l'artisanat à l'ère industrielle, avec une production de 500 et 600 unités par an, permettant de diviser le coût des satellites par 50 et d'offrir des connexions internet bon marché dans le monde entier. C'est une véritable rupture pour cette industrie habituée au sur-mesure. Airbus fait appel à des industriels issus par exemple du secteur de l'électronique automobile pour leur expertise dans la production en grandes séries à bas coût. L'activité industrielle engendrée par le programme OneWeb doit ainsi permettre de développer et de pérenniser en France des produits, processus et savoir-faire sans équivalent dans le monde spatial. La seconde génération de satellites OneWeb est déjà à l'étude et souligne combien ce programme est un véritable catalyseur de transformation pour toute la filière et permet à notre pays d'être désormais bien positionné sur le marché de méga-constellations de satellites.

De son côté, *Thales Alenia Space* a constitué son cluster d'innovation dès 2014. Trois Fab Lab ont été créés à Toulouse (2017), Rome (2018) et Cannes (2019) avec pour ambition de familiariser les ingénieurs du groupe aux technologies émergentes. Le centre d'innovation a incubé en mode start-up deux projets stratégiques dans les nanotechnologies et l'optique. Un troisième projet a abouti à la définition d'un mini-satellite géostationnaire de télécoms que le groupe propose dans les appels d'offres ; et un quatrième projet a permis à Thales de remporter le contrat du satellite de télécoms Bangabandhu-1 du Bengladesh lancé en mai 2018, grâce à une nouvelle architecture du système de communication optimisant les ressources.

Réussir à franchir la marche des technologies de rupture suppose également de mettre en place un écosystème favorable au financement du risque. C'est ainsi que le CNES a lancé le fonds CosmiCapital de soutien aux start-up en phase de démarrage et doté de 100 millions d'euros. Le CNES apporte son expertise et ouvre à de jeunes PME les portes de l'écosystème industriel spatial comme il le fait avec l'entreprise *Hemeria* qui a développé avec succès le projet de nano-satellite ANGELS.

Mais il s'agit également de favoriser l'investissement privé dans le financement de l'économie spatiale, au seuil d'un formidable essor si l'on en croît les projections de Morgan Stanley qui estime que le chiffre d'affaires du secteur triplera d'ici à 2040, à 1 100 milliards de dollars par an. Aux États-Unis, le succès de SpaceX a eu un effet d'entraînement : des ingénieurs ont quitté leurs postes à la Nasa, chez Boeing et même chez SpaceX pour créer leur propre start-up. Même si la relation au risque n'est pas la même en Europe qu'aux États-Unis, il s'agit néanmoins de créer les conditions optimales au développement de l'initiative privée dans ce secteur stratégique et à forte valeur ajoutée.

### *B. PROMOUVOIR UNE NOUVELLE GOUVERNANCE*

La nouvelle donne spatiale appelle à penser une nouvelle gouvernance, à tous les niveaux : national, européen et international.

#### 1. Au niveau national : la création d'un Commandement de l'espace

À nouvelles ambitions, nouvelle gouvernance.

Le 13 juillet 2019, le Président de la République a annoncé la création d'un Commandement de l'espace (CDE) au sein de l'armée de l'air, renommée pour l'occasion « Armée de l'air et de l'espace ».

Cette décision répond à la volonté de remédier à la fragmentation qui caractérise depuis longtemps le paysage spatial français et qui nuit à notre capacité d'action. De très nombreux organismes sont en effet utilisateurs de satellites militaires. On peut notamment citer :

- la direction du renseignement militaire (DRM) pour ce qui est des satellites d'observation et d'écoute ;

- la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) s'agissant du contrôle opéré sur les satellites de télécommunications ;

- l'armée de l'air, à travers le COSMOS (centre opérationnel de surveillance militaire des objets spatiaux) et sa mission de surveillance de l'espace ;

- la DGA (direction générale de l'armement) pour la conduite des programmes spatiaux d'armement ;

- le CNES, à travers son statut d'opérateur pour les satellites militaires et son activité de suivi des débris spatiaux et des retombées atmosphériques à risque.

Face à cette multiplicité d'acteurs, qui répondent à des stratégies diverses et à des chaînes hiérarchiques distinctes, le Livre blanc sur la

Défense et la sécurité de 2008 avait préconisé la création d'un commandement interarmées de l'espace (CIE), lequel a vu le jour en 2010. Il s'agissait alors, pour reprendre les termes employés par le général Michel Friedling à la tête du Commandement, lors de son audition parlementaire le 13 février 2019 par la commission des affaires étrangères, de la défense et des forces armées du Sénat « *de positionner le spatial au bon niveau dans les chaînes de décisions politico-militaires et de rassembler les diverses responsabilités du secteur dans un organisme unique afin de redonner une cohérence au domaine spatial militaire* ».

Le CIE s'est ainsi vu confier l'identification des besoins militaires en matière de capacités spatiale et la mise en œuvre des orientations définies au plus haut niveau de l'État. Néanmoins, en neuf années d'existence, le CIE n'a mis fin ni au morcellement des responsabilités, ni à la dispersion géographique et fonctionnelle des implantations et des acteurs, ni à l'absence de chaîne de commandement unifiée pour les opérations spatiales. Le fonctionnement de ce commandement a atteint ses limites face aux bouleversements à l'œuvre dans le champ spatial et à la définition de nouvelles priorités stratégiques. Avec des moyens humains très modestes – une quarantaine de personnes –, et sans finalement disposer de véritables prérogatives de commandement, le CIE devait soit disparaître, soit évoluer. C'est cette seconde option qui a été retenue avec à la clé une réorganisation tant hiérarchique que stratégique.

Dans leur rapport d'information consacré au secteur spatial de défense[1], les députés Olivier Becht et Stéphane Trompille préconisaient ainsi de donner une « incarnation organique » à la Défense spatiale en créant, au sein d'une armée de l'air et de l'espace, un « grand commandement » des forces spatiales, du niveau « quatre étoiles ». Ils proposaient également d'ériger ce commandement en « gestionnaire unique du milieu » spatial et d'améliorer sa coordination avec les services compétents du CNES.

Le rapport du groupe de travail « Espace » du ministère des Armées, a lui aussi appelé à adapter la gouvernance du spatial militaires au niveau d'ambition de de notre pays, considérant que « *la nouvelle ambition du ministère des armées impose de revoir l'organisation actuelle selon des principes d'efficacité opérationnelle interarmées, de cohérence, de visibilité et de simplicité* ». Dans son discours prononcé le 25 juillet 2019 sur la base aérienne 942 de Lyon, la ministre des Armées a ainsi précisé que « à terme », le CDE conduira « *l'ensemble de nos opérations spatiales, sous les ordres du chef d'état-major des armées, en lien avec le Centre de planification et de conduite des opérations (CPCO), à l'instar de l'ensemble de nos opérations* ».

L'arrêté du 3 septembre 2019 portant création et organisation du commandement de l'espace opère la traduction juridique de ces orientations

[1] *Rapport d'information n° 1574 de la commission de la défense et des forces armées déposé en conclusion des travaux d'une mission d'information sur le secteur spatial de défense, enregistré à la présidence de l'Assemblée nationale le 15 janvier 2019.*

politiques, son article 1er énonçant que le commandant de l'espace reçoit des directives fonctionnelles du CEMA et que le chef d'état-major de l'armée de l'air en exerce le commandement organique.

Le rattachement à l'armée de l'air est cohérent : outre que cette armée fournit 70 % des effectifs affectés aux activités spatiales, il existe des similitudes entre les deux milieux spatiaux et aériens. Loin d'être seulement utilisatrice de services spatiaux, l'armée de l'air considère ce milieu sous l'angle d'une certaine continuité entre les milieux spatial et aérien.

Il convient à présent de construire dans la durée ce nouveau commandement en le dotant des moyens humains, financiers et capacitaires dont il aura besoin pour remplir pleinement ses missions. En déplacement à Toulouse le 21 février 2020, la ministre des Armées a donné des indications sur le calendrier de montée en puissance du CDE. Actuellement composé de 220 agents répartis sur quatre sites (Paris-Balard, Toulouse, Lyon et Creil), le CDE dont le siège a été fixé à Toulouse, a vocation à concentrer toute l'expertise du domaine spatial dans un bâtiment dédié, implanté au plus près du CNES. Ce regroupement sur un même site doit permettre de rapprocher le cœur militaire du cœur industriel et permettra aux armées de devenir les opérateurs directs de leurs satellites. Le CDE abritera ainsi des fonctions multiples comme la formation, l'innovation, ou encore le cœur de la conduite des opérations spatiales ; ses effectifs vont doubler à moyen terme puisqu'il accueillera près de 500 experts à l'horizon 2025. La clarification de la relation avec le CNES sera un élément décisif pour le succès du CDE.

Il conviendra également de définir le cadre des relations entre le CDE et la communauté du renseignement, pour les trois services qui relèvent du ministère des Armées, à savoir la DRM, le DRSD et la DGSE. Au vu du large périmètre des missions assignées au CDE, une composante « renseignement » pourrait utilement être constituée au sein du commandement.

**Recommandation n° 51 : Clarifier le positionnement du commandement de l'espace en matière de renseignement et constituer en son sein une formation spécialisée « renseignement ». Celle-ci pourrait produire du renseignement d'intérêt spatial au niveau opératif et tactique pour appuyer la planification et la conduite des opérations spatiales militaires.**

### 2. Au niveau européen : pas d'ambition commune sans confiance mutuelle

Avec 9 milliards d'euros investis en 2019, l'Europe est la deuxième puissance spatiale au monde. Elle est pourtant confrontée à un défi majeur : ne pas se laisser distancer et rester dans la course. Car la concurrence

internationale est rude : en 2019, l'Europe a réalisé 9 lancements de satellites *via* Arianespace, contre 34 pour la Chine, 27 pour les États-Unis et 22 pour la Russie.

Indépendance stratégique, leadership technologique, positionnement géopolitique : le sujet de la coopération spatiale interroge sur la finalité même du projet européen, au sens où il renvoie à une réflexion sur la souveraineté, son périmètre et ses modalités d'exercice. En effet, plus la politique spatiale devient un enjeu de souveraineté pour les États, plus la coopération européenne revêt un caractère sensible. Rétrospectivement, la politique spatiale européenne ne s'est jamais aussi bien portée que lorsque les États membres considéraient soit que l'Europe était pour eux une façon d'accéder à un domaine qu'ils n'avaient pas les moyens d'investir seuls, soit qu'elle était un outil de déploiement et de rayonnement de leur souveraineté nationale. Or le développement du « *New Space* », en démocratisant l'accès à l'espace, a pour effet induit de renationaliser, au moins en partie, la politique spatiale des États membres.

L'avenir de la coopération européenne est soumis à deux prérequis que sont d'une part la confiance, et d'autre part l'ambition commune.

*a) La confiance*

Compte tenu de ses enjeux à la fois politique, militaire, économique et industriel, l'espace constitue un milieu fédérateur propice à l'affirmation d'une identité européenne de défense et de sécurité. Ainsi, au-delà du renforcement de son autonomie stratégique nationale, la France a toujours privilégié la coopération européenne dans le domaine spatial, en particulier pour les systèmes d'observation optique. La première génération de satellites HELIOS I a été conduite en coopération multilatérale avec l'Italie et l'Espagne ; la deuxième génération HELIOS II l'a été dans le cadre d'une coopération avec, outre l'Italie, trois autres pays que sont la Belgique, l'Espagne et la Grèce. De même, la troisième génération de satellites, CSO, est accessibles aux partenaires européens par des accords bilatéraux avec la France.

L'accord de Schwerin de 2002 avait fixé une répartition / spécialisation des rôles entre la France, l'Allemagne et l'Italie fondée sur l'échange d'images d'observation spatiale radars (fournies par l'Allemagne et l'Italie) et optiques (fournie par la France). Un équilibre reposant sur une dépendance mutuelle s'était instauré que le gouvernement allemand vient toutefois de rompre unilatéralement en autorisant le BND à développer un système autonome d'imagerie optique. Il en résulte une asymétrie franco-allemande, dès lors que la France se trouve de facto dans une situation de dépendance à l'égard de son partenaire allemand, s'agissant de l'imagerie radar.

Force est de constater qu'un climat de défiance est en train de s'installer au cœur même du couple franco-allemand s'agissant de la

coopération spatiale. Or sans stratégie commune entre Français et Allemands, aucun progrès européen substantiel ne pourra avoir lieu.

Un indicateur supplémentaire de cette rivalité est apparu lors de la dernière conférence ministérielle de l'Agence spatiale européenne, en novembre 2019. La France y a en effet perdu sa place de leader spatial historique en Europe avec 2,66 milliards d'euros de contribution (18,5 % du budget de l'ESA). Elle a été très largement distancée par l'Allemagne (3,29 milliards d'euros, soit 22,9 % du budget de l'ESA) sur un total de 14,38 milliards d'euros pour la période 2020-2025. Paris reproche à Berlin de lui avoir fait une mauvaise manière en cachant l'intention du gouvernement allemand. Avec 22,9 %, l'Allemagne est désormais le premier contributeur de l'ESA, suivie de la France (18,5 %, 2,66 milliards d'euros), de l'Italie (15,9 %, 2,28 milliards d'euros) et du Royaume-Uni (11,5 %, 1,65 milliard d'euros).

Mais la rivalité n'est pas seulement franco-allemande. La France se trouve aussi talonnée par l'Italie qui contribue à hauteur de 15,9 % au budget de l'ESA. En conséquence, l'ambition de la France sera forcément en recul par rapport à la stratégie de ses deux voisins européens. L'Allemagne et l'Italie, à la fois rivaux et partenaires de la France ont fait le choix d'investir des sommes importantes sur des programmes, d'avenir. L'Italie s'est également positionnée sur le marché des lanceurs, avec Vega V, aujourd'hui complémentaire d'Ariane 6, mais qui porte aussi en lui les germes d'une concurrence future.

Au final, il s'agit à présent de fixer le bon point d'équilibre entre une concurrence vertueuse à l'échelle européenne, car source d'innovation, et la définition d'intérêts stratégiques communs qui sous-tendent une approche partenariale pérenne au service d'une autonomie stratégique. Ce qui est certain c'est que face aux Américains et aux Chinois, aucun des grands pays européens (France, Allemagne, Italie, Royaume-Uni) ne peut rester une puissance spatiale sans s'allier plus étroitement aux autres, y compris au plan industriel. Mais il est nécessaire pour cela, de s'accorder sur une réelle ambition européenne, qui pourrait utilement s'appuyer sur une initiative franco-allemande de nature à restaurer un climat de confiance entre nos deux pays.

**Recommandation n° 52 : Restaurer un climat de confiance franco-allemand en élaborant une feuille de route commune au service d'une ambition spatiale commune européenne.**

*b) L'ambition*

Il existe aujourd'hui trois niveaux de décision à l'échelle européenne : celui de l'agence spatiale européenne intergouvernementale, celui des agences nationales comme le CNES français ou le DLR allemand et le niveau communautaire qui se développe depuis les années 2000.

Depuis l'entrée en vigueur du traité de Lisbonne en 2009, l'espace est devenu un domaine de compétence partagée entre l'Union européenne et les États membres. Sur cette base, la Commission européenne a adopté en 2011 une communication intitulée « Vers une stratégie spatiale de l'Union européenne au service du citoyen » qui constitue le cadre des actions de l'Union.

L'Union européenne a jusqu'à présent développé des programmes spatiaux exclusivement civils mais pour certains avec des volets « sécurité ». Il en est ainsi du programme européen « *EU Space Surveillance & Tracking* » qui souligne la valeur ajoutée peut apporter une coordination renforcée entre plusieurs États membres. Face aux risques de collisions et de fragmentations, aux rentrées atmosphériques non contrôlées et aux manœuvres des satellites actifs, l'Union européenne a en effet établi en 2014 un cadre de soutien à la surveillance de l'espace et au suivi des décisions en orbite[1] (SST). Ce cadre a conduit à la création d'un consortium d'États membres (Allemagne, Espagne, France, Italie, Royaume-Uni) représentés par leurs agences spatiales, rejoints en 2019 par la Pologne, le Portugal et la Roumanie. Ce consortium EU-SST fournit depuis le 1er juillet 2016 des services d'analyse des risques de collision, de suivi des rentrées et de caractérisation des fragmentations dans l'espace, permettant aux opérateurs et utilisateurs des satellites nationaux et européens de disposer d'un service européen de haute qualité dans ce domaine crucial. La France assure, à travers le CNES, la présidence du consortium depuis juillet 2017 et l'exercera jusqu'à la fin 2020, à la suite d'une décision à l'unanimité des États partenaires.

L'Europe spatiale se déploie également autour de trois autres programmes majeurs :

- le programme GOVSATCOM, lancé fin 2013, qui vise à permettre les communications gouvernementales par satellite et garantir la sécurité des services de communication aux organisations et opérateurs jugés stratégiques pour l'Union européenne. On voit à travers la crise sanitaire liée à la Covid-19 combien la sécurisation des communications électroniques est un impératif de premier plan ;

- le programme GALILEO de positionnement par satellite, opérationnel depuis 2018 et qui compte à ce jour plus d'un milliard d'utilisateurs dans le monde. GALILEO qui fait écho au GPS américain, est décisif pour l'indépendance européenne ;

- le programme COPERNICUS, système d'observation de la terre, avec des implications importantes en termes d'étude du changement climatique. Grâce à ce programme, l'Union européenne possède l'un des plus grands fournisseurs de données au monde avec plus de 12 Téra octets de données complètes, gratuites et ouvertes de haute qualité chaque jour. COPERNICUS conforte l'Union européenne dans le jeu politique

[1] *Décision 541/2014/EU.*

internationale, comme a pu en témoigner la couverture des incendies qui ont ravagé la Sibérie et l'Amazonie au cours de l'été 2019.

En conclusion de la 12e Conférence annuelle sur la politique spatiale européenne qui s'est tenue à Bruxelles les 21 et 22 janvier 2020, le Commissaire européen Thierry Breton a prononcé un discours particulièrement volontariste appelant les Européens à prendre leurs responsabilités. Une politique spatiale ambitieuse est en effet indispensable pour assurer l'autonomie stratégique et la sécurité de l'Europe, et à terme son indépendance et sa souveraineté même.

L'ambition de l'Europe spatiale doit se décliner à plusieurs niveaux :

- garantir un budget suffisant : la Commission a proposé un programme spatial européen de 16 milliards d'euros pour la période 2021-2027, soit une augmentation de près de 5 milliards d'euros par rapport au précédent cadre financier pluriannuel ;

- assurer la continuité des programmes spatiaux existants et prendre en compte les nouveaux enjeux, ce qui implique un effort important en matière de recherche et d'innovation ;

- s'adapter aux nouvelles réalités géopolitiques, stratégiques, industrielles et technologiques. Ceci suppose de faire tomber un certain nombre de tabous qui concernent la dimension de défense et de sécurité des programmes européens comme Galileo ou Copernicus. C'est également tout l'enjeu de la mise au point d'un système européen de connaissance de la situation spatiale (SSA) afin de ne plus dépendre des seules informations que les Américains veulent bien nous transmettre. C'est enfin le développement d'une approche innovante pour la commande publique en matière spatiale autour d'une préférence européenne ;

- conserver un accès indépendant à l'espace, ce qui nécessite de maintenir l'excellence européenne en matière de lanceurs.

Pour mener à bien ces objectifs, une nouvelle gouvernance européenne est nécessaire qui prenne en compte la dimension stratégique et de sécurité de la politique spatiale. Le nouveau règlement sur la politique spatiale européenne permet d'organiser un système de gouvernance unifié et simplifié.

Mais au-delà de ce qui est prévu par le règlement, et sans interférer sur les compétences régaliennes des États membres, un réseau européen des commandants de l'espaces créés dans plusieurs États pourrait utilement se constituer, et donner corps, le moment venu, à un CDE européen doté de capacités significatives d'opérations spatiales, qui permettrait à l'Union européenne et à ses États membres de reprendre à leur charge et en pleine souveraineté la sécurité de leur composante spatiale civile ou militaire.

### 3. Au niveau international : s'accorder a minima sur un code de bonne conduite

Coopération v/ confrontation : le droit peut-il être un rempart à l'arsenalisation annoncée de l'espace ? À l'époque de la guerre foire, le petit club des pays spatiaux s'était facilement mis d'accord sur leur intérêt commun à sanctuariser l'espace autour d'un principe simple selon laquelle la liberté des uns s'arrête où commence celle d'autrui.

Il existe ainsi bien un socle de droit international régissant le droit de l'espace, l'équivalent d'une « constitution » de l'espace à travers le traité « *sur les principes régissant l'activité des États en matière d'exploration de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes* », conclu en 1967, dix ans après l'envoi par l'URSS de son premier Spoutnik.

Ce traité a été ratifié par une centaine d'États dans le monde. Il consacre deux principes essentiels :

- d'une part, l'usage pacifique de l'espace, dont l'exploration doit être réservée à des fins pacifiques, conformément au droit international et donc à la Charte des Nations-Unies, et où il est proscrit d'introduire des armes nucléaires et autres armes de destruction massive ;

- d'autre part, sa non-appropriation, ce qui exclu toute proclamation de souveraineté.

D'autres accords internationaux sont venus compléter le traité de 1967, comme la convention de 1972 sur la responsabilité internationale pour les dommages causés par les objets spatiaux ou encore la convention de 1976 sur l'immatriculation des objets lancés dans l'espace extra-atmosphérique.

Mais ces principes suffisent-ils à constituer des garde-fous à la militarisation croissante de l'espace ? Peut-on et comment réguler les activités humaines dans le contexte de commercialisation croissante de l'espace ?

Plusieurs décennies ont passé et le secteur spatial demeure toujours soumis, pour l'essentiel, à sa réglementation originaire, contrairement à la plupart des domaines d'activité dont le corpus légal a profondément évolué au gré des transformations sectorielles.

Or force est de constater que l'espace extra-atmosphérique est déjà devenu un nouveau milieu de confrontations où les principales entités physiquement présentes sont les satellites. On considère généralement que la première occurrence de guerre dans l'espace a eu lieu en 1991 pendant la Guerre du Golfe. C'était en effet la première fois qu'une armée se servait de satellites en vue de soutenir ses activités militaires offensives. Une course à l'armement spatial commence à prendre de l'ampleur : Le Président

américain Donald Trump a ordonné la création d'une *Space Force*[1] tandis que l'Inde a réussi à détruire un satellite en trois minutes par un tir de missile. La Chine et la Russie ont également investi dans le développement de telles armes.

Le droit de l'espace en vigueur est-il encore adapté à cette nouvelle donne géopolitique et aux enjeux actuels du « *New Space* » ? S'il est généralement admis que non, aucune approche commune ne se dégage pour autant au sein de la communauté internationale sur les modalités d'une future régulation. Et si la France reste attachée aux conventions internationales sur l'espace extra-atmosphérique, nombre de puissances spatiales, actuelles ou en devenir, n'y ont pas adhéré, ce qui conduit *de facto* à faire de l'espace en un enjeu de pouvoir et de conquête. L'arrivée de nouveaux États menace de faire éclater le « club » des quelques *happy few* spatiaux, au point de conduire les principaux pays à se pencher sur l'élaboration de nouvelles règles internationales pour l'utilisation de l'espace. Une course aux armements dans l'espace rendrait, en effet, une guerre potentielle probablement encore plus destructrice que les deux guerres mondiales, même si à ce stade, le sujet concerne avant tout la multiplication des attaques à l'encontre des satellites.

Outre les acteurs publics, l'essor du « *New Space* » a également provoqué l'arrivée importante d'acteurs non étatiques avec des enjeux économiques et non plus seulement diplomatiques et géopolitiques. Se pose en effet désormais la question, pour les opérateurs privés opérant dans l'espace, de leur protection juridique contre les risques politiques.

Dans ces conditions, la régulation internationale de l'espace extra-atmosphérique prendra du temps, dans un contexte global où, partout, le multilatéralisme est en repli. Il semble néanmoins important que la France continue de porter, au sein de la communauté internationale, et en particulier des instances européennes et onusiennes, une approche coopérative.

La France vient ainsi de rejoindre, en février 2020, l'initiative de coopération spatiale interalliées CSpO (*Combined Space Operations*), véritable forum multilatéral de coordination, de réflexion et d'échanges, qui vise à coordonner les efforts dans le domaine de la défense spatiale, des sept nations participantes : États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande, Allemagne et France. Cette initiative poursuit plusieurs objectifs :

- coordonner les capacités alliées ;

- en augmenter la résilience pour assurer le soutien aux opérations multi-domaines ;

- garantir un libre accès à l'espace ;

[1] *Le* Spacecom *devient le 11e commandement militaire du Pentagone.*

- y protéger les moyens qui s'y trouvent, le cas échéant en coalition.

Par ailleurs, faute de consensus sur un nouveau cadre juridique international contraignant, il paraît nécessaire de s'accorder, à tout le moins, sur un code de conduite pour les activités humaines dans l'espace. L'Union européenne a soumis en 2015[1] un projet à la communauté internationale que la France doit continuer à promouvoir sur la scène diplomatique.

**Recommandation n° 53 : Promouvoir au sein de la communauté internationale l'adoption rapide du code de bonne conduite proposé par l'Union européenne pour les activités humaines dans l'espace.**

Ce code de conduite propose de compléter le droit international de l'espace avec trois nouveaux principes selon lesquels :

- les États devraient s'engager à prendre les mesures nécessaires pour améliorer la sécurité des opérations spatiales et réduire les débris spatiaux. Sauf nécessité absolue, cela implique de ne pas essayer ou employer des méthodes de guerre pouvant générer des débris ;

- le droit à la légitime défense individuelle et collective dans l'espace serait explicitement énoncé. Le Conseil de sécurité des Nations Unies pourrait donc exercer ses compétences dans l'espace pour maintenir et rétablir la paix et la sécurité internationale. Tout État pourrait également y exercer son droit de légitime défense ;

- les États s'engageraient à instaurer un climat de confiance et de coopération. Ils devraient se conformer à leur obligation d'immatriculation de tous les objets spatiaux, notifier leurs manœuvres spatiales, s'informer mutuellement sur leurs politiques spatiales respectives et se consulter le cas échéant.

*

* *

Le renseignement spatial évolue dans un univers en pleine révolution qui touche à l'exercice même de nos compétences régaliennes.

La crise sanitaire liée au coronavirus a mis en exergue les fragilités susceptibles de mettre en péril des pans entier de notre souveraineté si notre filière industrielle spatiale n'était pas suffisamment soutenue et protégée face à des intérêts hostiles.

---

[1] *Décision (PESC) 2015/203 du Conseil du 9 février 2015 visant à soutenir la proposition de code de conduite international pour les activités menées dans l'espace extra-atmosphérique, présentée par l'Union, afin de contribuer aux mesures de transparence et de confiance relatives aux activités spatiales.*

L’espace est notre nouvelle frontière, pas seulement technique mais aussi démocratique. L’exploitation des données issues de l’espace représente le nerf de cette nouvelle guerre qui touche autant à notre vie quotidienne qu’à nos intérêts vitaux, comme en témoigne, pour prendre un exemple récent, le développement des applications de traçage dans la lutte contre la Covid-19.

# CHAPITRE V :
# CYBERDÉFENSE, LA CONTRIBUTION MAJEURE DES SERVICES DE RENSEIGNEMENT

En quelques années avec la numérisation des communications et le développement des réseaux, le cyberespace est devenu un « espace commun » dans lequel se déploient des activités de toutes natures légales et illégales et des stratégies de puissance. Cet espace est encadré par les mêmes règles que celles qui s'appliquent dans le monde physique mais peinent à y trouver leur efficacité.

La protection des intérêts fondamentaux de la Nation s'étend à ce nouvel espace. Face au développement des menaces, **la France s'est progressivement dotée, depuis 2008, d'un dispositif de protection et d'action original, en ce qu'il distingue très clairement les activités de prévention et de protection placées sous le contrôle du Premier ministre, qui dispose d'une agence nationale de sécurité des systèmes d'information, l'ANSSI,** (avec un régime particulier s'agissant des armées depuis 2017) **et des activités plus offensives placées dans la chaîne de commandement des armées sous l'autorité du Président de la République et mises en œuvre selon une stratégie et une doctrine exposées le 18 janvier 2019 par la ministre des armées.**

**Elle se distingue donc très clairement du modèle anglo-saxon dans lequel toutes les activités de cyberdéfense étaient concentrées au sein des services de renseignement.**

**Pour autant, les services de renseignement français ne sont pas exclus des activités de cyberdéfense**, soit pour se protéger, soit pour contribuer à l'analyse des menaces, soit pour participer à leur entrave, en collectant du renseignement d'intérêt cyber (RIC). Ils doivent en outre pour réaliser leurs missions traditionnelles collecter du renseignement, dit d'origine cyber (ROC) dans ce nouvel espace, qui constitue par lui-même une mine d'importance, qu'il s'agisse de l'exploitation des innombrables données en source ouverte ou d'utiliser des techniques spécifiques de recueil dans le cadre légal défini par le législateur.

**Pour gagner en efficacité, l'action des différentes entités opérant au titre de la cyberdéfense doit être mieux coordonnée**. Tel a été l'objet de la Revue stratégique de cyberdéfense préparée sous la direction M. Louis Gautier, alors secrétaire général de la défense et de la sécurité nationale (SGDSN) et publiée en février 2018.

Si la Stratégie nationale du renseignement publiée en 2014 mentionnait déjà les cyberattaques parmi les menaces, la nouvelle version préparée par la CNRLT et publiée en juillet 2019 reconnaît, encore plus

explicitement la place du cyberespace et lui consacre un long développement dans la présentation des enjeux prioritaires du renseignement, au titre de la lutte contre les menaces transversales.

**La cyberdéfense dans la Stratégie nationale du renseignement**

*« En matière cyber, la menace qu'elle soit étatique, provenant d'entreprises privées ou d'organisations criminelles, a fortement évolué. Elle est de plusieurs natures : vol de données, sabotage au préjudice d'entreprises comme des administrations, pénétration aux fins d'espionnage, chantage en vue d'obtenir une rançon… Il convient de souligner que certaines de ces opérations de prédation relèvent désormais d'une nouvelle forme de cybercriminalité organisée. Aussi, l'acuité de la menace et les risques encourus sont tels qu'il est essentiel, au-delà des dispositifs de sécurité dont nous sommes dotés, que les services de Renseignement contribuent à leur recherche et à leur anticipation sans leurs champs respectifs de compétence.*

*Qui plus est, le développement de l'Internet des objets et des communications spatiales, ainsi que l'évolution des* maliciels *aux effets de plus en plus destructeurs nécessitent une adaptation constante des capacités des services et une meilleure diffusion du renseignement vers les entités chargées de la protection et de l'entrave.*

*Enfin, par le biais d'internet et des réseaux sociaux, l'espace cyber est un vecteur de diffusion de messages haineux et de manipulation de l'information qui mérite un suivi du renseignement, notamment en termes de lutte contre la cybercriminalité, pour identifier les messages ou les campagnes les amplifiant, en attribuer l'origine et faciliter leur entrave administrative et judiciaire. »*

La cyberdéfense ne fait en revanche pas l'objet de dispositions spécifiques dans la partie consacrée à la description générale des missions du renseignement, ni dans la partie consacrée aux perspectives pour le renseignement. Toutefois cette dernière insiste sur les réponses aux défis technologiques « *qui constituent également une priorité pour la communauté du renseignement* » avec trois enjeux majeurs : « *la diffusion de l'expertise entre les services pour s'approprier les nouveaux outils, la valorisation des données de plus en plus volumineuses et hétérogènes, la conception de nouveaux outils en anticipant les évolutions technologiques et en s'appuyant sur une culture de l'innovation en lien avec la recherche et l'industrie* ». L'application de ces perspectives au domaine cyber est évidente.

Ces directions devraient trouver des déclinaisons concrètes sous forme de plans d'actions ou au sein de la nouvelle version du Plan national d'orientation du renseignement (PNOR). Le PNOR reconnait d'ores et déjà la cyberdéfense comme une finalité et intègre la participation des services de renseignement à la politique publique de la cyberdéfense dans toutes ses dimensions.

**Recommandation n° 54 : La DPR demande que les différents traitements de la menace cyber par les services de renseignement fassent l'objet d'un développement actualisé dans le PNOR et sous forme de plans d'actions comprenant des objectifs à atteindre et des modalités d'évaluation de la réalisation de ces objectifs. Elle demande à pouvoir prendre connaissance de ces documents et, régulièrement, des résultats obtenus au titre de sa mission d'évaluation de la politique publique de renseignement.**

## I. DES MENACES PLUS NOMBREUSES, PLUS MASSIVES ET PLUS SOPHISTIQUÉES

**Telles que décrites dans les différents Livre Blanc sur la défense et la sécurité nationale depuis 2008, les menaces dans le cyberespace apparaissent toujours plus nombreuses, toujours plus massives, toujours plus sophistiquées, toujours plus multiformes, toujours plus disruptives dans leurs modes opératoires. Le cyberespace est, sans doute, l'espace commun dans lequel les menaces évoluent le plus rapidement donnant une impression d'insaisissable phénomène et rendant nécessaire un ajustement permanent des missions de connaissance et d'anticipation si l'on souhaite s'en prémunir et les contrer.**

### *A. L'ESPACE NUMÉRIQUE EST UN LIEU DE CONFRONTATION*

L'espace numérique est à la fois un lieu de communication et d'échanges favorable au progrès et un lieu de confrontation. Les actions offensives à l'encontre des systèmes informatiques de l'État, des infrastructures critiques ou des grandes entreprises sont quotidiennes, sans que l'on puisse toujours en saisir l'origine et en comprendre les motivations, ni même distinguer avec certitudes qui, acteurs étatiques ou non étatiques, en sont les commanditaires et les exécutants.

La plupart des crises intérieures ou internationales et des conflits inter ou intra-étatiques ont désormais une dimension cyber. Le constat d'une exposition accrue de nos sociétés de plus en plus numérisées et interconnectées au risque de crises cyber majeures s'impose sans conteste.

La menace ne cesse de croître dans ses formes et son intensité. Les attaquants informatiques poursuivent quatre types d'objectifs, non exclusifs entre eux : l'espionnage, les trafics illicites, la déstabilisation et le sabotage. Dans la poursuite de ces objectifs, les attaquants peuvent être amenés à conduire aussi bien des opérations très ciblées que massives et indifférenciées. Les attaques peuvent avoir des effets variables : invisibles lors d'une exfiltration discrète de données ou à l'inverse apparents lorsqu'il s'agit de paralyser une activité. Les dommages peuvent être facilement

réversibles ou au contraire nécessiter de longs et coûteux travaux de reconstruction (sabotage contre TV5 Monde et attaque contre l'OTAN et le Bundestag en 2015 ou l'attaque *Notpetya* dont le groupe Saint-Gobain a été une victime collatérale en 2017).

Les États sont aujourd'hui confrontés à une évolution de la menace informatique s'articulant autour de trois facteurs :

- la dangerosité de la menace sous l'effet de la multiplication des acteurs, de l'accroissement des capacités offensives de certaines puissances étrangères, de la prolifération des armes informatiques et de la banalisation des techniques d'attaques ;

- l'imbrication des enjeux de cybercriminalité et de sécurité nationale. Les outils traditionnellement utilisés à des fins de fraude et d'extorsion de fonds, peuvent causer des dommages aux systèmes d'information de l'État et des opérateurs en charges d'infrastructures critiques, paralysant ainsi la continuité de leurs activités (ex : en mai 2017, attaque par rançongiciel *Wannac*ry qui a touché Vodafone, Fedex, Renault , Téléfonica, Deutsche Bahn et le système de santé britannique) ;

- une exposition accrue de notre société à la menace du fait d'une numérisation plus étendue de celle-ci et à une utilisation à grande échelle d'objets connectés ;

- s'ajoutant aux innombrables opérations d'espionnage informatique très régulièrement détectées et aux risques bien documentés de pillage des données ou de déni d'accès, des actes de blocage ou de sabotage sont de plus en plus constatés.

Nos sociétés démocratiques sont en outre confrontées aux mésusages d'Internet et des réseaux sociaux à des fins de manipulation de l'opinion et de déstabilisation institutionnelle (les actions pour perturber l'élection présidentielle américaine de 2016, ou française de 2017 ou les élections européennes de 2019 en sont des exemples, comme la campagne massive de propagande et de désinformation développée par la Chine à l'occasion de la crise sanitaire en avril 2020).

De plus en plus d'attaques combinant différents modes d'action et semblant poursuivre plusieurs finalités révèlent un travail de planification et d'infiltration en amont mené par des acteurs dotés de capacités avancées.

Si les objectifs des cyberattaquants n'ont pas fondamentalement changé, les modes opératoires et techniques utilisés pour y répondre sont sans cesse renouvelés par l'émergence continue de nouvelles pratiques et technologies liées au numérique, ainsi que l'hyper-connectivité de nos équipements et réseaux.

Le cyberespace possède une dynamique qui lui est propre : instantanéité des échanges, diffusion en réseau, massivité de données accessibles à tous, effacement des frontières… Il est aussi un multiplicateur

d'efficacité pour peu que l'on dispose des bonnes données et informations, qui sont devenues une ressource critique, au cœur du fonctionnement politique, économique et social des sociétés modernes.

### *B. LES ÉVOLUTIONS RÉCENTES FONT APPARAÎTRE DE NOUVELLES TENDANCES*

La première est l'accessibilité des outils d'attaque, en raison de leur prolifération sur Internet (*darkweb*), ce qui abaisse le coût de l'investissement de départ et rend, de fait, le nombre d'attaquants toujours plus important.

La deuxième est que les attaquants les plus expérimentés[1], notamment ceux qui sont sponsorisés directement ou indirectement par les États, ont compris que, si les grandes organisations se sécurisaient de mieux en mieux, il fallait toucher les maillons faibles et que ceux-ci se trouvaient dans l'écosystème, en particulier les sous-traitants pour l'espionnage économique ou encore des établissements plus vulnérables comme les systèmes de santé[2] ou les collectivités territoriales[3] qui doivent délivrer sans délais des services indispensables à la population pour les attaques par rançongiciels.

La troisième est la sophistication croissante des modes opératoires visant à dissimuler leur origine réelle et désorienter les capacités d'attribution des attaques.

**Offuscation, dissimulation, sophistication des modes opératoires.**

Sur le plan des menaces de nature stratégique, l'ANSSI se heurte aujourd'hui à de nouvelles stratégies de dissimulation adoptées par les acteurs offensifs. Dans les échanges avec ses partenaires nationaux et internationaux, comme dans l'observation directe des infrastructures d'attaques, elle constate par exemple :

- un effort, particulièrement de la part des modes opératoires supposés russes, de renouvellement, de diversification et de banalisation des infrastructures de commande et contrôle (C2) visant à les rendre encore moins détectables et caractérisables ;

- un partage d'infrastructures et de codes malveillants entre des modes opératoire supposés russes et d'autres plutôt liés à l'Iran.

---

[1] *Les groupes cybercriminels se sont structurés et disposent de moyens conséquents, aidés par la disponibilité croissante sur Internet de nombreux outils d'attaques. Les actions conduites par ces groupes sont grandement planifiées et construites comme de véritables opérations de renseignement (ingénierie sociale en amont, ciblage, choix du moment opportun pour déclencher la charge, en amont de publication de résultats financiers par exemple).*

[2] *En France en 2019, 120 établissements du groupe privé Ramsay/Générale de Santé en août, les CHU de Montpellier (au printemps) et de Rouen (en novembre), en République Tchèque, l'hôpital de Brno en pleine crise sanitaire au printemps 2020*

[3] *Exemple récent de l'agglomération de Marseille à la veille des élections municipales*

À l'instar de la problématique posée par les modes opératoires russes, l'analyse de la menace des modes opératoires supposés chinois se confronte à d'importants efforts de dissimulation, afin de rendre hasardeuse toute stratégie d'attribution technique.

Enfin, les modes opératoires supposés chinois recourent souvent à une stratégie de compromission des chaînes d'approvisionnement de leurs cibles finales. Visant des prestataires de services numériques ou des bureaux d'études, ces attaques par rebond facilitent une pénétration discrète dans les réseaux de grands acteurs, réputés plus matures en matière de cybersécurité. La phase initiale de la compromission, souvent la plus sensible, se déroule donc généralement hors de portée des moyens d'investigation ou de détection étatiques qui s'appliquent préférentiellement aux réseaux des administrations centrales et des opérateurs d'importance vitale (OIV).

Enfin la dernière est la démystification de l'usage du cyber, que ce soit à des fins de sabotage ou de désinformation par des États qui l'assument comme une arme de déstabilisation ou de désorganisation massive à part entière[1].

Derrière ces tendances, il y a un changement de nature qui fait qu'aujourd'hui les États démocratiques réfléchissent à des changements de stratégie et d'organisation pour répondre à ces défis : le caractère massif de l'information, son instantanéité et les difficultés d'attribution ont mis les organisations face à une pression tout à fait nouvelle. Les stratégies tant française, qu'allemande ou britannique ont cherché à réévaluer cette menace et la façon d'y répondre.

### *C. L'EXPLOITATION DES VULNÉRABILITÉS DE LA NUMÉRISATION TOUCHE AUSSI LE CHAMP DE BATAILLE MILITAIRE*

Nos adversaires ont parfaitement compris l'avantage politique, économique ou opérationnel qu'ils pouvaient obtenir de l'exploitation des vulnérabilités de cette numérisation galopante, touchant aussi le champ de bataille militaire.

[1] *Comme le montre, l'utilisation décomplexée des réseaux sociaux par les diplomates chinois pendant la crise sanitaire du printemps 2020 en contradiction avec les usages diplomatiques pour commenter en public et critiquer ouvertement, dans la langue des États où ils exercent et en manipulant subtilement informations vérifiées et fausses informations crées de toute pièce, les décisions prises par les autorités de ces États. La centralisation de l'administration chinoise et le fait que ces diplomates aient reçues une formation spécifique dans ce domaine montre bien qu'il ne s'agit pas d'initiatives relevant de la créativité personnelle mais d'une stratégie de communication mûrement réfléchie.*

**État de la menace pour les armées**

**Les armées n'ont pas fait l'objet de cyberattaques ciblées à des fins de sabotage, de destruction, de dégradation, ou d'instrumentalisation de données. En revanche, elles ont déjà été exposées à des attaques à fins d'espionnage ou visant à nuire à leur image. Elles ne se considèrent toutefois pas à l'abri d'une cyberattaque indiscriminée via, notamment, les campagnes de rançongiciels qui balaient régulièrement l'Internet.**

**Le nombre d'incidents est passé de 830 en 2018 à 850 en 2019 mais parmi eux, 6 incidents majeurs ont été relevés en 2019, contre 4 en 2018.**

La tendance en 2019 montre la prépondérance de la cybercriminalité parmi les attaques détectées ; notamment par l'emploi de rançongiciels. Jamais directement prises pour cible, les armées ont pu, ponctuellement être victimes de campagne d'attaques non discriminées ou ciblant un secteur d'activité.

Des codes malveillants, souvent des virus informatiques anciens, ont été découverts sur des systèmes d'arme, généralement à l'occasion d'une maintenance par des industriels. Bien que n'ayant pas eu d'impact opérationnel à ce stade, ces infections démontrent la réalité de la menace.

Les opérations militaires font l'objet d'attaques informationnelles régulières sur les réseaux sociaux, parfois massives et a priori coordonnées, tout particulièrement en Afrique, et sont sujettes aux menaces cyber, qui sont la déclinaison des menaces générales propres au théâtre considéré. Les réseaux déployés en OPEX comportant moins d'interconnexions (donc davantage isolés), la menace criminelle semble moins prégnante, mais le caractère opérationnel des déploiements est susceptible d'attirer davantage une menace de niveau stratégique.

Certains systèmes déployés à l'étranger peuvent par ailleurs présenter certaines vulnérabilités à l'égard d'opérateurs de télécommunication locaux non maîtrisés et plus vulnérables à l'action de services étrangers (technologies 3G chinoises en Afrique, forte présence chinoise télécom à Djibouti).

**L'anticipation et la maîtrise de ce risque constituent les deux paramètres clefs d'une lutte informatique défensive (LID) devenue indispensable pour préserver le fonctionnement quotidien des intérêts nationaux**, qu'il s'agisse des administrations et services de l'État (y compris nos armées), des opérateurs d'importance vitale ou de services essentiels, ou de toutes autres formes d'activités ou d'organisations : des collectivités territoriales ou entreprises, en passant par les organes de presse ou les associations ou encore la vie quotidienne de nos concitoyens de plus en plus connectés.

**Cette maîtrise exige une implication croissante des services de renseignement, pour se protéger, prévenir en recueillant des renseignements d'intérêt cyber par leurs moyens classiques ou en opérant dans le domaine cyber, entraver les menaces en agissant dans le domaine cyber si nécessaire.**

## II. UN MODÈLE FRANÇAIS DE CYBERDÉFENSE CONSTRUIT PROGRESSIVEMENT, ÉPROUVÉ ET PERFECTIBLE

Dès lors, la cyberdéfense constitue un enjeu stratégique majeur pour la sécurité nationale et le développement économique. Depuis les années 2000, la France a réagi de façon continue aux évolutions extrêmement rapides qui caractérisent ce domaine.

### *A. LA CONSTRUCTION PROGRESSIVE D'UNE STRATÉGIE ET D'UN MODELE ORIGINAL DE CYBERDÉFENSE*

#### 1. Le Livre Blanc sur la défense et la sécurité nationale de 2008

Il a permis de franchir une étape décisive en annonçant la création, en 2009, de l'agence nationale de sécurité des systèmes d'information, l'ANSSI, rattachée au SGDSN, pour traiter les attaques informatiques et protéger les systèmes d'information de l'État et les infrastructures critiques. La France met progressivement en place un modèle fondé sur la séparation de ses capacités défensives et offensives et publie sa première stratégie de cybersécurité en 2011.

**Un système différent du modèle anglo-saxon**

**Contrairement au modèle initial anglo-saxon, et peut-être parce que la France ne disposait pas d'un service technique autonome comme le GCHQ en Grande-Bretagne ou la NSA aux États-Unis, le modèle français de cybersécurité s'est construit à l'extérieur des services de renseignement.**

**Plus fondamentalement, ce modèle original est le résultat d'une succession de choix politiques ambitieux** issus d'une double prise de conscience : d'une part, le numérique peut être utilisé pour mener des actions offensives contre nos intérêts nationaux ; d'autre part, la transformation numérique de la société, de l'économie et de l'action publique, ne pourra se faire qu'en confiance. Il s'agissait donc de créer les conditions de la confiance avec le secteur privé par la séparation nette entre le défensif et l'offensif, le civil et le militaire.

A l'inverse, si les modèles de fusion des capacités offensives et défensives au sein des appareils militaires ou de renseignement rendent possible une mutualisation des capacités techniques très précieuse, ils tendent structurellement à privilégier l'offensif sur le défensif. Aussi, pour efficace qu'il puisse paraître, le choix d'un modèle de concentration apparaît peu adapté à une politique de *cybersécurité globale* à vocation interministérielle. De fait, la confiance des acteurs économiques et sociaux peut également être amoindrie par la concentration des fonctions offensives et défensives dans une même entité, en particulier au sein de la communauté du renseignement. À ce titre, l'exemple américain est parlant. Conscient de ces lacunes, les États-Unis font progressivement évoluer leur modèle pour dissocier plus clairement les acteurs en charge de ces différents aspects et

regagner la confiance perdue du fait de cette confusion entre renseignement et protection.

### 2. En 2013, le nouveau *Livre Blanc* élève la cyberdéfense au rang de priorité stratégique

Il affirme également le principe d'une doctrine nationale de réponse aux agressions informatiques intégrant deux volets complémentaires avec la mise en place :

- d'une posture de protection des systèmes d'information de l'État, des opérateurs d'importance vitale (OIV) et des industries stratégiques, couplée à une organisation opérationnelle de défense de ces systèmes, coordonnée sous l'autorité du Premier ministre ;

- d'une capacité de réponse gouvernementale globale ajustée face à des agressions de nature et d'ampleur variées faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère des armées si les intérêts nationaux sont menacés ;

- la LPM (2014-2019) renforce la sécurité des OIV et prévoit un doublement des effectifs du ministère des armées dans le domaine cyber.

### 3. La réflexion a été approfondie dans la période récente par de nombreux documents stratégiques

*a) La revue stratégique de défense et de sécurité nationale (octobre 2017)*

- Constate (p.35) le renforcement des menaces dans le cyberespace (*cf. supra*) ;

- ce qui appelle notamment, le renforcement prioritaire des moyens de défense et le développement de capacités offensives comme défensives.

*b) La stratégie nationale de la cyberdéfense (février 2018)*

Préparée sous la direction du SGDSN[1], ce document propose la création de quatre chaînes opérationnelles pour conduire les missions de cyberdéfense dont une chaîne « renseignement », une chaîne « action militaire » et une chaîne « action judiciaire » ainsi que par la modernisation de la gouvernance.

La stratégie articule la politique de cyberdéfense autour de la notion de « défendabilité » des systèmes d'information la plus robuste possible et, au-delà, définit l'action des pouvoirs publics sur la base de six missions.

[1] *À l'époque, M. Louis Gautier*

**Les missions de cyberdéfense des pouvoirs publics**

• **Prévenir** : faire prendre conscience aux utilisateurs du risque représenté par la numérisation des organisations ou des équipements qu'ils servent[1] ;

• **anticiper : évaluer en permanence les probabilités de cyberattaques et prendre des mesures préventives lorsque la menace paraît suffisamment forte.** Cette mission incombe à l'ANSSI (et au COMCYBER sur le périmètre du ministère des armées), **en coordination avec les services de renseignement ;**

• **protéger** : diminuer la vulnérabilité des systèmes informatiques, à la fois en compliquant la tâche des attaquants potentiels et en facilitant la détection des cyberattaques ;

• **détecter : rechercher des indices d'une éventuelle cyberattaque en cours** ;

• **réagir : résister à une cyberattaque** afin qu'elle n'empêche pas la poursuite de l'activité. Une opération de LID, peut être déclenchée en liaison avec l'ANSSI. Elle peut entraîner l'emploi de moyens qui sortent du domaine de la cyberdéfense (saisie de la justice, action diplomatique, rétorsion économique, *etc.*), voire du ministère des armées ;

• **attribuer** : préciser l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices. **Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution. La décision d'attribution appartient aux plus hauts responsables politiques**.

Les actions de prévention et de protection concernent les systèmes informatiques situés principalement sur le territoire national. Les missions d'anticipation, de détection et de réaction s'intéressent aux systèmes informatiques appartenant aux autres catégories d'acteurs, le cas échéant situés à l'étranger.

**Le rôle majeur de l'ANSSI**

Au niveau interministériel, les capacités défensives de l'État sont pilotées par l'ANSSI qui est en charge d'assurer les trois missions suivantes :

• en tant qu'agence interministérielle au service de l'ensemble des administrations, elle coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;

• elle prescrit aux administrations et aux OIV des règles de sécurité préventives, en contrôle l'application et, en cas de crise majeure, peut leur imposer des mesures réactives ;

[1] *Cette mission incombe en première ligne aux Hauts fonctionnaires de défense et de sécurité des entités publiques et aux responsables de la sécurité des systèmes d'information des entités privées, mais est de plus en plus portée au sein des comités exécutifs des entreprises et des responsables politiques des entités publiques.*

• elle coordonne l'action gouvernementale en matière de défense des systèmes d'information et peut répondre, par des mesures techniques aux attaques visant les administrations et les OIV, le cas échéant, en neutralisant les effets des attaques.

L'ANSSI peut également apporter un soutien technique au ministère de l'intérieur et à l'autorité judiciaire en vue de caractériser les attaques, notamment en contribuant à la détermination des modes opératoires et à l'identification des auteurs de cyberattaques.

*c) La LPM (2019-2024) poursuit cet effort*

Elle renforce les capacités de l'ANSSI. Elle crée au sein du ministère des armées une « posture permanente cyber » qui s'appuie sur un commandement de cyberdéfense créé en 2017 ***** et des moyens des armées (1,6 milliards d'euros d'investissement dans le cyberespace)[1].

*d) La stratégie cyber des armées (janvier 2019)*

Esquissée par le discours du ministre de la défense sur la cyberdéfense à Bruz le 12 décembre 2016[2], une stratégie cyber des armées a été rendue publique par la ministre des armées le 18 janvier 2019[3]. Cette stratégie décline deux objectifs : l'un défensif, l'autre offensif.

La France consolide ainsi un modèle rénové de cyberdéfense, dont la création du commandement de la cyberdéfense (COMCYBER) en mai 2017[4] avait constitué une des étapes fondatrices au sein du ministère des armées. Le COMCYBER a la responsabilité de la cyberdéfense militaire, qui recouvre l'ensemble des actions défensives et offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère et l'efficacité des forces armées, dans la préparation, la planification et la conduite des opérations.

Cette capacité contribue à garantir la souveraineté nationale.

---

[1] Cf. *rapport n° 476 (2017-2018) de M. Christian Cambon au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense (16 mai 2018) p.28 et suivantes.*

[2] *https://www.defense.gouv.fr/actualites/articles/cyberdefense-bilan-et-nouveaux-chantiers-annonces-par-le-ministre*

[3] *https://www.google.com/search?client=firefox-b-e&q=discours+Parly+cyber+18+janvier+2019*

[4] *Décret n° 2017-743 du 4 mai 2017 relatif aux attributions du chef d'état-major des armées et l'arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées.*

(1) Garantir la cyberdéfense, en protégeant les réseaux, les systèmes et les données du ministère des Armées et du secteur de la défense

Le ministère des armées a souhaité r**edéfinir sa politique en matière de lutte informatique défensive (LID**)[1] dans une instruction ministérielle du 1er décembre 2018, et renforcer, en parfaite coordination avec l'ANSSI, la posture permanente de cyberdéfense.

(2) Intégrer l'arme cyber dans les opérations militaires

Evoquée depuis le Livre blanc de 2008, la lutte informatique offensive a été confirmée officiellement par le discours du ministre de la défense de Bruz le 12 décembre 2016, puis par la LPM 2019-2025. La ministre de la défense a rendu publics des éléments de doctrine le 18 janvier 2019[2].

(a) Une doctrine pour la lutte informatique offensive

Dans la doctrine française, la LIO est limitée à deux objectifs : l'appui aux opérations militaires extérieures d'une part, et d'autre part, l'appui à la lutte informatique défensive lorsque l'attaque informatique vise exclusivement les capacités opérationnelles des armées ou les chaînes de commandement de la défense.

**Elle permet d'obtenir certains avantages sur les théâtres d'opération des armées en** tirant parti des vulnérabilités des systèmes numériques adverses[3]. Elle élargit la palette des options modulables proposable au Président de la République en offrant **une capacité d'emploi d'initiative en opération extérieure : isolément ou en appui des moyens conventionnels, pour en démultiplier les effets et en renforçant l'arsenal offensif.**

Elle permet d'atteindre trois types d'objectifs opérationnels dans la conduite d'opérations militaires :

**1) renseignement** : évaluation de capacités militaires adverses : recueil ou extraction d'informations ;

**2) réduction voire neutralisation de capacités adverses** : perturbation temporaire ou création de dommages majeurs dans les capacités militaires ;

**3) déception** : modification des perceptions ou de la capacité d'analyse de l'adversaire (altération discrète de données ou systèmes,

---

[1] *https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive*

[2] *Éléments de doctrine publics, la doctrine en elle-même étant secrète. https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive*

[3] *L'arme cyber vise, dans le strict respect des règles internationales à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données.*

exploitation d'informations dérobées au sein d'un système d'information militaire).

Dans un article récent[1], d'anciens responsables des ministères de la défense et des affaires étrangères se sont interrogés sur l'intérêt pour la France de se doter de capacités de rétorsion en cas d'agression contre ses intérêts au-delà des seules opérations de riposte et d'entrave actuellement prévues à l'article L.2321-2 du code de la défense qui sont limitées à la seule fin de neutraliser les effets en attaquant les systèmes d'information à l'origine de l'attaque lorsque cette attaque menace les intérêts vitaux de la France (ou à l'article D. 3121-14-1 du code de la défense pour ce qui concerne uniquement les attaques contre les systèmes d'information du ministère des armées) et à distinguer des opérations de lutte informatique offensive confiée au COMCYBER dans le cadre des opérations extérieures. Afin de répondre à des tentatives de « cyber-coercition », ils appelaient à élargir la doctrine de janvier 2019 à la protection d'objectifs civils critiques en permettant d'engager aussi une riposte proportionnée à toutes attaques visant de tels objectifs.

(b) Une capacité interarmées

Sous l'autorité du Président de la République et aux ordres du chef d'état-major des armées, **le COMCYBER est l'autorité d'emploi de la capacité militaire cyber offensive**. Il a la responsabilité de concevoir, planifier et coordonner des opérations LIO au profit de la manœuvre interarmées[2]. Il assure la cohérence de la planification et de la conduite des actions de LIO avec les différents états-majors opérationnels et les services de renseignement, du niveau stratégique au niveau tactique.

Les opérations sont conduites par des unités spécialisées[3], dont l'expertise garantit l'analyse des risques et la maîtrise des effets, collatéraux voire fratricides, induits par la complexité du domaine. Leur action est pleinement intégrée à la manœuvre des armées, directement sur le terrain ou à distance.

---

[1] *Bernard Barbier, Jean-Louis Gergorin et Edouard Guillaud « Cybercoercition : un nouveau défi stratégique » Le Monde 28 janvier 2020.*

[2] *Réalisées sous l'autorité du sous-chef opérations de l'état-major des armées, concernent l'ensemble des interventions des forces armées françaises, ces opérations s'inscrivent dans le cadre de l'article 35 de la Constitution. La notion de théâtre d'opérations extérieures a bien un sens dans le domaine cyber« whitepaper» sur le droit international appliqué aux cyberopérations que la France a récemment proposé aux experts des Nations Unis (disponible en ligne sur le site internet du ministère).*

[3] *Le COMCYBER exerce un commandement fonctionnel sur le groupement des opérations numériques (GON) et le détachement des actions numériques (DAN) qui sont deux entités appartenant au commandement interarmées des actions sur l'environnement (CIAE) qui est le centre principal des armées en matière d'influence militaire. Le GON et le DAN sont les capteurs et les effecteurs du COMCYBER sur les médias sociaux.*

(c) La maîtrise des risques comme facteur de crédibilité et la promotion d'un comportement responsable comme facteur de stabilité

**La LIO est soumise, comme toute autre arme ou méthode de guerre, aux principes et règles du droit international, notamment le droit international humanitaire, ainsi qu'aux lois et règlements nationaux.** Elle n'est donc utilisée que dans le respect de règles opérationnelles d'engagement très restrictives. Le COMCYBER ne conduit pas d'opérations offensives sur le territoire national.

Mais la LIO recèle **des caractéristiques spécifiques** : immédiateté de l'action, dualité des cibles, hyper-connectivité sont autant de facteurs de risques qui ont été pris en compte dans l'élaboration de la doctrine; tout comme la notion d'irrégularité. Les actions offensives auxquelles nous faisons face dans le cyberespace ont, en effet, souvent le caractère de l'irrégularité[1].

**Ces caractéristiques imposent une maîtrise et un contrôle très stricts** du choix des modes d'action et de l'utilisation des moyens. Ce contrôle national vise notamment à éviter tout risque de détournement, de compromission ou de dommage collatéral d'une action dont les effets peuvent se propager au-delà de la cible visée en raison des interdépendances entre systèmes. **Pour en préserver l'efficacité et maîtriser les risques de détournement, l'ensemble des opérations de LIO menées par les forces armées demeure de nature secrète, mais les autorités politiques et militaires peuvent, selon les circonstances, les assumer publiquement voire les revendiquer. Cette posture est affaire de décision politique.**

### *B. UN MODÈLE DE GOUVERNANCE DE LA STRATÉGIE NATIONALE DE CYBERDÉFENSE*

**La cyberdéfense française repose sur un modèle d'organisation et de gouvernance qui sépare les missions et capacités offensives et défensives (*cf. supra*). Toutefois, il implique une très forte coordination entre ses deux pôles pour gagner en efficacité opérationnelle, tant pendant les cyberattaques qu'en amont de celles-ci tant qu'au niveau opératif au niveau stratégique[2].**

---

[1] *Ce milieu favorise les actions de type guérilla ou de harcèlement en raison de leur faible traçabilité et de la difficulté à les attribuer, de la grande difficulté à conserver dans la durée la maîtrise du cyberespace compte tenu de l'étendue du milieu et de sa complexité ce qui constitue un facteur permanent de vulnérabilité, et de la relative aisance pour les acteurs non-étatiques et les petits États d'accéder aux technologies nécessaires. Un outil de LIO peut être aisément volé copié ou imité par des adversaires ou des acteurs tiers. Il possède rarement les contraintes associées à des armes du haut du spectre réservées aux États possédant une certaine maturité technologique.*

[2] *C'est notamment l'un des enjeux de la future implantation de l'ANSSI à Rennes que de la rapprocher des autres acteurs du ministère des Armées (chaînes « action militaire » et « renseignement »)*

La Stratégie nationale de cyberdéfense de février 2018 **propose de renforcer les mécanismes de gouvernance et de cohérence technique de la cyberdéfense et d'en clarifier le fonctionnement en la formalisant autour de quatre chaînes opérationnelles.**

### 1. Une comitologie complète

*a) Le niveau politique*

**Les orientations et directives dans le domaine de la cyberdéfense sont prises en Conseil de défense et de sécurité nationale (CDSN).**

En plus du Conseil annuel consacré à la cybersécurité, **le Comité directeur de la cyberdéfense (dit « CODIR Cyber »)** a renforcé la coordination de l'action publique. **Ce comité** est chargé de suivre la mise en œuvre des décisions prises en matière de développement et d'organisation générale du domaine. Il n'intervient pas dans la conduite des opérations. Co-présidé par le chef de l'État-major particulier du Président de la République, le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) et le directeur de cabinet du Premier ministre, il se réunit une fois par an. Son secrétariat est assuré par le SGDSN. Les travaux du CODIR Cyber sont préparés par le comité de pilotage de la cyberdéfense (« COPIL Cyber »), placé sous la direction du cabinet du Premier ministre.

*b) Le centre de coordination des crises cyber (C4)*

Il est compétent pour les crises ne nécessitant pas la mise en œuvre de plans gouvernementaux, ainsi qu'en cas de publication de vulnérabilités majeures susceptibles d'être exploitées à court terme. Il est un mécanisme permanent d'analyse de la menace, de préparation et de coordination associant l'ensemble des ministères concernés par la crise.

Le C4 STRAT et sa déclinaison opérationnelle, le C4 TECHOPS, constituent les enceintes privilégiées pour le partage d'éléments, notamment techniques, entre les différentes entités. Cette mise en commun permet de croiser les informations pertinentes, déterminer les actions à entreprendre et se répartir la charge et la responsabilité de leurs mises en œuvre et d'activer les différentes chaînes opérationnelles.

Le C4 est l'enceinte privilégiée pour articuler l'action des différentes chaînes opérationnelles[1]. Il est structuré en quatre niveaux distincts :

---

[1] *Les caractéristiques et les finalités des cyberattaques sont les principaux critères qui conduisent à activer en priorité telle ou telle chaîne. A titre d'exemple, dans les cas de rançongiciels ou plus largement de cybercriminalité, l'activation rapide de la chaîne « judiciaire » est souvent pertinente car elle permet d'utiliser des leviers comme les gels de données ou les demandes d'entraide pénale internationale, afin de prévenir au plus vite la propagation éventuelle de l'attaque. Les victimes d'attaques informatiques sont libres de porter plainte si elles le souhaitent (le dépôt de plainte est généralement encouragé). Le parquet peut également ouvrir une instruction de son propre fait s'il l'estime nécessaire.*

*Tableau ******

• **Le C4 restreint permanent et technique à vocation technico-opérationnelle** permet une analyse partagée entre les services compétents, de la menace, des modes d'action et des acteurs menaçants ainsi que l'anticipation des réponses sur le court et moyen terme. Le niveau technico-opérationnel (C4 TECHOPS), dont les réunions sont hebdomadaires, permet de partager une analyse de la menace au travers d'échanges techniques. *****

• **Le C4 technique** présidé par le directeur général de l'ANSSI est une instance de coordination technique des responsable SSI et cyber des ministères activée en cas de crise nationale grave touchant plusieurs ministères. Il supervise l'emploi des moyens relatifs à la résolution des crises cyber de moindre ampleur, structure le dialogue entre les représentants des différents acteurs pour établir une évaluation technique de la crise en cours, veille à la cohérence des décisions techniques des services et l'État et à celle des mesures techniques avec les acteurs non cyber de la gestion de crise et fournit des éléments consolidés à la cellule interministérielle de crise (CIC) si elle est activée. Depuis la publication de la RSC en février 2018, aucune situation opérationnelle n'a nécessité l'activation de cette formation.

• Présidé par la SGDSN, **le niveau stratégique (C4 STRAT)** se réunit mensuellement afin de définir puis proposer aux autorités les stratégies de réponse les plus adaptées aux grandes menaces cyber. À ce titre, il favorise, par la confrontation des expertises de ses membres la préparation des options de réponse portées par les ministères et acteurs concernés lors de la crise. *****

*c)* *****

*****

*d)* *****

*****

*e) Autres instances de coordination impliquant des services de renseignement*

En dehors de la comitologie propre à la politique publique de cyberdéfense. Des instances de coordination existent dont l'objet portent sur des domaines connexes mais néanmoins très liés aux traitements des

*Dans les cas d'espionnages, le travail de qualification et d'analyse de l'impact de l'attaque par la chaîne « protection » peut s'avérer beaucoup plus long et souvent complexe. Il peut alors être nécessaire de temporiser l'activation de la chaîne « judiciaire » pendant ce temps (en coordination avec le parque). Le dépôt de plainte est susceptible d'entraîner l'activation de la chaîne « judiciaire ». Dans la majorité des cas, il fait l'objet d'échanges entre la chaîne « protection » et le parquet cyber quant à l'opportunité et au moment le plus propice pour le faire*

menaces dans le cyberespace et recourent à la contribution des services de renseignement.

Ainsi le Comité de lutte contre la manipulation de l'information (CLMI) piloté par le SGDSN, focalisé sur la menace exogène regroupe les MEAE, la DGSE, la DGSI, le SIG, la CNRLT, le MININT, le MINARM, le Ministère de la Culture et le porte-parolat.

La DGSI participe au GIP-ACYMA (plate-forme de signalement des actes de cyber malveillance et d'assistance aux victimes) aux côtés de la DMISC, de la DCPJ, de la DGPN et le la DGGN. Elle participe également avec la DMISC et l'ANSSI au groupe de travail « Technologies critiques et entreprises stratégiques du comité de filière des industries de sécurité (COFIS) » animé par le SISSE et le SGDSN qui participe à l'élaboration de la cartographie des entreprises stratégiques de la filière des industries de sécurité afin de mettre en œuvre un suivi spécifique des service de l'État ainsi qu'à la commission interministérielle de défense et de sécurité (CIDS), animée par le SGDSN, avec les HFDS, la DGPN, la DGGN, la DRSD et l'ANSSI, qui coordonne la mise en œuvre du dispositif de sécurité des activités d'importance vitale.

### 2. Quatre chaînes opérationnelles

Les quatre chaînes opérationnelles prévues par la Revue stratégique de cyberdéfense (*cf. supra*) ont été mises en place.

La chaîne « protection » est animée par le SGDSN. Le directeur général de l'ANSSI y est responsable des opérations de cyberdéfense. Cette responsabilité est déléguée au COMCYBER pour ce qui concerne les systèmes d'information du ministère des armées. **Les services de renseignement sont susceptibles de contribuer à cette mission de protection en alimentant la chaîne, notamment à travers le dispositif du C4, avec des éléments relatifs à la connaissance et à l'anticipation de la menace d'origine cyber.**

**S'agissant de la chaîne « renseignement », elle recouvre sous l'autorité du Gouvernement, l'ensemble des actions entreprises dans un but de renseignement et notamment en vue d'attribution.** Le document rappelle les règles applicables en matière d'utilisation des techniques de renseignement, donne pour mission au CNRLT, ***** de favoriser le partage du renseignement d'intérêt cyber entre les services et indique qu'il peut ponctuellement s'appuyer sur l'inspection des services de renseignement pour assurer un rôle de conseil et de contrôle des capacités.

## III. LES SERVICES DE RENSEIGNEMENT DANS LA POLITIQUE PUBLIQUE DE CYBERDÉFENSE

*L'étude est limitée aux services du premier cercle.*

**Les services de renseignement contribuent à la politique publique de cyberdéfense** pilotée par l'ANSSI et le COMCYBER en assurant la protection de leurs systèmes d'information, en participant à l'anticipation, à la détection et à l'attribution des cyberattaques par la fourniture de renseignement d'intérêt cyber et, dans certains cas, aux actions entreprises dans le domaine de la lutte informatique défensive, de l'action militaire et de l'action judiciaire.

**Ils réalisent également leurs missions traditionnelles dans le cyberespace**, le renseignement d'origine cyber constitue désormais une source importante d'information (*cf.* IV du présent chapitre).

### *A. LES MISSIONS GÉNÉRALES*

#### **1. *****

*****

*a)* *****

*****

(1) *****

*****

(a) *****

*****

(b) *****

*****

(c) *****

*****

(d) *****

*****

(e) *****

*****

*b)* *****

*****

(1) *****

*****

(2) *****

*****

(a) *****

*****

(b) *****

*****

### 2. Les services de renseignement participent ponctuellement à la mission de prévention

Le degré de prise de conscience des risques numériques reste encore insuffisant et nombre d'entreprises ou de collectivités peinent à dégager les ressources nécessaires à leur cybersécurité. La mission de prévention et de sensibilisation définie par la RSC revêt un caractère interministériel et s'appuie localement sur l'action des préfets et des services de l'État. Dans le cadre de cette mission qui incombe principalement à l'ANSSI et au COMCYBER pour le périmètre du ministère des armées, certains services de renseignement apportent leur contribution notamment aux entités auprès desquelles ils assurent une mission spécifique. C'est le cas de la DRSD auprès des partenaires industriels et services du ministère des armées, et de la DGSI et du renseignement territorial dans le cadre de la politique de protection des intérêts économiques, par exemple.

*a) La contribution de la DRSD à la mission de prévention*

Une des principales missions de la DRSD, service enquêteur et inspecteur du ministère des armées, est la protection du secret de la défense nationale et du potentiel scientifique et technique de la Nation, dans le périmètre des entités ou établissements relevant de l'autorité de la ministre ainsi que des entreprises intéressant la défense. Elle participe, à ce titre, à l'élaboration des mesures nécessaires à la protection des informations et des matériels sensibles intéressant la défense et en contrôle l'application[1].

La prévention et la sensibilisation au risque cyber font aussi partie de sa mission de contre-ingérence, en renseignant sur les menaces

[1] *La DRSD effectue des inspections et des contrôles inopinés sur les SI du ministère et les organismes de tutelle sur demande du HFCDS ou de la DPID. Les comptes rendus sont communiqués au COMCYBER.*

potentielles ou avérées, en alertant sur les vulnérabilités et en contribuant aux mesures d'entrave et de protection.

Elle coopère dans cet espace avec les autres services de renseignement et agit en complémentarité avec l'ANSSI et le COMCYBER[1] auprès desquels elle dispose d'officiers de liaison.

*b) La contribution de la DGSI*

Dans le cadre de ses actions de sensibilisation aux risques de contre-ingérence, la DGSI mène des actions de sensibilisation auprès des institutions publiques et des entreprises, auxquelles le renseignement territorial est ponctuellement associé en région.

La DGSI mène également des sensibilisations au risque cyber auprès des entreprises et entités avec lesquelles elle est en relation, à travers le réseau territorial cyber créé à la fin 2019.

*c) Une évaluation insuffisante de cette politique*

Dans son rapport sur les missions et effectifs de l'État contribuant à la cybersécurité, de février 2019, la mission commune d'inspection[2] relevait qu'« *au-delà de l'absence de coordination ministérielle, les actions de prévention et de sensibilisation ne sont pas encadrées par une stratégie nationale et souffrent de plusieurs faiblesses* » : objectifs insuffisamment définis, publics insuffisamment segmentés, canaux de communication insuffisamment articulés, absence d'évaluation structurée. Elle proposait d'impliquer davantage le GIP Acyma dans ce nécessaire travail de coordination.

S'agissant de la DGSI et de la DRSD qui participent à cette mission de prévention, la DPR demande qu'elles soient associées à cette réflexion.

**Recommandation n° 55 : Associer la DGSI et la DRSD à la réflexion sur la coordination institutionnelle et la définition d'une stratégie nationale de prévention et de sensibilisation aux risques cyber.**

[1] *La coordination avec la DRSD se fait via le commandement de la cyberdéfense, point d'entrée privilégié de l'ANSSI au sein du ministère des armées. Les relations avec la DRSD avec le COMCYBER s'articulent autour de la présence d'un officier de liaison de la DRSD au sein du centre des opérations cyber du COMCYBER et de deux réunions de coordination : une réunion mensuelle « SSI/Cyber » présidée par le chef du cabinet militaire de la ministre des armées et une réunion trimestrielle « défense et sécurité » présidée par le chef de cabinet de la ministre.*

[2] *Contrôle général des armées, Conseil général de l'économie, Inspection générale de l'administration, Inspection générale des finances, Inspection générale de la Justice*

### 3. Les services de renseignement apportent une contribution majeure aux missions d'anticipation, de détection et d'attribution des cyberattaques

*a) Les différentes missions pour lesquelles les services sont appelés à concourir*

(1) La mission d'Anticipation

Les attaques peuvent être anticipées (prévenues, atténuées ou neutralisées dans leurs effets) par le biais d'une meilleure connaissance des groupes d'attaquants. L'ANSSI estime à une soixantaine le nombre de modes opératoires différents actuellement mis en œuvre par des groupes d'attaquants susceptibles de porter atteinte à des intérêts relevant de la sécurité nationale.

Les services de renseignement contribuent au recueil des informations sur ces groupes et sur leurs modes d'action qu'ils font remonter vers le C4 sous forme de notes. Les relations entretenues avec les services de renseignement relevant du ministère des armées, notamment la DGSE, la DRSD et la DRM, permettent au COMCYBER de disposer du soutien ***** afin de caractériser les menaces pesant contre le ministère[1].

(2) La mission de Détection

La détection d'une attaque est liée à l'observation des effets de l'attaque ou à l'identification d'éléments techniques liés au mode opératoire de l'attaquant. Ces éléments peuvent provenir de sociétés privées de cybersécurité, de partenaires étrangers, des services de renseignement ou de l'administration. Ils sont centralisés à l'ANSSI qui doit assurer la bonne coordination de différentes entités. En plus de ce travail de consolidation et de coordination, elle a en charge la détection des attaques sur les systèmes de l'administration (et, depuis la LPM 2019-2024, dans certains cas, sur les réseaux des opérateurs de communications électroniques et sur les systèmes d'information des fournisseurs de service de communication au public en ligne). Le COMCYBER, par délégation de l'ANSSI assure la détection sur le périmètre des armées.

Les capacités des services de renseignement dans le domaine de la détection sont complémentaires. Si l'ANSSI est résolument tournée vers les victimes, les services sont susceptibles d'utiliser leurs capteurs pour détecter « plus au loin » *****. Les services de renseignement ont donc une place importante dans ce dispositif de détection.

---

[1] *Il peut s'appuyer sur les capacités de ces services pour compléter ses analyses, les deux premiers disposant de leurs propres capacités de détection pour la protection de leurs systèmes d'information.*

(3) La mission d'Attribution

Après la détection d'une attaque, il est essentiel de remonter à l'instigateur afin de lancer des poursuites judiciaires ou de préparer une réponse adaptée.

Le repérage des indices[1], réalisé lors de la détection de l'attaque et de l'investigation qui s'en suit, est souvent insuffisant pour obtenir des éléments probants. Pour les compléter, les services de renseignement peuvent agir aux moyens de toute la palette de leurs capacités propres.

**La décision d'attribution formelle d'une attaque majeure à son auteur ou à son commanditaire reste une décision politique**. *****

*****

**À ce jour, la France n'a jamais entrepris d'attribution publique**. Cela tient en grande partie à sa volonté de conserver un dialogue stratégique et opérationnel franc et direct avec l'ensemble des homologues étrangers, y compris ceux susceptibles d'être impliqués dans des cyberattaques ciblant la France.

*****

*b) La contribution des services à la chaîne renseignement*

À la suite de la Revue stratégique de cyberdéfense, a été structurée *« sous l'autorité du Gouvernement, une chaîne opérationnelle « renseignement» qui recouvre l'ensemble des actions entreprises dans un but de renseignement et notamment en vue d'attribution »*, y compris par la mise en œuvre de capacités offensives. Les services doivent mobiliser leurs moyens au service de la cybersécurité des intérêts nationaux en collectant les renseignements d'intérêt cyber (RIC). Les renseignements peuvent être issus d'une collecte sur une victime, fournis par des partenaires, ou de capteurs spécialisés tels que le ROEM (origine électromagnétique) et le ROHUM (origine humain) ou non, tel que le ROSO (origine source ouverte).

*****

(1) *****

*****

(2) *****

*****

(3) *****

*****

[1] *Par une société privée, les services de police et de gendarmerie ou bien l'ANSSI.*

*c) L'utilisation des techniques de renseignement pour le recueil de renseignement d'intérêt cyber*

Lorsqu'une cyberattaque menace les intérêts fondamentaux de la Nation[1], les services spécialisés de renseignement agissant dans le cadre de leurs missions peuvent solliciter la mise en œuvre d'une technique de renseignement pour compléter les informations dont ils disposent sur le plan national ou international, du fait de l'action de leurs agents ou par leurs partenaires, dans les conditions prévues par les lois **du 24 juillet et du 30 novembre 2015**, **dans la limite des sept finalités définies par celles-ci, après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et autorisation par le Premier Ministre**. Les autorités d'emploi sont les directeurs des services concernés, sous l'autorité de leur ministre de tutelle.

**La question avait été évoquée d'une finalité spécifique liée à la cybersécurité**, **elle avait été écartée au motif que les techniques utilisées par les attaquants ne constituaient pas en elles-mêmes une finalité mais un simple moyen et que leur utilisation s'inscrivait dans la réalisation d'une finalité prévue par la loi pour justifier l'utilisation d'une technique de renseignement.**

Sur le périmètre cyber, en raison de la nature même de la matière, qui est à la fois mondiale et mouvante, les techniques utilisées plus particulièrement, mais non exclusivement sont le dispositif technique de surveillance internationale (DTSI, articles L. 854-1 et suivants du Code de la Sécurité Intérieure, CSI) et le recueil de données informatiques, qu'elles soient sous la forme de copies de supports numériques ou d'interception de flux (article L. 853-2 du CSI). Ces techniques sont également utilisés aux fins de renseignement pour prévenir ou entraver d'autres menaces, on parle alors de renseignement d'origine cyber (ROC) (*cf. infra*).

D'autres techniques peuvent être mises en œuvre et utilisées au profit de la matière, comme des interceptions de sécurité (articles L. 852-1 et suivants du CSI), ou encore la mise en œuvre des accès administratifs aux données de connexion (articles L. 851-1 CSI).

Les demandes d'autorisation d'utilisation d'une technique de renseignement (TR) présentant une dimension « cyber » sont donc toujours attachées à une finalité de l'article L.811-3 du code de la sécurité intérieure.

---

[1] *Limitativement énumérés à l'article L. 811-3 du code de la sécurité intérieure : 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; 4° La prévention du terrorisme ; 5° La prévention : a) Des atteintes à la forme républicaine des institutions ; b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive.*

Dès lors, il est difficile de distinguer, au sein des services l'utilisation des TR, y compris de celles mises en œuvre pour recueillir des renseignements d'origine cyber, celle mises en œuvre pour la recherche de renseignement d'intérêt cyber. Nombre de services ont indiqué ne pas réaliser de décomptes spécifiques.

*****

**On notera toutefois que le législateur à l'occasion de l'examen de la loi de programmation militaire du 13 juillet 2018, a introduit des dispositions permettant que des vérifications ponctuelles puissent porter sur des correspondances utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national**, qui sauf exception prévue à l'article 854-2 du CSI sont prohibées, **pour deux finalités exclusivement** : la détection, en cas, d'urgence, d'une menace terroriste et **la détection d'une attaque informatique susceptible de porter atteinte aux intérêts fondamentaux de la Nation**. La CNCTR a indiqué que si elle fournit désormais une statistique sur le nombre d'avis préalables rendus au titre de la surveillance internationale, elle n'est pas en mesure de préciser d'emblée les cas relatifs à une attaque informatique.

*****

**Cette situation est regrettable car elle ne permet pas d'évaluer concrètement l'action des services de renseignement au profit de la cyberdéfense.**

**La DPR demande la mise en place d'un outil statistique permettant de recenser les autorisations d'utilisation des techniques de renseignement accordées pour le recueil de renseignement d'intérêt cyber. Ces éléments seront pris en compte dans le dispositif d'évaluation de la contribution des services de renseignement à la politique publique de cyberdéfense souhaité par la DPR (*cf.* recommandation n° 59).**

*d) Le besoin de disposer d'un outil d'évaluation de la contribution des services au renseignement d'intérêt cyber*

Bien évidemment, l'évaluation de cette contribution à travers le seul recensement des autorisations d'utilisation de TR accordées est insuffisante mais elle constituera une première brique dans la constitution d'un outil d'évaluation nécessaire aux autorités de l'État et aux services eux-mêmes qui devraient également recenser les notes produites et transmises, en les répertoriant selon leurs objectifs (anticipation, détection, attribution). Cet outil devrait également permettre de mesurer la pertinence des renseignements ainsi collectés et l'utilisation qui en a été faite.

**Le travail de synthèse et d'évaluation de ces informations n'est pas réalisé actuellement.**

Le rapport annuel d'activité des services spécialisés de renseignement et des services mentionnés à l'article L.811-4 du CSI établis en

vertu des dispositions de l'aliéna 3° de l'article 6 *nonies* de l'ordonnance n°58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées ne contient pas de statistiques de cette nature. La seule statistique ayant un lien avec le cyberespace qu'il produit, concerne au titre des mesures d'entrave et de neutralisation à caractère administratif, les déréférencement et blocages de site internet.

**Pourtant, un outil d'évaluation fondé sur un recueil de statistiques est indispensable aux autorités de l'État, y compris le Parlement, pour évaluer de manière objective, la contribution des services de renseignement à la politique publique de cyberdéfense qui fait d'ailleurs aussi partie de leur mission au titre de la politique publique du renseignement, définie par la Stratégie nationale et le PNOR.**

**La DPR demande, en conséquence, au CNRLT de conduire une étude sur les outils nécessaires à l'évaluation de la contribution des services à la chaîne « renseignement » de la cyberdéfense**. Il en a les compétences. La RSC indique en effet : *« Le CNRLT favorise, le partage de renseignement d'intérêt cyber. Il peut ponctuellement s'appuyer sur l'inspection des services de renseignement pour assurer un rôle de conseil et de contrôle des capacités »*.

**Cet outil d'évaluation devra pouvoir mesurer l'efficacité des services de renseignement en matière de recueil et d'analyse du renseignement d'intérêt cyber. Il constituera un élément important du dispositif d'évaluation de la contribution des services de renseignement à la politique publique de cyberdéfense souhaité par la DPR (*cf.* recommandation n° 59).**

### 4. Les services de renseignement peuvent agir aux fins d'action

Le dernier volet de la cyberdéfense consiste à permettre la réalisation d'actions destinées à entraver ou faire cesser une cyberattaque, en réprimer pénalement les auteurs et commanditaires, ou pour appuyer des opérations militaires. Dans chacune de ces actions, les services de renseignement, peuvent être mis à contribution.

*a) Les capacités d'entrave ou d'interruption d'une attaque en cours*

L'article L.2321-2 du code la défense prévoit que « *pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque* ». **Il donne donc au Premier ministre les outils**

**juridiques indispensables pour permettre de défendre les infrastructures d'importance vitale contre une cyberattaque dans un cadre légal[1].**

Telles qu'elles ont été définies par le Premier ministre dans l'instruction classifiée du 7 mars 2016, les conditions de mise en œuvre de ce dispositif prévoient une coordination de l'action des différents services concernés sous la responsabilité de l'ANSSI qui définit, organise et dirige les opérations techniques nécessaires à la neutralisation des effets d'une attaque informatique, après une évaluation préalable des conséquences potentielles des opérations techniques envisagées. *****.

*****

*****. **Les conditions de mise en œuvre de cet article n'ont pas encore été rencontrées**. *****.

*b) Les capacités de répression pénale des auteurs*

Une attaque informatique peut entraîner le déclenchement d'une enquête judiciaire. *****

La chaîne « investigation judiciaire » recouvre l'action des services de police et de gendarmerie et de la justice. Sous le contrôle de l'autorité judiciaire, certains services sont chargés de mettre à disposition des services d'enquêtes, spécialisés ou non, des outils et techniques modernes d'investigation. *****

(1) *****

*****

**Le périmètre de compétence de la SDAJ**

Elle est chargée de diligenter des enquêtes judiciaires lors de la commission d'une ou plusieurs infractions de cybercriminalité prévues aux articles 323-1 et suivants du code de procédure pénale, au préjudice des acteurs suivants : opérateurs d'importance vitale (OIV) entreprises à protéger en priorité (EPP), entreprises comprenant des ZRR (zones à régime restrictif), entreprises ni OIV, ni EPP mais "*particulièrement innovantes*", ministères et administrations d'État[2] qui sont déjà suivis par la DGSI au titre de ses missions de contre-ingérence, d'intelligence économique et de sécurité des infrastructures sensibles et institutions publiques;

[1] *Dans une récente tribune (*Le Monde 28 janvier 2020*), d'anciens responsables des ministères de la défense et des affaires étrangères se sont interrogés sur la définition de la nature de l'attaque informatique justifiant la mise en œuvre des opérations de riposte et d'entrave visées à l'article L.2321-2 du code de la défense estimant qu'elles devraient «* couvrir le prépositionnement d'implants *». La rédaction actuelle de l'article ne l'interdit pas. Le prépositionnement d'implants pourrait être considéré comme des actes préparatoires ou comme le commencement d'exécution d'une attaque.*

[2] *Par ailleurs, la DGSI peut également saisir lorsqu'il s'agit d'une entreprise non énumérée, a parmi ses clients des entités qui seraient, elles, des OIV, EPP ou des administrations de l'État.*

**Le protocole actuel de répartition des enquêtes réserve à la DGSI les faits d'atteinte aux intérêts fondamentaux de la Nation commis au préjudice des acteurs énumérés** et écarte les infractions dont le but est de nature crapuleuse[1] Une quarantaine de procédures sensibles sont traitées annuellement par le service, dont une vingtaine sous l'autorité du parquet de Paris[2].

*****

(2) D'autres services peuvent ponctuellement concourir aux investigations judiciaires

**Tracfin** n'est pas un service de police judiciaire mais un partenaire, pouvant fournir de l'information *via* ses transmissions ou en réponse aux réquisitions qui lui sont transmises. Le service a créé en juillet 2018 une cellule dédiée à la lutte contre la cybercriminalité financière. Parmi les transmissions d'informations à l'autorité judiciaire, il est à noter des dossiers liés à des paiements de *ransomware* par des crypto-actifs (soit des délits d'introduction frauduleuse de données et modification dans un système automatisé de données et d'entrave au fonctionnement d'un système automatisé de données), des escroqueries dont le produit est converti en crypto-monnaies, un dossier de blanchiment par des crypto-actifs du produit de la vente de cartes bancaires volées et commercialisées notamment sur le *darknet*, un dossier de *cryptojacking* (installation d'un malware minant du bitcoin).

Conformément aux dispositions définies par la Revue stratégique de cyberdéfense, **la DRSD** n'est pas un acteur de la chaîne judiciaire. Néanmoins sur son périmètre et dans le cadre de ses missions, le service transmet à la direction des affaires juridiques du ministère des Armées les éléments qui sont susceptibles d'être dénoncés au procureur de la République près le tribunal judiciaire de Paris (art. 40 ou 698-1 du code de procédure pénale).

En revanche, la **DGSE** ne traite pas de cybercriminalité, ne prélève pas de traces techniques d'attaques en France aux fins de poursuites judiciaires, par exemple.

*c) L'action militaire*

La numérisation offre l'opportunité d'actions cyber en soutien aux opérations militaires. Quelques pays utilisent déjà massivement des moyens cyber pour réaliser des opérations de renseignement ou soutenir des

[1] *Cependant, cette distinction est parfois difficile à réaliser d'emblée, notamment dans certains cas de personnes morales victime d'un rançongiciel. Dans ces cas, il arrive que la DGSI soit co-saisie avec un autre service judiciaire (OCLCTIC, C3N ou BEFTI) un dessaisissement de l'enquête pouvant intervenir ultérieurement.*

[2] *Rapport de la mission commune d'inspection sur les missions et effectifs de l'État contribuant à la cybersécurité - février 2019.*

opérations spéciales (l'exemple le plus marquant reste celui de la Russie en Crimée et dans le Donbass).

L'arme cyber est un outil qui peut être très sélectif et dont les effets peuvent être réversibles. Utilisées pour garantir la supériorité dans le cyberespace, les capacités cyber permettent aussi aux armées de mener leurs opérations traditionnelles de manière plus efficace et moins coûteuse.

La France a déjà investi dans ce domaine et la capacité cyber est désormais intégrée à toutes les opérations militaires (voir les discours des ministres Jean-Yves Le Drian le 12 décembre 2016 et de Florence Parly le 18 janvier 2019).

(1) Les services de renseignement en appui du COMCYBER dans la LIO

*****

Le COMCYBER assure la cohérence de la planification et de la conduite des actions cyber :

- au niveau stratégique, avec les commandements opérationnels et directions concernées ;

- aux niveaux opératif et tactique, avec les commandants de forces (un officier de liaison cyber peut être mis en place auprès de l'autorité de théâtre), qui disposent également d'officiers de liaison des services de renseignement.

Le COMCYBER et la DRM conduisent des réunions bilatérales pour coordonner leurs activités opérationnelles et de développement capacitaire.

*****

(2) *****

*****

## IV. LE CYBERESPACE : NOUVEAU TERRAIN D'ACTION DES SERVICES DE RENSEIGNEMENT

À côté des missions menées pour soutenir la politique de cyberdéfense, et dans le cadre de leurs missions respectives de renseignement, les services recueillent et exploitent le renseignement d'origine cyber à partir des innombrables sources en libre accès sur l'Internet, mais aussi aux moyens de techniques qui font l'objet lorsqu'elles sont mises en œuvre sur le territoire national ou concernent au moins un identifiant rattaché au territoire national d'un encadrement légal au titre des lois de 2015 sur le renseignement et sur la surveillance des communications internationales.

### *A. LES DONNÉES DE SOURCES OUVERTES*

**Face à la masse de ces données, l'efficacité des services dépend de leurs capacités à les sélectionner, à les traiter en nombre au moyen de puissantes solutions d'analyse et de calcul recourant aux technologies du *big data* et de l'intelligence artificielle, et à les fusionner avec les renseignements recueillis par d'autres sources ou techniques. Un effort de recherche, de conception et de développement de solutions est poursuivi depuis plusieurs années en ce domaine** *(cf. infra).*

### *B. L'UTILISATION DE TECHNIQUES DE RENSEIGNEMENT*

Pour l'ensemble de leurs missions de renseignement les services du premier cercle peuvent mettre en œuvre les techniques de renseignement qui leurs sont ouvertes soit par la loi du 24 juillet 2015 sur le renseignement soit par celle du 30 novembre 2015 sur la surveillance des communications électroniques internationales, lorsque le besoin opérationnel le justifie.

**Sur le périmètre cyber, *stricto sensu*, les techniques utilisées sont le dispositif technique de surveillance internationale (DTSI, articles L. 854-1 et suivants du Code de la Sécurité Intérieure, CSI) et le recueil de données informatiques, qu'elles soient sous la forme de copies de supports numériques ou d'interception de flux (article L. 853-2 du CSI).**

#### 1. Les techniques de renseignement ouvertes par la loi du 24 juillet 2015

*a) Des techniques utilisées par trois services uniquement*

**À l'exception de Tracfin[1], les services du premier cercle sont tous autorisés à collecter du renseignement par le biais d'opérations autorisées sur le fondement de l'article L.853-2 du CSI soit de recueil de données informatiques (RDI, article L.853-2-1°) soit de captation de données informatiques (CDI, article L.853-2-2°). Mais tous ne l'utilisent pas.**

**Ces techniques sont complexes à mettre en œuvre et les agents qui opèrent doivent être individuellement désignés et habilités.**

**La première technique est utilisée largement par les services. En 2019, elle a fait l'objet de plus de 4060 demandes (contre plus de 3350 en 2018), la seconde très rarement, 3 demandes en 2019 (contre 4 en 2018)[2].**

S'agissant de la mise en œuvre effective, le nombre de demandes ne reflète pas nécessairement la mise en œuvre réelle des techniques. Le CNRLT a réalisé une enquête qui montre une mise en œuvre effective inférieure à 50 %. Ceci est dû « *à l'absence d'opportunité opérationnelles pour la mise en œuvre*

[1] *Tracfin ne sollicite pas d'évolutions législatives à cet égard.*
[2] *Source : CNCTR.*

*ou à la nécessité d'effectuer une demande de renouvellement dans l'attente d'une telle opportunité. En effet, le décompte du temps d'autorisation commence dès la signature du Premier ministre. Ainsi les services peuvent être amenés à soumettre à nouveau des demandes sur le même objectif, l'opportunité opérationnelle ne s'étant pas présentée dans la durée d'autorisation, augmentant inutilement la charge administrative, de l'ensemble des acteurs impliqués dans le processus d'autorisation*[1] ».

*****. Compte tenu de la difficulté de distinction des domaines informatiques de stock (RDI) et de flux (CDI), seul le RDI est utilisé. *****

**Toutes finalités confondues, la DGSE** utilise de façon régulière la RDI et indique que la captation de données informatiques n'a fait l'objet que d'une vingtaine de demandes initiales. Seules quelques-unes ont fait l'objet de demandes de renouvellement, parfois à plusieurs reprises. Ces demandes de renouvellement s'expliquent par les difficultés techniques de ces opérations qui nécessitent un très long travail préparatoire.

La **DNRED** a également recours, en tant que de besoin, à la mise en œuvre de techniques de renseignement (TR). *****

Opérant principalement hors du territoire national dans un objectif de renseignement d'intérêt militaire, la **DRM** n'a, à ce jour, pas sollicité l'autorisation de mettre en œuvre ces techniques de renseignement auxquelles elle peut légalement avoir recours. Il en va de même pour la **DRSD** à ce jour.

*b) Un assouplissement des règles sollicité par la DGSI*

Actuellement les 1° et 2° de l'article L. 853-2 du CSI qui font une distinction entre le recueil de données informatiques (données stockées dans un système informatique), dont la durée d'autorisation est de 30 jours, et la captation de données informatiques (données informatiques captées sous forme de flux), dont la durée d'autorisation est de 2 mois. Très complexe, cette distinction est impossible à mettre en œuvre, et conduit à ne solliciter que la technique de recueil de données informatiques, la plus restrictive, en plein accord avec la CNCTR. Pour coller à la réalité opérationnelle et technique mais aussi pour donner une meilleure lisibilité au dispositif législatif, le regroupement en un seul régime juridique avec un délai de réalisation de deux mois, qui au surplus éviterait les renouvellements répétés de demandes de techniques qui n'ont pu être réalisées pour des raisons opérationnelles, est souhaité (*cf.* recommandation n° 5). Cet assouplissement est également considéré comme souhaitable par la DNRED.

[1] *CNRLT Rapport annuel d'activité des services spécialisés 2018 p.73.*

### 2. Les techniques relevant de la surveillance internationale

La majorité des cibles évoluant à l'extérieur du territoire national, la DGSE utilise principalement les mesures de surveillance internationale prévues par les articles L.854-1 et suivants du CSI. Elle s'est dotée à ce titre d'installations destinées à fournir aux autorités publiques, une capacité de renseignement efficiente.

Depuis l'entrée en vigueur de la loi de programmation militaire 2019-2025 et l'élargissement des possibilités d'exploitation des données collectées dans le cadre de la surveillance internationale, la CNCTR a indiqué avoir rendu 971 avis en 2018 et 2133 en 2019. Le rapport n'indique pas la répartition par services mais tout indique que ces nouvelles capacités ont été rapidement et pleinement utilisées par les services et notamment par des services qui y recouraient peu jusqu'à présent[1], en particulier les services de sécurité intérieure (*cf.* chapitre I).

### 3. Les outils spécifiques

*a) La DNRED*

**La DNRED** mène des investigations sur Internet pour lutter contre la cybercriminalité. Elle cible les profils d'internautes se livrant à de la fraude douanière (tabac, contrefaçons, stupéfiants, armes, biens culturels, produits de santé, espèces protégées) afin de les « désanonymiser » et de mettre un terme à leurs agissements.

*****

Dans ce cadre, elle a recours aux pouvoirs du code des douanes (notamment l'article 65 quinquies, entré en vigueur le 1er janvier 2019, qui permet l'obtention d'informations auprès des fournisseurs d'accès à Internet et des hébergeurs de données en ligne) dans le cadre d'enquêtes administratives, après autorisation du procureur de la République compétent. *****.

Une fois la fraude détectée, les services mettent en œuvre les pouvoirs du code des douanes pour identifier les personnes concernées, puis procéder aux interpellations et investigations douanières[2]. A l'issue de la retenue douanière, le Procureur de la République territorialement compétent décide des suites à donner à l'enquête judicaire qui peut être poursuivie par le service national de douane judiciaire (SNDJ) ou par un autre service de police judiciaire.

---

*1* *****

*2 Dans le cadre de la mise en œuvre de coups d'achat ou d'enquête sous pseudonyme, un contact est pris au cours des investigations avec le parquet territorialement compétent pour obtenir son autorisation ou l'informer de l'action envisagée.*

**Activité et résultats de Cyberdouane**

L'unité Cyberdouane de la DNRED est chargée de la lutte contre les infractions douanières sur le clearnet et le darknet. Ce service exerce son activité principalement sur initiative, mais est également sollicité par les services douaniers (DNRED ou services territoriaux) en assistance sur des problématiques nécessitant une expertise technique particulière.

Le service ouvre chaque année plusieurs centaines d'enquêtes qui donnent lieu à l'exercice de nombreux droits de communication visant à désanonymiser les cibles.

*****

En 2018 et 2019, Cyberdouane a privilégié le démantèlement de forums du darknet, induisant un fort engagement de ses agents *****. Les plateformes Black Hand (2018) et French Deep Web Market (2019)[1], ainsi que les plateformes satellites, ont été démantelées à cette occasion, occasionnant une très forte baisse d'activité sur la partie francophone du *darknet*.

*****

*b) Tracfin*

Dans le cadre de ses missions, **Tracfin** traite depuis de nombreuses années et sous l'angle financier des dossiers en lien avec la criminalité organisée recourant au cyberespace. Les investigations sous forme de ROSO (renseignement d'origine source ouverte) viennent ainsi en appui des investigations financières du service[2]. La cybercriminalité a su s'adapter à la recomposition du secteur financier, notamment au travers des *fintech*[3].

[1] *Ainsi elle a permis de démanteler le 12 juin 2019 d'une immense plateforme du* darkweb *francophone nommée* « French-Deep-Web-Market » *sur laquelle les internautes pouvaient se procurer des stupéfiants, des rames ou encore des faux papiers. Cette opération qui a visé 5 sites distants a mobilisé 90 agents de la DNRED, de la police nationale et de l'ANSSI. Les administrateurs et développeurs de la plateforme ont été arrêtés, des matériels saisis ainsi que des cryptomonnaies. Auditionnées en retenue douanière, les suspects ont été remis à la police judiciaire.*

[2] *Ces dossiers portent par exemple sur des escroqueries aux placements financiers à l'encontre de très nombreux particuliers : placements aux investissements sur les options binaires, les diamants, le FOREX, les terres rares, les vaches laitières, etc. Ces escroqueries utilisent les facilités offertes par Internet pour démarcher leurs clients à distance (*cf. Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018*).*

[3] *Le service constate une hausse des dossiers avec des fraudes à l'usurpation d'identité dans le cadre de la digitalisation des relations d'affaires financières* (cf. Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2018-2019*).*

**La cellule de lutte contre la cybercriminalité financière**

Créée en juillet 2018, cette cellule traite de tous les dossiers liés aux crypto-monnaies et effectue dans le cadre de son activité des recherches sur le *darknet*[1]. *****. Les investigations ont une importante composante internationale. Le canal spécifique de coopération des cellules de renseignement financier permet ainsi d'obtenir des informations financières, souvent de grande qualité. Dans le cadre du renseignement cyber, son activité a, depuis sa création, pris plusieurs formes qu'il s'agisse de transmissions d'informations à l'autorité judiciaire ou de transmissions d'informations aux services de renseignement du premier cercle comme des dossiers d'achats ou de tentatives d'achat d'arme sur le *darknet* par des particuliers et par le biais de crypto-monnaies, un dossier de financement de terrorisme *via* des crypto-actifs et une étude financière sur une société spécialisée du secteur de la cryptographie.

*c) La DRM*

La **DRM** dispose en propre du centre de recherche et d'analyse du cyberespace (CRAC) créé en 2015. Avec un effectif de 100 personnes, il assure trois missions : la **production** de renseignement d'origine cyber (ROC), le **pilotage de la production** du renseignement d'intérêt militaire (RIM) relatif au cyberespace et de **l'orientation** des capteurs cyber de la DRM et de la fonction interarmées du renseignement (FIR).

*****.

Compte tenu de son orientation vers le renseignement d'intérêt militaire, les actions réalisées par la DRM sur les théâtres d'opération (par exemple l'analyse de supports informatiques saisis à l'ennemi), ne relèvent pas d'une autorisation de technique de renseignement.

*d) La DRSD*

Le cyberespace constitue pour la **DRSD** un milieu stratégique dans lequel elle entend renforcer ses capacités de contre-ingérence. Elle est amenée à collecter du renseignement d'origine cyber *via* les moyens autorisés par la loi renseignement de 2015 et dans sa sphère de compétences.

L'exploitation de l'information constitue aujourd'hui un défi majeur. L'émergence de la donnée, associée à l'explosion des flux et à l'hétérogénéité des supports, pose la question de son contrôle (intégrité, confidentialité, disponibilité) mais plus encore de son traitement et de sa mise en perspective. La DRSD conduit le développement d'un nouveau système de recueil et d'exploitation du renseignement (SIRCID) qui constituera la première solution nationale en matière de SI d'un service de renseignement

[1] *Au vu de la porosité de ces sujets, cette cellule traite également des dossiers en lien avec la pédopornographie, une importante partie de ces dossiers passant par le darknet et, de plus en plus, les crypto-actifs.*

et contribuera à renforcer de façon significative sa capacité en matière d'exploitation de l'information de masse.

## V. LA MONTÉE EN PUISSANCE DES SERVICES DE RENSEIGNEMENT DANS LE DOMAINE CYBER

Cet investissement dans la surveillance du cyberespace exige des moyens nouveaux pour les services : une adaptation de leur organisation, des personnels spécialisés dans les technologies de la sécurité informatique, dans le développement de nouveaux outils et de l'exploitation de ceux-ci, et enfin des moyens financiers pour concevoir, développer, acquérir et exploiter les nouveaux outils. Cet effort suppose, en outre, le développement parallèle d'une filière industrielle souveraine. Il est nécessaire si la France veut pouvoir maintenir son rang et ses capacités car l'ensemble des services de renseignement se dotent de capacités dans ce domaine.

### *A. LA MONTÉE EN PUISSANCE DES SERVICES FRANÇAIS DE RENSEIGNEMENT*

Des informations recueillies auprès des services on constatera notamment :

- un effort continu de recrutement et d'investissement des services consacré au domaine cyber ;

- la recherche d'une mutualisation des investissements et des capacités avec des entités appartenant au même ministère (armées/DGSE, armées et CRAC-DRM, douanes, police/DGSI) avec des modalités d'usage différentes (séparation étanche des missions pour le ministère des armées et la DGSE, forte intégration du CRAC au sein de l'état-major du COMCYBER, compétence nationale de la DGSI pour opérer les captations de données dans le cadre judiciaire, délégation à une entité spécifique « Cyberdouane » pour la DNRED ;

- la commune difficulté des services à recruter et fidéliser des ingénieurs et techniciens informatiques de haut niveau spécialistes de la sécurité et de la gestion des données. Des initiatives ont été prises, par exemple au sein des armées pour mutualiser la formation des cadres intervenants dans ce domaine[1].

[1] *Ainsi le COMCYBER préside la commission d'adaptation de la formation (CAF) « SIC/cyber » et co-préside un groupe de travail « Opérer dans le cyberespace » avec la DRH-MD. Il participe également à la gouvernance de la famille professionnelle « Renseignement » à travers la CAF « Renseignement » qui a vocation à faire évoluer la description des métiers et des compétences cyber nécessaires dans cette famille.*

### 1. La DGSE

Dans le domaine de la lutte informatique défensive, la DGSE poursuit le développement de sa capacité à détecter, caractériser et surtout aider à attribuer les cyberattaques menées à l'encontre des intérêts français. En particulier, maintenir une connaissance actualisée sur l'état de la menace et accroître la visibilité sur les opérations numériques offensives des pays tiers supposera de multiplier les accès techniques, humains ou opérationnels à du renseignement capté auprès des attaquants.

*a) Un effort de recrutement et de formation*

En 2019, la DGSE a consacré environ ***** ETP à sa mission de cyberdéfense. En fin de loi de programmation militaire, cet effectif devrait atteindre *****. Ces agents sont majoritairement affectés à des missions *****.

Au titre de la LPM 2019-2025, la DGSE bénéficiera de 772 créations dont 502 sur la période 2019-2023 (310 de 2019 à 2022) au sein desquels 290 devraient être affectés à la fonction « cyberdéfense » et ces effectifs seront renforcés par 173 militaires de l'EMA[1].

*****

*b) Des investissements importants*

L'intensification et la consolidation capacitaire des grands programmes interministériels et de la cyberdéfense, avec notamment l'acquisition et le développement de matériels permettant de tenir compte des évolutions technologiques et de l'augmentation du volume et de la qualité des données à traiter ainsi que du développement et de l'industrialisation des processus techniques constituent le socle nécessaire au maintien de l'efficacité de la DGSE. Dans un monde où la collecte des données, notamment en source ouverte est massive, la performance d'un service de renseignement se mesurera davantage par ses capacités à exploiter intelligemment et rapidement l'information utile.

*****. Quand cela est possible les investissements capacitaires sont mutualisés au sein du ministère des armées dans une double logique d'économie des moyens et de respect des attributions et responsabilités du CEMA et du DGSE. La DGSE a reçu à ce titre un financement spécifique de l'EMA de ***** en 2019. D'autres investissements sont financés pour partie au titre de capacités techniques interministérielles mutualisées (CTIM) par

[1] *Les agents affectés à la DGSE et travaillant dans le domaine cyber sont rémunérés sur l'article 50-01 du programme 212 pour 65 % d'entre eux environ et sur leur BOP d'origine pour les 35 % restant (renforts EMA/Cyber).*

transfert au budget de la DGSE de crédits du programme 129 « coordination de l'action du Gouvernement [1]».

La DGSE a consacré ***** à sa mission de cyberdéfense de 2015 à 2019. Elle poursuit sa montée en puissance et y consacrera près de ***** sur la période 2020-2024 (***** par rapport à la période précédente). Ces montants n'intègrent pas les crédits transférés au titre des programmes interministériels, ni les montants financés aux moyens des fonds spéciaux contrôlés par la CVFS.

**2. La DGSI**

*a)* *****

*****

*b)* *****

*****

*c)* *****

*****

**3. La DNRED**

*****

**4. Tracfin**

Au niveau humain, il convient de distinguer les moyens mis au service de la sécurité informatique du service de ceux liés aux aspects cyber des missions du service, et dont lutte contre la cybercriminalité.

S'agissant de la sécurité informatique du service, en septembre 2019, une cellule dédiée a été créée. Deux ingénieurs sécurité des systèmes d'information ont été recrutés en 2019 et au printemps 2020 pour renforcer l'officier de sécurité-chef de la cellule de sécurité des systèmes d'information.

Une cellule dédiée à la lutte contre la cybercriminalité, créée en septembre 2018, comporte depuis janvier 2020 4 enquêteurs (agents titulaires de catégorie A). Un développement de cette cellule est envisagé au regard du nombre de dossiers à traiter et de l'évolution des typologies de fraudes rencontrées.

[1] *Le montant des transferts s'est élevé à 73 M € en 2019 pour couvrir l'intensification et la consolidation des grands programmes interministériels et de la cyberdéfense.*

**La démarche capacitaire de Tracfin**

*****

Une mutualisation des achats entre services des ministères économiques et financiers, voire entre services de renseignement, peut faire diminuer le coût des licences. C'est le cas pour les outils qui sont référencés par l'UGAP, centrale d'achat qui négocie les tarifs avec les éditeurs sur la base d'un volume de commandes mutualisé entre les différents acheteurs publics. Pour les outils qui ne sont pas référencés à l'UGAP, l'économie réalisée serait à mettre au regard des coûts de coordination que cette mutualisation occasionnerait, les services ayant en général des processus et supports contractuels d'achat différents.

### 5. La DRM

Depuis 2015, la DRM dispose du centre de recherche et d'analyse du cyberespace (CRAC) qui concentre ses capacités de recueil de renseignement d'origine cyber et d'analyse des menaces (*cf. supra*). Ce centre emploie un effectif de 100 personnes. La dualité de ses missions impose de disposer de profils variés d'analystes-rédacteurs. Si ces derniers sont une ressource relativement facile à capter, d'autres métiers sont soumis à une concurrence plus marquée. Ainsi les spécialistes de l'investigation sur supports numériques, qui requiert à la fois des connaissances en télécommunications, en électronique et en base de données, s'avèrent plus difficile à recruter et fidéliser (cursus de formation long, peu compatible avec le jeu des mutations militaires). De même, les spécialistes « télécoms » et « systèmes d'information et de communication », constituent une population sous tension.

Outre les compétences, la gestion de l'équilibre entre personnels militaires et civils représente un enjeu pour le domaine afin, notamment, de répondre aux besoins des théâtres d'opérations (exemple du laboratoire de renseignement multicapteurs en charge, entre autre, de l'extraction des données téléphoniques saisies). Le CRAC aujourd'hui est composé de près de 46 % de personnels civils (contractuels ou fonctionnaires, très majoritairement de catégorie A). A moyen terme, la DRM entend stabiliser le ratio civils/militaires aux environs de 30/70.

Sur la période de LPM (2019-2025), la DRM sera renforcée d'un total de 238 ETP. Il est actuellement prévu d'attribuer 2 de ces ETP au CRAC. Des études sont néanmoins en cours en interne DRM afin d'évaluer la possibilité de réévaluer à la hausse cette cible afin de mieux répondre aux besoins du domaine.

En matière de développement capacitaire, le CRAC s'inscrit dans la cohérence d'ensemble de la DRM. Le recours à des outils développés par des entreprises est courant et permet de constituer un socle de solutions pour conduire, par exemple, la veille sur les réseaux, l'investigation dans le *dark*

*web*, l'extraction et l'exploitation des données numériques issues de différents supports (GSM, disques durs, puces mémoires…) ou des tâches de traitement de données (requêtage, croisement, analyse prédictive).

Les investissements, limités, sont essentiellement portés par le programme 178 de la mission Défense et s'inscrivent dans la gouvernance générale du ministère afin de garantir un niveau optimal de coordination avec les autres acteurs impliqués (DGA, DIRISI, DGSE, DRSD…). Les investissements consentis au profit du CRAC représentent chaque année plus de 4 millions €.

Les échanges réguliers entretenus avec le reste de la communauté du renseignement garantissent la bonne coordination/mutualisation des efforts et investissements. En matière de recueil en sources ouvertes ou sur les réseaux sociaux (OSINT), le besoin peut être mutualisé. Actuellement une preuve de concept (POC – outil ROSINT) portée par la DGA et Cap Gemini est à l'étude afin de fournir un espace de stockage cloud dédié à ces données. La DRM pourrait en faire bénéficier d'autres entités (unités des armées ou service).

A noter enfin que les données collectées par le CRAC, notamment par le biais de l'exploitation des supports saisis sur les théâtres d'opération, sont partagées avec la communauté au moyen des programmes mutualisés. Ces données (contacts, localisation, etc) contribuent directement aux résultats opérationnels des armées.

### 6. La DRSD

La montée en puissance des effectifs de la DRSD dans le domaine cyber s'inscrit dans le cadre de la remontée en puissance du service prévu par la LPM 2019-2025.

La plus grande part du personnel relevant du domaine cyber appartient à la sous-direction technique au sein de laquelle l'officier de cohérence cyber du service coordonne la manœuvre cyber de l'ensemble de la DRSD. Cette sous-direction inclut en particulier un centre opérationnel de surveillance et sécurité (COSS) dont les missions principales sont d'assurer la sécurité cybernétique interne et de contribuer aux actions du ministère des armées dans ce domaine. La composante cyber est également représentée au sein de la sous-direction de la contre ingérence.

Les principales activités du service en matière de cyber, hors activités à vocation de surveillance interne et de certaines TR, relèvent principalement des inspections en milieux industriel et étatique (50 à 60 par an) d'une part et des investigations numériques (70 à 80 par an) de l'autre.

En 2019, 192 postes décrits relevaient du domaine cyber. A l'horizon 2025, l'effectif lié au domaine cyber doit atteindre 249 postes.

D'ici à 2025, le service entend consacrer 192 emplois temps plein (ETP) au domaine cyber. 85 % de ces postes sont d'ores et déjà armés. Ils se répartissent comme suit :

- 70 personnels (objectif : 80) agissent au profit de la cybersécurité de la sphère de défense (43 %) et mettent en œuvre des compétences spécialisées ;

- 84 personnels (objectif : 97) sont dans l'environnement cyber et participent à l'élaboration du renseignement d'origine cyber (ROC). Il s'agit essentiellement de postes d'analystes, d'administrateurs et d'experts « renseignement » ;

- enfin, en sa qualité d'AQSSI (autorité qualifiée en SSI), la DRSD emploie 9 personnels (objectif : 15) pour assurer la sécurité de ses propres systèmes d'information.

Dans un contexte d'accélération de l'innovation technologique, le cadencement des recrutements vise à répondre à l'augmentation progressive du besoin. Les compétences et les profils recherchés prévalent sur la répartition statutaire et concernent l'ensemble des différents métiers de la cyberdéfense et en particulier des datascientists, des datamanagers, des développeurs et des experts des techniques cyber ou de l'investigation numérique. Au-delà du nombre, elle déploie également des efforts significatifs dans la formation avec la mise en place à compter de la fin 2020 de nouveaux parcours de carrière et de formations ayant vocation à dynamiser les carrières et renforcer le professionnalisme de ses agents. Le service ne fait qu'administrer le personnel qu'il emploie. Il n'est donc pas en mesure de chiffrer précisément le coût (T2) de ce personnel essentiellement supporté par les gestionnaires pourvoyeurs de ressources.

La DRSD a investi 500 000 € en 2019 dans des projets cyber. Les besoins pour les années 2020 et 2021 sont établis à ce jour respectivement dans le cadre de la planification pluriannuelle à hauteur de 700 000 € et 1,5 millions €.

Elle développe de façon autonome certains outils mais s'appuie principalement sur la mutualisation interservices. La cohérence avec les différents projets en cours est systématiquement recherchée dans le domaine cyber comme dans les autres et en particulier celui du nouveau système d'information du service (SIRCID, premier outil d'analyse et de traitement des données hétérogènes). **La montée en puissance des moyens des services consacrés à la cyberdéfense doit être poursuivie compte tenu de l'évolution des menaces et des opportunités qu'offre le cyberespace pour le recueil de renseignement.**

**Recommandation n° 56 : Maintenir un niveau de financement suffisant pour garantir le niveau des investissements des services dans la cyberdéfense et leur permettre de recruter et de fidéliser des personnels de haut niveau.**

**Compte tenu des moyens financiers engagés en investissement comme en fonctionnement et en ressources humaines, il serait souhaitable de mettre en place au niveau du CNRLT un dispositif d'évaluation de la performance de la politique menée avec ses moyens croissants. Un outil permettant d'homogénéiser les informations sur les moyens consacrés par les services de renseignement à la cyberdéfense devra être intégré dans ce dispositif (*cf.* recommandation n° 59).**

*B.* *****

**1.** *****

*****

**Recommandation n° 57 : Poursuivre la mutualisation dans le développement des outils, la formation et les échanges de bonnes pratiques entre les services de renseignement.**

### 2. La nécessaire émergence d'une filière industrielle souveraine

La sécurité dans l'espace cyber contre tout adversaire repose sur la pleine autonomie dans la mise en œuvre des outils de cyberdéfense et donc la maîtrise de capacités critiques souveraines. Plus encore lorsqu'il s'agit de protéger les services de l'État et les activités d'importance vitale ou de soutenir l'action des armées ou des services de renseignement.

Dans nombre de technologies-clés, l'excellence scientifique française est reconnue grâce au niveau de formation de ses mathématiciens et ingénieurs et à la qualité de ses organismes de recherche. Mais la constitution d'une industrie française de logiciels de cybersécurité, capable de rivaliser avec les entreprises américaines ou israéliennes tarde à venir. Ce qui pose un problème pour l'autonomie de notre cyberdéfense et renchérit probablement les coûts.

Cette situation est mise en évidence dans le rapport commun des inspections sur les missions et effectifs de l'État contribuant à la cybersécurité de février 2019. Ce rapport note que la Revue stratégique de cyberdéfense préconise que la France se dote d'une véritable stratégie industrielle. Si la filière française a connu une croissance de 12 % de 2013 à 2016, elle présente trois faiblesses : sa dépendance aux composants électroniques fournis par une industrie du numérique de moins en moins européenne, un tissu de PME trop peu structuré, une filière qui peine à s'organiser au niveau national. Dès lors, même dans l'administration, les produits étrangers liés à la souveraineté numérique représentent une place importante des achats.

Aussi l'acquisition par la DGSI du service proposé par Palantir en 2016 a-t'elle suscite deux initiatives françaises :

- un groupe de 22 sociétés françaises (dont Atos, Airbus Defence & Space et Thalès) réunies au sein d'un cluster Data intelligence initié par le GICAT[1], en 2016, propose depuis la fin de l'année 2018 une alternative technologique et commerciale à Palantir, visant les acteurs institutionnels de la défense et de la sécurité et dans un second temps les marchés civils. La DRSD a signé un marché pour son système d'information SIRCID avec Airbus Defence & Space ;

- en novembre 2017 la DGA a notifié l'initiative Artemis à la société Atos-Bull, à la société Capgemini et au groupement Thalès-Sopra-Stéria. Cette initiative vise à la mise en place d'un écosystème permettant aux innovateurs d'apporter leurs créations et de les faire mûrir jusqu'à des solutions utilisables par les forces grâce à une gamme de produits complète. A terme, Artemis a vocation à faire émerger des applications utilisant l'intelligence artificielle pour le traitement massif des données qui permettent aux combattants de se concentrer sur les informations importantes afin de prendre des décisions rapides et efficaces.

On peut y ajouter l'initiative soutenue par la DRM d' « Intelligence Campus » et celle du « Campus de la Cybersécurité » lancée par l'ANSSI afin de réunir et renforcer l'ensemble des acteurs de l'écosystème français[2].

Le rapport des inspections générales, préconise qu'une stratégie industrielle de souveraineté en cybersécurité en lien étroit avec les enjeux numériques soit élaborée sous la conduite du SGDSN pour établir un état des lieux des dispositifs multiples de soutien à la politique de recherche et à la politique industrielle, fixer les priorités au niveau du CODIR Cyber et assurer le pilotage au niveau du COPIL Cyber. Cet objectif est louable mais la proposition manque d'ambition. Pour réussir cette stratégie doit être impulsée et coordonnée au plus haut niveau politique de l'État[3]. Le développement de cette politique ambitieuse de cybersécurité passe aussi par une politique de gestion des compétences, des formations et de carrières au sein des administrations de l'État.

La mise en œuvre de cette stratégie devrait pouvoir orienter l'action des services de renseignement pour protéger et promouvoir les intérêts fondamentaux de la Nation dans le domaine économique.

---

[1] *Groupement des industries de défense et de sécurité terrestres et aéroterrestres*

[2] *Mission confiée par le premier ministre à Michel Van Den Berghe, directeur général d'Orange Cyberdéfense*

[3] *Comme le propose, à l'instar de la coordination du renseignement et de la lutte contre le terrorisme les trois anciens hauts responsables de la défense et des affaires étrangères dans la tribune données au Monde le 28 janvier 2020 précité.*

**Recommandation n° 58 : Associer les services de renseignement au travail prospectif d'élaboration d'une nouvelle stratégie industrielle de souveraineté en cybersécurité et orienter leur action dans sa mise en œuvre.**

### *C. CETTE MONTÉE EN PUISSANCE EST INDISPENSABLE POUR CONSERVER UN NIVEAU D'EFFICACITÉ COMPARABLE AUX AUTRES SERVICES PARTENAIRES*

Cet effort doit être poursuivi, consolidé et renforcé car l'ensemble des services de renseignement étrangers et des forces armées se dotent de capacités cyber importantes. A titre d'exemple la Grande-Bretagne et l'Allemagne ont entrepris des réformes pour, d'une part poursuivre le rapprochement et l'intégration des capacités cyber et, d'autre part, intégrer la dimension cyber à leurs doctrines de recherche du renseignement. Les États-Unis ont actualisé leur stratégie cyber en 2018 dans un sens plus offensif.

La nature très confidentielle des informations concernant la cybersécurité ne permet pas d'effectuer des comparaisons solides des capacités des différentes puissances en ce domaine. Les informations, autour des incidents de cybersécurité reflètent souvent davantage la posture agressive que la performance de capacités étatiques. Les développements qui suivent, très partiels et sommaires ne sont là que pour illustration des efforts consentis par les États dans ce domaine tant pour se doter de forces cyber plus robustes que pour promouvoir et protéger leurs entreprises.

#### 1. La Grande-Bretagne

Depuis 2003, la Grande-Bretagne a mis en place une stratégie nationale en matière de sécurité de l'information en plaçant la cyberdéfense comme l'une des priorités nationales.

En 2010, le *National Cyber Security Program* (NSCP) avait doté de 860 millions £ pour la période 2011-2016 les activités de sécurité et de renseignement du *Government Communications Headquarters* (GCHQ) qui centralise le renseignement technique et les activités cyber du ministère de la défense (MOD). Cette enveloppe a été portée à 1,9 milliards £ pour la période 2016-2021 (+ 121 %) puis récemment à 2,3 milliards £.

Dans ce cadre, le Royaume-Uni a annoncé en février 2020 mettre en place une « *National Cyber Force* », fruit de la collaboration entre le GCHQ et le ministère de la défense. Il assume avoir une politique offensive dans le cyberespace. Cette force doit à terme être composée de 500 spécialistes et elle renforcera les capacités existantes. Son but est de faire de la Grande-Bretagne une cyber-puissance, capable de cibler les réseaux, les satellites, les communications, les infrastructures informatiques des pays hostiles ou de

groupes terroristes. Ce service s'annonce ultraconfidentiel, ses actions devraient rester classées secret-défense, la nature des cyberarmes et le nom de son directeur ont été gardés secrets, ce qui pose la question du contrôle démocratique sur l'objectif et l'éthique de la cyberattaque, les circonstances dans lesquelles elle pourrait être utilisée et les types d'effets qui pourraient être ou non acceptables.

La stratégie cyber évolue aussi vers une plus grande coopération entre le Gouvernement et les entreprises privées jusqu'alors privilégiées dans la mise en œuvre de cette politique avec le lancement d'une plateforme numérique de partage d'informations en temps réel entre les secteurs privé et public et la mise en place auprès du GCHQ du *National Cyber Security Centre*, interface entre le Gouvernement et l'industrie qui centralise l'ensemble des activités et des informations relatives à la cyberdéfense.

Parmi les membres du G20, la Grande-Bretagne est pionnière dans le secteur digital qui représente 16 % de son produit intérieur, 10 % des emplois et 24 % de ses exportations. Parmi les 50 entreprises de cyberdéfense les plus importantes dans le monde en 2018, 7 sont britanniques comme BAE, PwC ou KPMG. L'industrie de la cyberdéfense est traitée comme un service voué à l'exportation et à l'expansion de l'influence du Royaume-Uni sur la scène internationale.

### 2. Les États-Unis

Les États-Unis ont rendu publics en 2018 plusieurs textes comme le *White House National Cyber Strategy*, l'*Unclassified Summary Department of Defense Cyber Strategy* et le *Department of Homeland Security (DHS) Cyber Secrurity Strategy*, qui dessinent les contours d'une nouvelle stratégie globale plus offensive que les précédentes mise en œuvre par le *United States Cyber Command* devenu officiellement un des commandements interarmées unifiés du *United States Strategic Command* le 4 mai 2018.

Le *White House National Cyber Strategy*, premier texte à vocation globale depuis 2011 constitue une nouvelle doctrine dont les objectifs consistent à assurer le renforcement de la capacité américaine de dissuasion dans le cyberespace ainsi qu'à maintenir son influence et sa prospérité. Le document du department of defense s'appuie sur l'usage d'un nouveau concept doctrinal « *defend forward* » consistant à arrêter la menace avant qu'elle n'atteigne sa cible » en construisant une force plus létale. Avec *l'International Cyber Deterrence Initiative*, les États-Unis déclarent vouloir prendre la tête d'une coalition avec leurs alliés pour coordonner les réponses aux cyberattaques, partager du renseignement et surtout appliquer des sanctions.

Le budget alloué à cet effort a cru de 35 % entre 2016 et 2017 portant l'effort à 19 milliards de dollars pour des programmes visant à attirer et retenir des compétences au sein d'une armée se préparant à tous les types de conflits.

En outre, les États-Unis maintiennent leur cyberdéfense des entreprises privées, en particulier celles de la BITD – classées « infrastructures critiques » afin d'améliorer la confidentialité de leurs informations, garantes de leur supériorité militaire. Ceci s'inscrit dans une logique globale de promotion des entreprises américaines et de défense de leurs parts de marchés mondiales, dans un contexte de très forte concurrence et d'espionnage économique.

*

*  *

Au terme de cette étude, il convient de mettre en exergue :

- l'importance des enjeux menacés, l'évolution rapide et inquiétante de la menace, mais aussi les opportunités qu'offre le cyberespace aux services de renseignement ;

- l'effort consenti par les gouvernements successifs depuis 2008 pour doter notre pays d'une politique publique de cyberdéfense comprenant la prévention et la protection, la lutte informatique défensive et, dans des conditions encadrées, une stratégie de lutte informatique offensive. Cette politique repose sur une délimitation précise de la compétence des différents acteurs auxquels l'exécution est confiée : l'ANSSI et le COMCYBER, mais aussi les services de renseignement, notamment la DGSE et la DGSI ;

- toutefois, cette contribution n'est pas évaluée de façon globale.

En conséquence, la DPR demande la mise en place sous l'autorité du CNRLT d'un outil d'évaluation et de suivi de la contribution des services de renseignement à la politique publique de cyberdéfense. Cet outil permettra de mesurer les moyens qu'ils y consacrent et les résultats qu'ils obtiennent dans chacune des missions qui leurs sont attribuées. Tout au long de cette étude, la DPR a relevé les points d'intérêts qui pourraient figurer dans ce dispositif (information à recueillir, tableaux de bord à réaliser…) L'inspection des services de renseignement pourrait participer à la conception de cet outil. Une fois, ce travail méthodologique réalisé, la DPR souhaite que les résultats de cette évaluation et de ce suivi lui soient communiqués dans le rapport annuel d'activité des services.

**Recommandation n° 59 : Mettre en place, sous l'autorité du CNRLT, un outil d'évaluation et de suivi de la contribution des services de renseignement à la politique publique de cyberdéfense. L'inspection des services de renseignement pourrait participer à la conception de cet outil. Une fois ce travail méthodologique réalisé, la DPR souhaite que les résultats de cette évaluation et de ce suivi lui soient communiqués dans le rapport annuel d'activité des services.**

# CHAPITRE VI :
# RAPPORT GÉNÉRAL DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX SUR L'EXERCICE 2018

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* ».

Depuis janvier 2019, sa composition est la suivante :

- M. Michel Boutant, sénateur (SOC) de la Charente, président ;

- M. François-Noël Buffet, sénateur (LR) du Rhône ;

- M. Loïc Kervran, député (LREM) du Cher ;

- M. Patrice Verchère, député (LR) du Rhône.

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

Elle s'est ainsi rendue :

- à la DGSE, les 23 mai, 11 septembre, 14 et 21 octobre, 29 novembre et 5 décembre 2019 ;

- à la DGSI, les 27 juin et 13 novembre 2019 ;

- à la DRM, les 4 juin, 5 septembre et 18 octobre 2019 ;

- à la DRSD, le 2 juillet 2019 ;

- à la DNRED, le 18 juillet 2019 ;

- à Tracfin, le 17 juillet 2019 ;

- au groupement interministériel de contrôle (GIC), les 18 juin et 4 octobre 2019.

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

Elle a également effectué un déplacement à l'étranger, du 16 au 24 septembre 2019, pour visiter des postes de *****.

Par ailleurs, la CVFS a auditionné le 4 décembre 2019, un membre de la mission de l'inspection des services de renseignement (ISR) chargée par le Premier ministre d'un rapport sur la gestion des fonds spéciaux en date du 11 janvier 2019 communiqué par le Premier ministre à la CVFS le 19 juin 2019. Enfin, le président de la CVFS a été reçu le 17 décembre par le conseiller affaires intérieures du Premier ministre pour un échange sur la mise en œuvre des recommandations du rapport de l'ISR.

* * *

## I. PRÉSENTATION GÉNÉRALE DES FONDS SPÉCIAUX EN 2018

### *A.* *****

Les services spécialisés de renseignement et le GIC ont disposé en 2018 d'un montant plus important de ressources en fonds spéciaux, en comparaison avec l'exercice précédent. Le total s'élève à *****, soit une hausse de plus de 8,7 % par rapport à 2017 (*****). Ce montant se rapproche du pic enregistré en 2015 (*****) du fait du lancement cette année-là d'investissements pluriannuels très consommateurs de fonds spéciaux.

La trajectoire des fonds spéciaux progresse, en 2018, un peu plus vite que celle de l'enveloppe totale des crédits en fonds normaux consacrés au renseignement, qui s'est établie à 2 516 M€ en 2018 (+ 4,3 %).

**RESSOURCES EN FONDS SPÉCIAUX – ÉVOLUTION 2017/2018 (EN M€)**

*Tableau* *****

*****

En additionnant la dotation initiale, les abondements en cours d'exercice et les autres produits, on observe qu'en 2018, trois des six services spécialisés de renseignement disposent désormais de ressources significatives en fonds spéciaux, supérieures au million d'euros.

### *B.* *****

En 2018, le montant des fonds spéciaux dépensés dans l'année a continué de progresser à un rythme très soutenu *****.

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

*Tableau* *****

La hausse des dotations en fonds spéciaux enregistrée en 2018 ne suffit pas à couvrir la hausse des dépenses puisque l'on constate un écart défavorable de *****.

*****

**VENTILATION PAR POSTES DE DÉPENSES (EN M€)**

*Tableau* *****

*****

Compte tenu, d'une part, de la relative stabilité des ressources alloués aux services et entités bénéficiaires, et d'autre part, de l'augmentation de leurs dépenses, le niveau global de la trésorerie a diminué en 2018. *****

*****

*****. Elle recommande en conséquence un resoclage de la dotation en fonds spéciaux inscrite au programme 129 pour tenir compte des besoins réels et de l'évolution de l'activité opérationnelle des services (**recommandation générale n° 1**).

**Recommandation générale n° 1 : Effectuer un resoclage de la dotation en fonds spéciaux inscrite au programme 129 pour tenir compte des besoins réels et de l'évolution de l'activité opérationnelle des services.**

*****

Elle observe néanmoins avec satisfaction l'augmentation sensible (+10 M€) de la dotation inscrite au programme 129 dans le PLF pour 2020. La rationalisation des procédures de dialogue budgétaire et de suivi de l'exécution des dépenses en fonds spéciaux, entre les services et le Premier ministre, animées par la CNRLT (*cf. infra*) devrait permettre de mieux faire ressortir les besoins et d'ajuster le niveau global de la dotation comme sa répartition *****.

## II. OBSERVATIONS COMMUNES À L'ENSEMBLE DES SERVICES

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

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

***A.*** *****

Dans ses précédents rapports, la CVFS a toujours souligné la nécessité de ne recourir aux fonds spéciaux que dans les cas où l'utilisation de fonds normaux se révélait inappropriée. *****. La CVFS se félicite de la mise en œuvre progressive de sa recommandation par les services concernés (*cf. supra*).

*****. Dans son dernier rapport, la CVFS s'était interrogée sur la pertinence du périmètre d'éligibilité aux fonds spéciaux.

*****

*****, dans la présentation annuelle du programme 129 « coordination du travail gouvernemental », il est précisé que les fonds spéciaux sont consacrés au financement de « diverses actions liées à la sécurité extérieure ou intérieure de l'Etat ».

*****

Dans ce rapport, la CVFS avait rappelé les principes qu'il importe de respecter scrupuleusement, indépendamment de l'interprétation que l'on puisse avoir sur le périmètre des fonds spéciaux :

*- que les fonds soient attribués pour un usage conforme à la doctrine d'emploi gouvernant les fonds spéciaux progressivement élaborés par la CVFS et donc ne constituent pas un moyen d'échapper aux règles gouvernant les crédits généraux.*

*****

*- que le service attributaire soit clairement identifié, qu'il tienne le compte d'emploi des fonds attribués et se dotent une réglementation de gestion et d'un mode de contrôle interne.*

*****

*- qu'il n'existe pas de subdélégation de fonds spéciaux et que le service utilisateur soit le service attributaire.*

***** (**recommandations générales n° 2 et 3).**

| |
|---|
| **Recommandation générale n° 2 :** ***** |
| **Recommandation générale n° 3 :** ***** |

*****

*- que la CVFS effectue sur ce service un contrôle de même nature que celui réalisé sur les autres services et selon les modalités définies à l'article 154 de la loi de finances pour 2002.*

*****

*- que le Parlement soit informé des modifications de périmètre des fonds spéciaux et que le vote des lois de finances soit éclairé en conséquence.*

La CVFS comprend que pour préserver la confidentialité sur les services et entités bénéficiaires, cette information puisse être restreinte.

Elle-même en a été informée lors de la communication par le CNRLT de la répartition annuelle des fonds spéciaux.

Il serait néanmoins souhaitable de **donner une base juridique plus solide à cette répartition annuelle en désignant par un arrêté ou une circulaire, non publié au *Journal officiel*, les entités et services susceptibles de bénéficier de fonds spéciaux.** Cet arrêté ou circulaire, et les modifications apportées ultérieurement, seraient communiqués sans délai à la CVFS. Cette recommandation est d'autant plus nécessaire que le périmètre est désormais étendu au-delà du premier cercle de la communauté du renseignement (**recommandation générale n° 4**). *Cette recommandation remplace la recommandation n° 17.01 qui est clôturée.*

**Recommandation générale n° 4 : Désigner par arrêté ou circulaire, non publié au *Journal officiel*, les entités et services susceptibles de bénéficier de fonds spéciaux. Cet arrêté ou circulaire, et les modifications apportées ultérieurement, seraient communiqués sans délai à la CVFS.**

### *B. UNE RATIONALISATION DES PROCÉDURES*

Par une *recommandation générale n° 16.14* à destination du CNRLT, la CVFS avait suggéré de confier à l'ISR une mission relative à l'effectivité du dispositif de contrôle interne applicable aux règles de gestion des fonds spéciaux et, plus généralement, développer des interventions de l'ISR sur les fonds spéciaux.

**L'ISR s'est vue confier, au printemps 2018, l'élaboration d'un rapport sur la gestion de ces fonds.** Les rapporteurs de l'inspection ont rencontré à deux reprises le président de la CVFS et leur rapport a été communiqué au Premier ministre le 11 janvier 2019. La CVFS en a reçu communication du Premier ministre le 19 juin. Elle a reçu le chef de cette mission le 4 décembre de la même année.

**Ce rapport a surtout consisté, conformément à la lettre de mission du directeur de cabinet du Premier ministre en date du 7 juin 2018, à identifier le calendrier budgétaire de gestion des fonds, mais aussi à faire des recommandations permettant de structurer cette procédure et de définir les compétences des différents acteurs** qui concourent à l'expression

des besoins, à son évaluation et aux différents arbitrages permettant de déterminer l'enveloppe globale annuelle inscrites au programme 129, puis sa répartition. Il a émis également des recommandations permettant d'assurer un meilleur suivi d'exécution des dépenses.

**Cette procédure a été formalisée par la circulaire du Premier ministre du 8 novembre 2019 (non publiée)** qui impose **une nomenclature commune** aux différents services et entités bénéficiaires **et les invite à plus de transparence s'agissant de leur trésorerie et de leurs ressources externes**. **Une mission d'animation et de pilotage de cette procédure préalable à l'arbitrage final du Premier ministre est confiée au CNRLT.**

**La CFVS se réjouit des améliorations sensibles apportées par cette circulaire qui faciliteront son contrôle.** *****

*****

La plupart de ces recommandations ont été retenues par le cabinet du Premier ministre et commencent à être exécutées par les services *****.

*****

La CVFS adhère à l'ensemble des recommandations retenues dont elle a pu constater, à l'occasion de ses échanges avec les services et la CNRLT, que nombre d'entre elles connaissaient un début de mise en œuvre en 2019.

**Cette mise en œuvre permet de considérer qu'un certain nombre de recommandations de la CVFS issues de ses rapports sur les exercices 2016 et 2017 sont satisfaites** :

- inviter les services à définir plus précisément leur trésorerie immobilisée et gagée afin de fixer le montant de leur dotation en fonds spéciaux à un niveau correspondant à leur besoin réel (*recommandation générale n° 16.01*) ;

- mieux définir les besoins des services en fonds spéciaux afin d'éviter des réintégrations trop importantes de crédits non consommés d'un exercice sur l'autre (*recommandation générale n° 16.04*) ;

- constituer un groupe de travail sur les modalités de conservation et d'archivage des comptabilités en fonds spéciaux, incluant le sujet de la dématérialisation, afin d'homogénéiser des pratiques actuellement très différentes d'un service à l'autre (*recommandation générale n° 16.11*) ;

- ***** *(recommandation générale n° 17.06) ;*

- définir un cadre commun sur la définition et la mise en œuvre de règles minimales de démarquage communes à l'ensemble des services (*recommandation générale n° 16.06*) ;

- renforcer les fonctions du CNRLT en matière de pilotage global des fonds spéciaux : identification des besoins, coordination, évaluation et suivi des recommandations de la CVFS (*recommandation générale n° 17.07) ;*

- assouplir l'exigence de production de pièces justificatives pour les menues dépenses dont le montant est laissé à l'appréciation des services (*recommandation générale n° 16.10*).

**D'autres peuvent être considérées comme en cours de mise en œuvre et feront en 2020 l'objet d'une attention renouvelée :**

- ***** (*recommandation générale n° 16.05*) ;

- constituer un groupe de travail sur les possibilités de démarquage existantes dans le logiciel Chorus (*recommandation générale n° 16.07*) ;

- renforcer et formaliser les environnements de contrôle interne – en particulier dans les services bénéficiant d'une augmentation significative de leur dotation en fonds spéciaux – et établir à l'attention de la CVFS une synthèse documentée sur les contrôles mis en œuvre et leurs résultats (*recommandation générale n° 16.13*) ;

- 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. (recommandation générale n° 17.03) ;*

- encourager la mise en place d'un travail interservices pour définir un cadre de mutualisation en matière d'acquisitions techniques et expertiser les outils de mutualisation les plus appropriés : ***** (*recommandation générale n° 17.04) ;*

- ***** *(recommandation générale n° 17.05).*

S'agissant plus particulièrement du contrôle interne, la CVFS observe une prise de conscience générale et des efforts pour se doter de moyens d'audit interne plus conséquents, même si beaucoup n'ont pas atteint, à ce stade, un degré de maturité suffisant. *****

La CVFS demande que des efforts significatifs soient réalisés dans ce domaine de façon à sécuriser l'emploi des fonds spéciaux mais aussi d'évaluer plus précisément l'efficacité de la dépense, et plus particulièrement de certaines acquisitions de matériels ou de prestations coûteux au regard du besoin opérationnel exprimé (*recommandations générales n° 16.13 et n° 17.03 restant ouvertes*). Elle s'attachera au cours de ses prochains contrôles à suivre la mise en place et l'exécution de ces procédures. En conséquence, elle souhaite que soit réaffirmé son pouvoir d'accéder aux rapports d'inspection et d'audit interne nécessaires à sa pleine information et à l'exercice de son contrôle (**recommandation générale n° 5**).

**Recommandation générale n° 5 : 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.**

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

Les données transmises à la CVFS d'un exercice sur l'autre ne sont pas toujours présentées sous un format comparable. Il serait souhaitable d'établir une grille d'indicateurs similaires d'un exercice sur l'autre et de faire converger les indicateurs élaborés par les différents services.

Par ailleurs, dans le cadre des auditions menées sur l'exercice budgétaire 2017, la CVFS avait eu connaissance d'événements significatifs ayant impacté les fonds spéciaux sur des exercices antérieurs, qui ne lui avaient pas été transmis au moment de son contrôle. *****. Aussi, avait-elle rappelé l'obligation qui incombe aux services de lui communiquer spontanément toute anomalie constatée dans la gestion des fonds spéciaux *(recommandation générale n° 17.02)*. Cette recommandation a été mise en œuvre *****.

La CVFS rappelle régulièrement cette règle de transparence lors des contrôles qu'elle effectue. *La recommandation générale n° 17.02 peut dès lors être clôturée.*

### *D. LA MUTUALISATION DES ACQUISITIONS TECHNIQUES* *****

Dans son précédent rapport, la CVFS avait observé des achats de plus en plus importants en fonds spéciaux destinés à l'acquisition d'équipements, *****.

*****

La commission émet donc deux recommandations :

- mettre en place, au sein de chaque service, des indicateurs ***** (**recommandation générale n° 6**) ;

- mettre en place une cellule interservices ***** (**recommandation générale n° 7**). *****

*****

**Recommandation générale n° 6 : Mettre en place, au sein de chaque service, des indicateurs *****.**

**Recommandation générale n° 7 : Mettre en place une cellule interservices *****.**

*E.* *****

*****

*F. LA GESTION DES CAISSES*

A l'occasion de ses contrôles effectués *****, la CVFS a constaté des méthodes disparates s'agissant de la gestion des caisses et sous-caisses, sans pour autant avoir observé de quelconques irrégularités.

Aussi avait-elle invité les services à définir une doctrine claire et précise pour la gestion des caisses et sous-caisses ainsi que pour la réalisation des contrôles et des arrêtés d'encaisse, et à adapter ses formulaires d'arrêté d'encaisse en conséquence.

*****

*G. LA PERSISTANCE D'ANOMALIES PONCTUELLES*

Dans le cadre de ses contrôles sur place et sur pièces réalisés en 2018, la CVFS a examiné de nombreuses pièces comptables. Si les fonds spéciaux font globalement l'objet d'une gestion très rigoureuse, la commission continue néanmoins de relever un certain nombre d'anomalies ponctuelles.

**1.** *****

*****

**2.** *****

*****

**3.** *****

*****

**4.** *****

*****

**5. Quelques failles observées dans les processus d'anonymisation**

Le secret est au cœur de la raison d'être des fonds spéciaux, et justifie la mise en œuvre de procédures d'anonymisation rigoureuses. La

plupart du temps, l'absence d'anonymisation fait *de facto* tomber la justification du recours aux fonds spéciaux.

Dans ses rapports sur les exercices 2016 et 2017, la CVFS avait déjà révélé un certain nombre d'anomalies qui soulignaient aussi la situation inégale des services en termes de capacités d'anonymisation.

Si des progrès ont été accomplis, des dysfonctionnements, certes moins nombreux, persistent. La CVFS a en effet mis une nouvelle fois en évidence le défaut d'anonymisation de certaines pièces justificatives établies au nom de l'agent ou du service.

***** (*recommandation générale n° 17.06 clôturée*).

## III. SUIVI DES RECOMMANDATIONS DE LA CVFS SUR LES EXERCICES 2016 ET 2017

Au début de l'exercice 2018, 18 recommandations générales émises en 2016 (11) et 2017 (7) restaient à mettre en œuvre ou ne l'avaient été que partiellement.

Au terme du contrôle réalisée par la CVFS, 9 recommandations générales peuvent être clôturées : **7 ont été mises en œuvre, une est considérée comme satisfaite même si le résultat de la réflexion engagée ne va pas dans le sens recommandé) et une a été remplacée par une recommandation nouvelle plus précise :**

- inviter les services à définir plus précisément leur trésorerie immobilisée et gagée afin de fixer le montant de leur dotation en fonds spéciaux à un niveau correspondant à leur besoin réel (*recommandation générale n° 16.01*) ;

- mieux définir les besoins des services en fonds spéciaux afin d'éviter des réintégrations trop importantes de crédits non consommés d'un exercice sur l'autre (*recommandation générale n° 16.04*) ;

- constituer un groupe de travail sur les modalités de conservation et d'archivage des comptabilités en fonds spéciaux, incluant le sujet de la dématérialisation, afin d'homogénéiser des pratiques actuellement très différentes d'un service à l'autre (*recommandation générale n° 16.11*) ;

- rappeler aux services bénéficiaires l'obligation d'informer systématiquement la CVFS de toute anomalie constatée dans la gestion des fonds spéciaux **(***recommandation générale n° 17.02) ;*

- ***** *(recommandation générale n° 17.06)* et définir un cadre commun sur la définition et la mise en œuvre de règles minimales de démarquage communes à l'ensemble des services (*recommandation générale n° 16.06*) ;

- renforcer les fonctions du CNRLT en matière de pilotage global des fonds spéciaux : identification des besoins, coordination, évaluation et suivi des recommandations de la CVFS (*recommandation générale n° 17.07).*

**Une recommandation peut être clôturée car elle a fait l'objet d'une étude par le rapport de l'ISR et d'une décision du cabinet du Premier ministre, même si elle n'a pas été suivie :** assouplir l'exigence de production de pièces justificatives pour les menues dépenses dont le montant est laissé à l'appréciation des services (*recommandation générale n° 16.10*).

**Enfin, une recommandation générale a fait l'objet d'une rédaction plus précise.** Au vu des évolutions des structures et des besoins, requestionner le périmètre des services éligibles aux fonds spéciaux *(recommandation générale n° 17.01,* **remplacée par la recommandation générale n° 4).**

**Restent ouvertes au titre du contrôle des exercices 2016 et 2017, 9 recommandations :**

- l'exclusion des fonds spéciaux de l'assiette du calcul de la réserve de précaution du programme 129 (*recommandation générale n° 16.02*) ;

- ***** (*recommandation générale n° 16.05*) ;

- constituer un groupe de travail sur les possibilités de démarquage existantes dans le logiciel Chorus (*recommandation générale n° 16.07*) ;

- augmenter la dotation en fonds normaux à due proportion des montants transférés en fonds spéciaux (*recommandation générale n° 16.09) ;*

- renforcer et formaliser les environnements de contrôle interne – en particulier dans les services bénéficiant d'une augmentation significative de leur dotation en fonds spéciaux – et établir à l'attention de la CVFS une synthèse documentée sur les contrôles mis en œuvre et leurs résultats (*recommandation générale n° 16.13*) ;

- engager une réflexion sur un renforcement des moyens de contrôle et des ressources humaines mis à la disposition de la CVFS en termes d'expertise et de connaissance des services spécialisés de renseignement (*recommandation générale n°16.16*) ;

- 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. (recommandation générale n° 17.03) ;*

- encourager la mise en place d'un travail interservices pour définir un cadre de mutualisation en matière d'acquisitions techniques et expertiser les outils de mutualisation les plus appropriés : ***** *(recommandation générale n° 17.04) ;*

- ***** *(recommandation générale n° 17.05).*

*

*  *

***Délibéré par la commission de vérification des fonds spéciaux lors de sa réunion du 17 décembre 2019.***

# ANNEXE :
# REPRISE DES RECOMMANDATIONS DE LA DPR AU 29 FÉVRIER 2020

## Rapport 2016

| | | |
|---|---|---|
| Complètement prise en compte | 3 | 11 |
| Partiellement prise en compte | 3 | |
| En cours de prise en compte | 5 | |
| Non prise en compte | 2 | |
| Non cotée | | |
| TOTAL | 13 | |

## Rapport 2017

| | | |
|---|---|---|
| Complètement prise en compte | 12 | 16 |
| Partiellement prise en compte | 2 | |
| En cours de prise en compte | 2 | |
| Non prise en compte | 5 | |
| Non cotée | | |
| TOTAL | 21 | |

## Rapport 2018

| | | |
|---|---|---|
| Complètement prise en compte | 22 | 40 |
| Partiellement prise en compte | 7 | |
| En cours de prise en compte | 11 | |
| Non prise en compte | 2 | |
| Non cotée | 5 | |
| TOTAL | 47 | |